
JEFFY MWAKALINGA

Doctoral Dissertation in Computer and Systems Sciences, Stockholm Sweden
“One day, students in one of Albert Einstein’s classes were saying they had decided there was no God. Einstein asked them how much of all the knowledge in the world they had among themselves collectively, as a class. The students discussed it for a while and decided they had 5% of all human knowledge among themselves. Einstein thought their estimate was a little generous, but he replied: “Is it possible God exists in the 95% you don’t know?”” (Creation, 2009, p 2)
I dedicate this thesis to Jesus Christ
ABSTRACT
This research proposes a framework for adaptive information security systems that considers both the technical and social aspects of information systems security. Initial development of information systems security focused on computer technology and communication protocols. Researchers and designers did not consider culture, traditions, ethics, and other social issues of the people using the systems when designing and developing information security systems. They also seemed to ignore environments where these systems run and concentrated only on securing parts of the information systems. Furthermore, they did not pay adequate attention to the enemies of information systems and the need for adaption to a changing environment. The consequences of this lack of attentions to a number of important factors have given us the information security systems that we have today, which appear to be systemically insecure.

To approach this systemic insecurity problem the research was divided into mini studies that were based on the Systemic-Holistic paradigm, Immune System concepts, and Socio-Technical System theory. Applying the holistic research process the author started first by exploring adaptation systems. After exploring these systems, the focus of the research was to understand the systems and features required for making information security systems learn to adapt to the changing environments. Designing and testing the adaptive framework were the next steps. The acquired knowledge from this research was structured into domains in accordance to ontological principles and relationship between domains was studied. These domains were then integrated with the security value-based chain concept, which include deterrence, prevention, detection, response, and recovery functions to create a framework for adaptive information security systems.

The results of the mini studies were reported in a number of papers, which were published in proceedings of international conferences and a journal. For this work, 12 of the thesis papers are included. A framework for adaptive information security system was created. Trials to apply and validate the framework were performed using three methods. The first method was a panel validation, which showed that the framework could be used for providing adaptive security measures and structuring security work. The second method mapped the framework to the security standards, which showed that the framework was aligned with the major information systems security standards. The third and last validation method was to map the framework with reported ICT crimes cases. The results indicated that most crimes appear to occur because the security systems in place lacked deterrence security measures and had weak prevention, detection, and response security measures. The adaptive information security systems framework was also applied to a number of areas including a secure e-learning, social networks, and telemedicine systems.

It is concluded in this thesis that this adaptive information security system framework can be applied to minimize a number of systemic insecurity problems and warrants more applied research and practical implementations.
ACKNOWLEDGEMENTS

I am so grateful to my supervisors, Professor Louise Yngström, and Associate Professor Stewart Kowalski for their wonderful supervision and insights. I give thanks to Professor Sead Muftic for his supervision and support in the first part of the research, the Licentiate of Technology. I thank Professor Paul Johansson for his comments, I thank Associate Professor Mikael Goldstein for his corrections and creative comments. I thank Dr Albin Zuccato for his comments. I am grateful to Professor Oliver Popov for his comments and advice. I give thanks to Dr Anne Håkansson for her comments and Associate Professor Hercules Dalianis for his comments.

I acknowledge the support from the DSV teachers and employees, ICT School employees and teachers, the PhD candidates, members of the Filadelfia church, members of Newlife church and my friends. I appreciate the support of my wife, my son Rasmus Dahlberg, my daughter Dorcas, mother Eva Samuel, Prophet Christine Namagala, Hebron Samuel, Rita Omari, Anna Kalinga, Ambele Samuel, Atu Kalinga, Jenny Kalinga, Naomi Kalinga and all my relatives.
LIST OF INCLUDED PUBLICATIONS


TABLE OF CONTENTS

Table of Figures ........................................................................................................... xxiii
Table of Tables ............................................................................................................. xxvi
Acronyms ..................................................................................................................... xxviii

CHAPTER 1 INTRODUCTION ....................................................................................... 1

1.1 Background ............................................................................................................. 1
1.2 Thinking Process (Research Process) ................................................................. 2
  1.2.1 Overview .......................................................................................................... 2
  1.2.2 Topic Area, fundamental theories and end product ........................................ 3
  1.2.3 Research problem ............................................................................................ 3
  1.2.4 Synthesis ......................................................................................................... 8
    1.2.4.1 The Framework for adaptive information security systems ...................... 9
    1.2.4.2 Architecture for implementation ............................................................... 12
  1.2.5 Themes and Values of Papers ......................................................................... 14
    1.2.5.1 Paper I - Authorization System in Open Networks Based on Attribute Certificates ......................................................... 15
    1.2.5.2 Paper II - Integrated security administration in a global information system ................................................................. 17
    1.2.5.3 Paper III - Integrated security system for e-government based on SAML standard .......................................................... 19
    1.2.5.4 Paper IV - Sketch of a Generic Security framework based on the Paradigms of Systemic-Holistic Approach and the Immune System ................................................................. 21
    1.2.5.5 Paper V - Securing Mobile Agents for Survivable Systems .................... 23
    1.2.5.6 Paper VI - Framework for Securing Mobile Software Agents ................. 25
    1.2.5.7 Paper VII - Methodology for considering environments and culture in developing information security systems ............................................................. 27
    1.2.5.8. Paper VIII - A Holistic and immune system inspired security framework .... 29
    1.2.5.9. Paper IX - Securing e-learning system using a holistic and immune security framework ......................................................... 31
    1.2.5.12 Paper XII – Architecture for adaptive information security systems as applied to social networks .................................................................................. 37
  1.2.6 Reflection ........................................................................................................... 38
  1.2.7 Results - A Framework for adaptive information security systems ................ 39
  1.2.8 Have we solved the problem? ......................................................................... 40
Chapter 2: Validation of the framework for adaptive information security systems

2.1 Validation approach 1: Theoretical Analysis

2.2 Validation approach 2: Panel validation model

2.2.1 Objective, chosen criteria, and evaluation processes

2.2.2 Design of validation instrument

2.2.3 Selecting panel experts

2.2.4 Present results of the validation

2.2.4.1 Usefulness and applicability of the holistic and immune security framework

2.2.4.2 Adaptability features of the security framework to environments

2.2.4.3 Adaptability principles of the security framework to values of users

2.2.5 Relation of results to success criteria

2.3 Validation approach 3: Analysis of Reported ICT Crime Cases

2.4 Summary of validation

Chapter 3 Contributions and Conclusions

3.1 Contributions

3.1.1 Framework for adaptive information security systems

3.1.2 Method of considering culture, traditions, ethics, and other social issues of users when developing information security systems

3.1.3 Model for understanding the methods of an adversary of IT

3.1.4 Principles for securing mobile agents

3.1.6 Principles for securing E-governments

3.1.7 Culture and security value-based chain functions

3.1.8 Application of the framework to secure e-learning and social networks

3.2 Concluding remarks

3.3 Future Work

References

Paper I

1 INTRODUCTION

1.1 General principles

1.2 Requirements

1.3 Authorization Policies

2 Current Approaches

2.1 Some Solutions on Restricting Access
3 Use of Attribute Certificates for Authorization in Open Networks ........................................ 71

3.1 Attribute Certificates ........................................................................................................ 71
3.2 Authentication of Clients and Assignment of Roles ......................................................... 71
3.3 Synchronization of Roles and Authorization Attributes .................................................... 72
3.4 Enforcement in the Authorization System ........................................................................ 72
3.5 Management Infrastructure ............................................................................................... 73
3.6 Delegation of Attributes .................................................................................................... 74

4 Implementation of a Prototype ................................................................................................ 74

4.1 The Access Control Library Suite ................................................................................... 74
4.2 Implementation ................................................................................................................ 75

5 Conclusions .......................................................................................................................... 77
References ................................................................................................................................ 78

PAPER II .................................................................................................................................... 79

1 Introduction ............................................................................................................................ 81

Organization of Sections ......................................................................................................... 82

2 Related work ........................................................................................................................ 82
2.1 Smart Card System ............................................................................................................ 82

2.2 Role–Based Access Control (RBAC) System for Securing a Web-based Workflow .......... 82

3 INTEGRATION .................................................................................................................... 83

3.1 Methodology ...................................................................................................................... 83
3.2 Design of the System ......................................................................................................... 83
3.3 The General Model of the System ..................................................................................... 86

3.4 Registration of Directory Objects from one Interface ....................................................... 86

3.5 Certification of Clients ....................................................................................................... 86
3.6 Smart Card System’s Administration ............................................................................... 86

3.6.1 Creation of File System of the Smart Card ................................................................. 87
3.6.2 Initialization of the Smart Card .................................................................................... 87
3.6.3 Personalization of the Smart Card ............................................................................... 87

3.7 Authorization System ......................................................................................................... 87

3.8 Security Assertion Markup Language (SAML) ............................................................... 87
4 Prototype

4.1 The Directory System

4.2 The PKI System

4.3 Smart Cards System

4.3.1 Initialization of the Smart Card

4.3.2 Personalization of the Smart Card

5 Conclusions

Acknowledgement

References

References

A P P E N D I X

PAPER III

1 INTRODUCTION

2 RELATED WORKS

2.1 Security Assertion Markup Language (SAML) Standard

2.2 INTEGRATED SECURITY SYSTEM (ISS)

2.3 The Challenges of an On-line Government Services

3 E-GOVERNMENT SECURITY SYSTEM

3.1 Architecture of the System

3.2 Security Services

3.2.1 Multiple Authentication Methods

3.2.2 Multiple Authorization Methods

3.2.3 Multiple Non-repudiation schemes

3.2.4 Multiple Integrity Schemes and Availability

3.2.5 Audit, Privacy, Confidentiality and Anonymity

3.3 Advantages and Validation of the System

3.4 Limitation of the System

4 Conclusion

REFERENCES

PAPER IV

1 INTRODUCTION

2 Basic Principles

2.1 Systemic-Holistic Approach

2.2 The Human’s Immune System

2.4 Digital Immune System

XIV
The Monitored System .......................................................................................................................... 149
5 Conclusion ........................................................................................................................................ 151
REFERENCES ..................................................................................................................................... 151
PAPER VII ........................................................................................................................................... 155
1 Introduction ....................................................................................................................................... 158
1.1 Information Systems and Environments ....................................................................................... 158
1.2 Culture and Information Systems ................................................................................................. 159
2 The Steps to take when considering culture of users and system environments in the holistic and immune security framework ........................................................................................................... 160
  2.1 Analyse the threat agent .............................................................................................................. 160
  2.2 Classify Assets and perform risk management ............................................................................ 160
  2.3 Analyze environments where the systems in focus operate ....................................................... 160
  2.4 Assess the effects of culture and traditions of users to information security ......................... 161
    2.4.1 Informal cultural model ......................................................................................................... 161
  2.5 Apply Socio-Technical measures where culture and traditions create weak links in information security ..................................................................................................................................... 163
  2.6 Provide features to make an information system learn to adapt to environments .................. 163
  2.7 Compare allocations of economical resources on the different security value-based chain functions ..................................................................................................................................... 166
  2.8 Educate users of information systems in social engineering and about the security framework. 166
  2.9 Evaluate the outcomes of the implementation of the framework for adaptive information security systems ..................................................................................................................................... 167
3 Conclusion and Limitation .................................................................................................................. 167
4 References .......................................................................................................................................... 167
PERMISSIONS ....................................................................................................................................... 169
PAPER VIII ........................................................................................................................................... 171
1. Introduction ....................................................................................................................................... 173
2. The holistic and immune system inspired security Framework ......................................................... 175
  2.1. Components of the framework ................................................................................................... 175
  2.2 The adaptability system .............................................................................................................. 175
    2.2.1 The environment analyzer .................................................................................................... 175
    2.2.2 The people’s value analyzer ................................................................................................. 176
    2.2.3 The threat analyzer .............................................................................................................. 177
3. Communication in the framework ................................................................. 178
   3.1. Overview .................................................................................................. 178
   3.2. Creation of mobile agents ...................................................................... 178
   3.3. Security of mobile agents ...................................................................... 182
   3.4. Protecting the subsystems ...................................................................... 182
   3.5. Sending an agent for cloning ................................................................. 182

4. Validation ........................................................................................................ 183

5. Conclusion ....................................................................................................... 183

6. References ....................................................................................................... 184

PAPER IX ........................................................................................................... 187
1. Introduction ..................................................................................................... 189

2. Holistic and immune security framework .................................................... 189
   2.1. Provision of Security in an e-learning system ........................................ 190
       2.1.1. Software agents provide security services ...................................... 192

3. Adaptability of the e-learning security system ............................................. 193
   3.1. Environmental analyzer ......................................................................... 193
   3.2. E-learning system users’ cultural values analyzer ................................. 194
   3.3. E-learning system threat analyzer .......................................................... 195

4. Conclusion ....................................................................................................... 195

5. References ....................................................................................................... 195

PAPER X ........................................................................................................... 197
1. BACKGROUND AND INTRODUCTION ......................................................... 200

2. GENERATIONS AND ORGANIZATION OF THE ENEMY OF IT SECURITY .... 201
   2.1 Generations of the Enemy of IT .............................................................. 201
   2.2 The Organization of Hackers .................................................................... 202

3. THE SOCIO-TECHNICAL SECURITY MODEL ............................................. 203
   3.1 Value Chain Model ................................................................................ 204
   3.2 A Socio-Technical System ...................................................................... 206

4. ATTACKING A SYSTEM USING THE SOCIO-TECHNICAL MODEL ............. 207

5. CONCLUSIONS AND DISCUSSION ............................................................. 209

6 REFERENCES .................................................................................................. 210

XVIII
PAPER XI .......................................................................................................................... 212

1. INTRODUCTION ........................................................................................................ 213
   1.1. The Top ten Internet Crimes .................................................................................. 214
   1.2 ICT Crime Prevention Efforts .................................................................................. 214

   2.1 Critical Sub Systems .............................................................................................. 215
   2.2 Critical Systems in the Immune System ............................................................... 215
   2.3 The Architecture .................................................................................................. 216

3. Analysis of Cases ........................................................................................................ 217
   3.2.1 Socio-Technical Measures .............................................................................. 217
   3.2.2 The Cyber Theft Case ..................................................................................... 219

4. Recommendations to Improve the ICT Security ......................................................... 220

5. Conclusions ................................................................................................................ 221

References ..................................................................................................................... 222

Paper XII ......................................................................................................................... 225

Introduction ..................................................................................................................... 227

2. Requirements for a security architecture .................................................................... 228

3. Related security architectures ..................................................................................... 229
   3.2. Security architecture for mobile networks ............................................................ 229
   3.2. Security control framework .................................................................................. 231

4. The architecture for adaptive information security systems ....................................... 231
   4.1. Adaptation services ............................................................................................ 233

5. Securing social networks using the architecture for adaptive information security systems ................. 234

6. Conclusion .................................................................................................................. 236

References ..................................................................................................................... 236

APPENDIX A: Interview preparations .............................................................................. 239
   A.1 Letters .................................................................................................................. 239
   A.2 The respondents ................................................................................................... 239
   A.3. Method of surveying ............................................................................................ 240
      A.3.1 Questions on the strength of the Framework for adaptive information security systems .................................................................................................................. 240

XIX
A.3. Questionnaire to a group of Master students in Information Security and bachelor students in computing science ................................................................................................................................................. 242

APPENDIX B - Template for the Survey on Social and Technical Security measures ........ 247

APPENDIX C – Related work ........................................................................................................ 248

C.1 Related Work: The First Group .......................................................................................... 248
C.1.1 Discussion topic: What is the Old Security Paradigm? .................................................... 248
C.1.2 Why Information Security is Hard – an Economic Perspective ..................................... 249
C.1.3 Three Paradigms in Computer Security ........................................................................... 249

C.2 Related Work: The Second Group ....................................................................................... 250
C.2.1 Information Security Management - A new Paradigm .................................................... 250
C.2.2 The Holistic Security Management Framework for Electronic .................................... 251
C.2.3 Integrating Artificial Immune Algorithms for Intrusion Detection .................................. 252

APPENDIX D – Criteria analysis, results and analysis of surveys ............................................. 256

D.1. Results and analysis of surveys ......................................................................................... 256
D.1.1 Survey of information security experts .......................................................... 256
D.1.1.1 Usefulness and applicability of the holistic and immune security framework ............. 257
D.1.1.2 Adaptability features of the new security framework .............................................. 259
D.1.1.3 Comments ............................................................................................................. 260
D.1.1.4 The Suggested Architecture for Implementation ..................................................... 261
D.1.2 Survey of a group of Master students in Information Security ........................................ 262
D.1.2.1 Usefulness and applicability of the holistic and immune security framework .......... 262
D.1.2.2 Adaptability features of the holistic and immune security framework ................. 263
D.1.2.3 Strength of the new framework in preventing attackers ........................................... 264
D.1.2.4 Allocation of economical resources on the different security value-based chain functions ..................................................................................................................................... 265

D.1.3 Results of a survey in a group of bachelor of science students in computer and engineering .......................................................... 266
D.1.3.1 Usefulness and adaptability of the holistic and immune security framework ............ 266
D.1.3.2 Adaptability features of the holistic and immune security framework ............. 266
D.1.3.3 Strength of the holistic and immune security framework in preventing attacks 266
D.1.3.4 Allocation of economical resources on the different security based chain functions .......................................................... 269

D.1.4 Survey of the master students on the effects of culture on users decisions .................. 270
D.1.5.2.1 Usefulness of the holistic and immune security framework .................................. 272
D.1.5.2.2 Adaptability features of the holistic and immune security framework on environments ............................................................................................................ 273
D.1.5.2.3 Adaptability features of the holistic and immune security framework to values of people ..................................................................................................................................... 274
G.3.4 Other Motivation theories

G.3.3 Why do People deviate?

G.3.2 McClelland’s Theory of Needs

G.3.1 Hierarchy of Needs

G.2.4 Deception and Design: The impact of communication technology on lying behavior

G.2.3 Towards a theory of online learning

G.2.2 The praxis of educating action researchers - the possibilities and obstacles in higher education

G.2.1 Inner person, soul, and outer person

G.1. Overview

APPENDIX E - Overview of Research Methodologies

E.3. Security requirements

E.2. Specific Research Methodologies for Systems

E.1 General research methodologies

APPENDIX F - Theoretical analysis - functional requirements of Common Criteria

F.5 Class User Data Protection

F.4 Class Cryptographic Support

F.3 Class Communication

F.2 Class Security Audit

F.1 Class protection of target of evaluation of security functions (TSF)

APPENDIX G: Culture and motivation

G.3. Theories of Motivation

G.2. Related theories

G.1. Overview

D.1.5.2.5 Allocation of economical resources to the security value-based chains for students from different countries

D.1.5.2.4 Allocation of economical resources to the security value-based chains of the holistic and immune security framework on environments
G.4 Could we apply the same theories to motivate people to do have good security behavior and to motivate people not to have bad security behavior? ................................................................. 310

G.4.1 Motivating the normal employees to do good security management ............... 310
G.4.2 Motivating the deviant employees not to do bad in security management .......... 312
  G.4.2.1 Using negative and positive value-based chain functions to teach deviants.... 313
  G.4.2.2 Designing security system that discourage lying behavior ....................... 315
  G.4.2.3 Entertaining using knowledge bots .......................................................... 315

G.5 Conclusion ............................................................................................................. 318

References .................................................................................................................... 318

APPENDIX H: Autopsy of ICT reported Crime cases ......................................................... 319

H.1 Summary of the reported ICT crimes ..................................................................... 319
H.2 Results of analysis ................................................................................................. 322
TABLE OF FIGURES

Figure 1: The thinking (research) process ................................................................. 2
Figure 2: Security Technology Hype Cycle .............................................................. 3
Figure 3: Trends of Attacking Techniques – Sophistication vs Attacker Knowledge .......... 6
Figure 4: Abuse Opportunities and Control Capabilities vs. Time ............................... 7
Figure 5: Components and relationships of a research process .................................... 9
Figure 6: Holistic research process in developing the Systemic Holistic Approach ............. 10
Figure 7: Overview and details of the framework and the methodology for Security Informatics – the Systemic-Holistic Model ................................................................................. 11
Figure 8: The holistic research process in developing SBC model and STS system ........... 12
Figure 9: A Socio-Technical system ............................................................................ 13
Figure 10: The Security by Consensus model-Semantically syntactical chains ................. 14
Figure 11: A holistic research process in this thesis .................................................... 16
Figure 12: Structuring knowledge in this research ..................................................... 18
Figure 13: The basic model of the framework for adaptive information security systems .... 20
Figure 14: Architecture for implementation ............................................................. 22
Figure 15: Analyzing the weak links caused by culture ............................................... 25
Figure 16: Overview of contributions ......................................................................... 27
Figure 17: Reflection between the end product, research problems, and Questions ........... 36
Figure 18: The Framework for adaptive information security systems .......................... 38
Figure 19: Applying the value-based chain functions for socio-technical controls ......... 39
Figure 20: Validation approach 1: Mapping of the security framework to security standards 41
Figure 21: Average of Results from the survey on technical and social security measures allocation on the value-based chain functions ......................................................... 43
Figure 22: Validation approach 2: using information security experts ........................ 45
Figure 23: Suggested Architecture for Implementation ............................................... 50
Figure 24: Validation approach 3: analysis of Reported Ict Crimes ............................... 51
Figure 25: Future plans of Theory and Practice in IS and IT security ............................ 59
Figure 26: Model of System Components ................................................................ 73
Figure 27: Choosing an Item to Generate .................................................................. 75
Figure 28: SPIF Generator ....................................................................................... 75
Figure 29: Certificate Manager ................................................................................ 77
Figure 30: AdminTool ............................................................................................. 77
Figure 31: Security Assertion Markup Language ..................................................... 85
Figure 32: Login to the System ............................................................................... 90
Figure 33: SAML Architecture ............................................................................... 98
Figure 34: Architecture of Integrated Security System ............................................... 99
Figure 35: Architecture of E-government Security System ......................................... 100
Figure 36: Clonally Selection Algorithm in a Computer Immune System .................... 113
Figure 37: System Model ...................................................................................... 115
Figure 38: Generic Security Framework .................................................................... 117
Figure 39: Mobile Agent Computing Model ........................................................... 126
Figure 40: Generic model for Survivable Systems .................................................... 130
Figure 41: Agents .................................................................................................. 131
Figure 42: Agent Stations ...................................................................................... 131
Figure 43: Helper agent ....................................................................................... 142
| Figure 44: Subsystems | .......................................................... | 145 |
| Figure 45: Architecture of the Mobile Agents Structure | .......................................................... | 149 |
| Figure 46: Login to the System | .......................................................... | 150 |
| Figure 47: Interface of the system | .......................................................... | 150 |
| Figure 48: Interface of the smart system | .......................................................... | 151 |
| Figure 49: Organization: resources of IT and its environment | .......................................................... | 158 |
| Figure 50: Inputs from Environments | .......................................................... | 160 |
| Figure 51: Informal cultural model | .......................................................... | 162 |
| Figure 52: Viable System Model | .......................................................... | 165 |
| Figure 53: Variety and regulation | .......................................................... | 166 |
| Figure 54: Cybernetic structural model | .......................................................... | 166 |
| Figure 55: Security value-based chain | .......................................................... | 174 |
| Figure 56: Components of the Holistic and immune system inspired security framework | .......................................................... | 175 |
| Figure 57: The modified cybernetic structural model | .......................................................... | 177 |
| Figure 58: Informal cultural model | .......................................................... | 177 |
| Figure 59: Agents’ generation process | .......................................................... | 179 |
| Figure 60: Layers of an e-learning system and the holistic immune security framework | .......................................................... | 191 |
| Figure 61: The model of the Holistic and immune security framework | .......................................................... | 191 |
| Figure 62: The modified cybernetic structural model | .......................................................... | 194 |
| Figure 63: Overview of Hackers Types | .......................................................... | 202 |
| Figure 64: The Socio-technical security model | .......................................................... | 203 |
| Figure 65: Average allocation of resources on deterrence, prevention, detection, response, and recovery | .......................................................... | 204 |
| Figure 66: Average allocation of resources on deterrence, prevention, detection, response, and recovery | .......................................................... | 205 |
| Figure 67: Value based chain for computers | .......................................................... | 206 |
| Figure 68: A Socio-technical System | .......................................................... | 206 |
| Figure 69: Applying the Socio-technical security model to attack and to defend systems | .......................................................... | 208 |
| Figure 70: Example of security attack budget using value-based chain | .......................................................... | 209 |
| Figure 71: Centre of gravity | .......................................................... | 210 |
| Figure 72: The model for opportunity theory | .......................................................... | 213 |
| Figure 73: The adaptive information security systems model | .......................................................... | 215 |
| Figure 74: The architecture of the adaptive information security system | .......................................................... | 216 |
| Figure 75: The Socio-Technical System | .......................................................... | 217 |
| Figure 76: How fraud works | .......................................................... | 218 |
| Figure 77: Organization of hackers | .......................................................... | 218 |
| Figure 78: Average allocation of resources on different sub system | .......................................................... | 220 |
| Figure 79: Victimological risk analysis model | .......................................................... | 221 |
| Figure 80: The Security services model NIST | .......................................................... | 229 |
| Figure 81: Security architecture for mobile networks | .......................................................... | 230 |
| Figure 82: Security Control framework of CISCO | .......................................................... | 231 |
| Figure 83: The architecture for adaptive information security systems | .......................................................... | 232 |
| Figure 84: Organization of the threat agent | .......................................................... | 234 |
| Figure 85: Focusing on detection, response and recovery functions | .......................................................... | 235 |
| Figure 86: A sample of results of distribution of a security budget on deterrence, prevention, detection, response, and recovery functions | .......................................................... | 236 |
Figure 87: Components of Information security management system ........................................... 251
Figure 88: Holistic Security Management Framework ................................................................. 252
Figure 89: Conceptual Architecture of the Artificial Immune Model ............................................ 253
Figure 90: Suggested Architecture for Implementation ............................................................... 262
Figure 91: Usefulness of the new for respondents that agree .................................................... 273
Figure 92: Usefulness of the new for respondents that do not agree ......................................... 275
Figure 93: Adaptability features of the holistic and immune security framework ....................... 274
Figure 94: Adaptability features of the holistic and immune security framework to values of users .................................................................................................................. 278
Figure 95: Adaptability features of the holistic and immune security framework to values of users for respondents that do not agree ........................................................................... 275
Figure 96: Allocation of economical resources on the security value-based chain functions 276
Figure 97 Results of allocation of economical resources for a sample of countries ................. 278
Figure 98 Difference in allocation between women and men ....................................................... 279
Figure 99: Results of allocation of technical security measures in the security value-based chain functions...................................................................................................................... 280
Figure 100: Average of Results from the survey on technical and social security measures allocation on the value-based chain functions ....................................................................... 281
Figure 101: Results of allocation of social security measures in the security value-based chain functions .................................................................................................................................. 282
Figure 102: Allocation of budget on security value-based chain from different countries ......... 283
Figure 103: Reasoning in the Design research circle ................................................................. 286
Figure 104: Soft systems methodology ....................................................................................... 287
Figure 105: Inner person, soul and outer person ......................................................................... 299
Figure 106: A model of online learning ...................................................................................... 302
Figure 107: Results from the survey on the need for achievement ......................................... 305
Figure 108: Results from the survey on the need for power ..................................................... 306
Figure 109: Results from the survey on the need for affiliation ................................................. 306
Figure 110: Model of Needs, means and ends ............................................................................. 307
Figure 111: Needs and interaction means .................................................................................... 308
Figure 112: Application of the model in society .......................................................................... 308
Figure 113: Deviants curve ......................................................................................................... 310
Figure 114: The mindset of individuals as a wall protecting ideas ............................................. 311
Figure 115: How to influence individuals .................................................................................... 311
Figure 116: The deviancies mindset wall inside the cultural mindset wall ................................. 313
Figure 117: Positive and negative value-based chain functions .............................................. 314
Figure 118: Attributes for teaching ............................................................................................ 315
Figure 119: Knowledge (ro) bot for teaching and entertaining deviant employees ................. 316
Figure 120: The knowledge bot suggests a break to the employee ............................................ 317
Figure 121: Time used when using a quick guide as compared to when using a knowledge chatbot .................................................................................................................. 317
Table 26: How useful would this holistic and immune security framework and the subsystems can be to your organization?

Table 27: How satisfied are you with the adaptability features of this holistic and immune security framework to environments?

Table 28: How satisfied are you with the adaptability features of this holistic and immune security framework to the values of the people using the information security systems?

Table 29: This Holistic and immune security framework its subsystems will be useful in your organization

Table 30: The adaptability features of this holistic and immune security framework will make information systems learn to adapt to environments where the information systems operate.

Table 31: The adaptability features of this Holistic and immune security framework will make information system adapt to the values of the people (tradition, culture, laws, etc) using the information systems.

Table 32: This Holistic and immune security framework will be successful in preventing an adversary of IT from attacking an information system

Table 33: Results of allocation on different sub systems

Table 34: This Framework for adaptive information security systems its subsystems will be useful in your organization

Table 35: The adaptability features of this Framework for adaptive information security systems will make information systems learn to adapt to environments where the information systems operate

Table 36: The adaptability features of this Framework for adaptive information security systems will make information system adapt to the values of the people (tradition, culture, laws, etc) using the information systems

Table 37: This Framework for adaptive information security systems will be successful in preventing an adversary of IT from attacking an information system

Table 38: Results of the allocation

Table 39: Results of distribution on the security value-based chain functions

Table 40: Results of Outline of budget on the security value-based chain functions

Table 41: Allocation of resources on the different sub systems

Table 42: Distribution of resources to subsystems

Table 43: Differences in allocation between the 60 students’ and the 37 students’ surveys

Table 44: Results of crime cases

Table 45: Social and Technical security measures in the ICT crime case

Table 46: Security services breached in the ICT crime cases

Table 47: Value-based chain functions in the ICT crime cases
ACRONYMS
ACE - Age of Computer Emergence
ACM - Association for Computing Machinery
APCIP - Age of Pre-Computer Information Processing
ASN 1 - Abstract Syntax Notation One
CA – Certification Authority
CC - Common Criteria
CIDF - Common Intrusion Detection Format
CML - Certificate Management Library
DSS - Digital Signature Standard
FIPS - Federal Information Processing Standards
HMAC - Hash-keyed Message Authentication Code
ICT – Information and Communication Technology
ISMS - Information Security Management System
JASP - Jurassic Age Security paradigm
KQML - Knowledge Query and Manipulation Language
NIST – National Institute of Standards and Technology
PKCS – Public Key Cryptographic Standard
PKI – Public Key Infrastructure
PIA - Privacy, Integrity, and Availability
RBAC - Role-Based Access Control
RSA – Rivest Shamir Adelman
SAML - Security Assertion Markup Language
SBC – Security by Consensus Model
SFL - Storage and Retrieval Library
SHA – Systemic-Holistic Approach
SMART - Secure Mobile agents Run-Time System
S/MIME - Secure/Multipurpose Internet Mail Extensions
SOAP - Simple Object Access Protocol
SNACC - Sample Neufeld Abstract Syntax Notation to C/C++
SPIF - Security Policy Information File
STS - Socio-Technical System
TCSEC - Trusted Computer System Evaluation Criteria
TOE – Target of Evaluation
TSF – Target of Evaluation Security Functions
CHAPTER 1 INTRODUCTION

1.1 BACKGROUND

Information security deals with the protection of systems that process, communicate, and store information and include such systems as operating systems, database systems, management systems, and the Internet. These systems are difficult to secure largely because of the initial assumptions made by their designers. Many researchers and security designers of information systems have ignored non-technical issues like culture, laws, and other social issues of the individuals using the systems and the environments where these systems run (Yngström, 1996; Kowalski, 1994). Ross Anderson also points out the need to include both technical and non-technical perspective to deal with the information security problem.

Anderson (2001, p 7), “The management of information security is a much deeper and more political problem than is usually realized; solutions are likely to be subtle and partial, while many simplistic technical approaches are bound to fail. The time has come for engineers, economists, lawyers, and policymakers to try to forge common approaches.”

Many security researchers assumed that cryptography would keep information systems secure. Schneier (1996) in the book Applied Cryptography suggested that cryptography would keep systems safe and secure. However, in Secrets and Lies Schneier (2000) commented four years later that cryptography cannot exist in a vacuum.

Schneier (2000, pp. 1-2), “Cryptography is a branch of mathematics. In addition, like all mathematics it involves numbers, equations, and logic. Security, palpable security that you and I might find useful in our lives, involves people, things people know, relationships between people, people and how they relate to machines. Digital security involves computers: complex, unstable, buggy computers. Mathematics is perfect; reality is subjective.”

To deal with the subjective reality of insecurity in information the author decided to consider both technical and non-technical aspects of information security. Another problem with the traditional approaches to information security is that it has been assumed that all systems, static and dynamic, can be correctly verified with formal methods. However, to verify formally that a static system does what it is supposed to do is expensive, and to verify formally that a dynamic system is correctly implemented has been shown to be impractical (Somayaji, Hofmeyr & Forrest, 1997). Consequently, formal verification methods for information systems are not sufficient and hence other or complementary methods are necessary (Yngström, 1996). The author applied a number of complementary methods. The following methods were applied: the Systemic-Holistic Approach (Yngström, 1996), the immune system (Somayaji, Hofmeyr & Forrest, 1997), and the Socio-Technical System (Kowalski, 1994) as the fundamental concepts. The thinking (research) process (Armstrong, 2006) was applied to guide the investigation, as shown in Figure 1. The next section describes the thinking process.
1.2 Thinking Process (Research Process)

1.2.1 Overview
The thinking process (Armstrong, 2006) was applied for planning and guiding the research process in this thesis as outlined in Figure 1.

The author identified and defined the topic area, the fundamental theories and concepts, the research problem and research questions, and research methodology. The thinking process was further applied to integrate the results of the research and to identify the contributions. The thinking process was also applied to make reflections between the research problems, expected end-product, and the contributions. The process was applied to draw conclusions on whether the goal of the research was fulfilled and whether the gap was filled. The process starts with the topic area and the fundamental theories.
1.2.2 TOPIC AREA, FUNDAMENTAL THEORIES AND END PRODUCT
The first step in the research (thinking) process is to define the topic area of the research. The topic area for this thesis is security for information systems. The second step is to identify the fundamental theories and conceptual models. The fundamental theories for this thesis include the General Systems Theory (von Bertalanffy, 1956), Cybernetics (Wiener, 1948), and General Living Systems Theory (Miller, 1978). Conceptual models as mentioned above include the Systemic-Holistic Approach (Yngström, 1996), the Socio-Technical System model (Kowalski, 1994) and the Immune System model (Somayaji, Hofmeyr & Forrest, 1997). The third step is to state the expected end-product which for this thesis is a framework for adaptive information security systems. After describing the topic area and the fundamental theories and conceptual models, the next step is outlining the research problem, the research questions, and the goal of the thesis.

1.2.3 RESEARCH PROBLEM
One of the systemic problems with ICT and security is that it is a double-edge sword. As Dalal, points out it can be used for constructive and destructive purposes (Dalal, 2006). Over the years, we have seen continuous waves of new technologies to construct better and better security solutions for ICT systems. First, simple reference monitors were developed to monitor and separate different users. Then, multipurpose operating systems, firewalls, intrusion detection systems, and prevention systems were developed.

![Figure 2: Security Technology Hype Cycle (Gartner, 2006)](image-url)
These point security products provide solutions to a single problem rather systems solutions. However, as Gartner’s Hype cycle curve in Figure 2 illustrates many of these technologies do not meet stakeholders’ expectations and it can take between 2 and 10 years for a security product to mature (Gartner, 2006). Von Solms suggests that there are five waves of information security (von Solms, 2010). In the first wave, which lasted until the 1980’s, information security was considered as a technical issue. The second wave, starting at the end of the first wave, resulted with the realization of the need to include the management dimension in dealing with information security. The third wave started in the middle of the 1990s and was based on the need to develop information security standards. The fourth wave, started in 2005, relates to the governance of information security. It is in the fourth wave that senior management understood the impact of social engineering. It was realized that the information security problem could not be solved only by technical measures and that the human side of using IT systems create risks. In the first four waves, companies provided security services in their companies making it hard for criminals to access information in companies. Because of this, criminals turned their attention to the end users who are the weakest link in the chain. The criminals use mechanisms based on social engineering and the Internet is used as an access tool. This led to the fifth wave called cyber security.

The fifth wave, which started in 2006, includes such criminal activities using techniques like phishing, spoofing, malware, and scams. “From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site received 336,655 complaint submissions. This was a 22.3% increase as compared to 2008 when 275,284 complaints were received” (BJA, 2010). The first crime in the report is the category called the FBI scams with 16.6% of the total crimes. In this fraud, a victim receives an e-mail supposed to be coming from the FBI director. In the e-mail, it appears that FBI is trying to get something, like money or identity information, from the victim.

Another type of scam is when a sender uses threatening methods to make a victim part with money. A victim receives an e-mail, which the sender claims to be sent by a gang to assassinate the victim because of some offense against the gang. The victim is asked to send a certain amount of money within 72 hours to the sender or die if the victim does not do that. The second in the top ten Internet crimes is the non-delivery of merchandize in which the victim bought something but it never arrived. Advanced fee fraud is an incident where a victim is promised to receive a huge amount of money if the victim helps to transfer a huge sum of money from the sender. The victim is to pay some kind of expense fee before the transfer. Identity theft is an incident where someone steals an identity or identity information. Overpayment fraud is an incident in which a seller of an item advertizes on the Internet.
Table 1 outlines the top ten most common Internet crime complaints (BJA, 2010).

**TABLE 1: 2009 TOP 10 MOST COMMON INTERNET COMPUTER CRIME COMPLAINT CATEGORIES (COMPLAINS RECEIVED)**

<table>
<thead>
<tr>
<th>Complaint crime category</th>
<th>Percent of total complaints received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  FBI Scams</td>
<td>16.6%</td>
</tr>
<tr>
<td>2  Non delivery of merchandize</td>
<td>11.9%</td>
</tr>
<tr>
<td>3  Advanced fee fraud</td>
<td>10.4%</td>
</tr>
<tr>
<td>4  Identity theft</td>
<td>10.3%</td>
</tr>
<tr>
<td>5  Overpayment fraud</td>
<td>7.9%</td>
</tr>
<tr>
<td>6  Miscellaneous consumer fraud</td>
<td>5.7%</td>
</tr>
<tr>
<td>7  SPAM</td>
<td>4.8%</td>
</tr>
<tr>
<td>8  Credit card fraud</td>
<td>4.5%</td>
</tr>
<tr>
<td>9  Auction fraud</td>
<td>4.3%</td>
</tr>
<tr>
<td>10 Computer damage (intrusion/hacking)</td>
<td>3.5%</td>
</tr>
</tbody>
</table>

The purchaser gives to the seller a counterfeit cheque that has an amount in excess of that agreed. The seller is asked to deposit the cheque and wire back the excessive amount immediately to the buyer but the cheque bounces at the bank and the wired amount is never returned. Miscellaneous consumer frauds are different types of frauds where victims are asked to send money where nothing is bought or sold. Spam is unwelcome mass distributed e-mails. Credit card fraud is an incident where someone is charging goods or services to victims’ credit cards. Auction fraud occurs during online auction transactions. Computer damage occurs because of intrusions or some kind of hacking to victims’ computers.

These categories of Internet crimes are proven difficult to prevent using only technological controls. It appears that we need to provide both social and technical controls in combinations since the attackers use both technology and social engineering methods to attack information security systems.

The attackers do not need much technical knowledge to attack systems because there are many tools (Ciampa, 2010) as outlined in Figure 3.
Information security systems that use only technical security measures have a hard time keeping up with attackers who use both social and technical measures. Attackers can design new social and technical methods of attacking information security systems. Therefore, we need to apply both social and technical security measures to defend systems. In addition, we need to have social and technical security measures that are adaptive.

As Figure 4 (Kowalski, 1994, p 57) suggests there is always a gap between what we can do and what we can control with ICT, which creates a systemic risk area along with, the computer abuse opportunity, curve, the social, socio-technical, and technological controls curves. Figure 4 also outlines the capability to control computer abuse over time in a society. Because of this systemic gap, the ability for information systems to adapt to cultural and environmental
changes is lower than the ability for information security systems to adapt. To make the information security system adapt in accordance to the need more effort should be placed upon socio-technical controls. There is a need to provide adaptive social and technical security measures to environments and culture in the framework.

![Diagram of Abuse Opportunities and Control Capabilities vs. Time](image)

**FIGURE 4: ABUSE OPPORTUNITIES AND CONTROL CAPABILITIES VS. TIME (KOWALSKI, 1994, P 57)**

In short, one can describe the research problem as how to minimize the gap between the capabilities of information security systems to control abuse and the needed capabilities as Figure 4 indicates. That is, to reiterate, how do we make sure that what we can do with information systems match well with what we can control?

The research problem was divided into the following research questions.
a) What are the critical systems for adaptive information security systems? According to Miller (1978), 19 critical systems must be present in every living system for it to survive in different environments. The author believes that there are critical systems or functions that should be present in every framework for adaptive information security systems in analog to living systems.

b) What adaptation systems are needed to making information security systems adapt to environmental and cultural changes? Studies should be performed to understand how to provide adaptation measures in information security systems for adapting to environmental and cultural changes.

c) How can identity management be provided in adaptive information security systems? Study how to provide security services in the adaptive information security systems.

d) What models are IT adversaries using to attack information systems and how can these be circumvented? In order to understand how to defend information systems it is necessary to understand the methods and tools that an enemy is applying to attack information systems.

e) How can these results from the investigation be applied to protect information systems?

The goal of this holistic investigation was to explore, understand, explain, design, test, and discover how to minimize the gap between the ability of information systems to adapt to environmental and cultural changes and the ability of information security systems to adapt to these same changes.

1.2.3 Research Methodology

The fourth step is to select the research methodology. The author did a literature survey (see related work in appendix C). The author tested and reviewed a number of different research methodologies (see overview of research methodologies in appendix E) and selected the holistic research process as outlined by (Schwaninger, 2007). Figure 5 outlines the holistic research process. With the Schwaninger methodology, a researcher can start at any point in the holistic research process and what is important is to close the loop. If a researcher starts with exploration, the result could be discovery of knowledge if the goal was to discover knowledge (arrow 1). Discovery can also be targeted through systematic testing (arrow 3). Discoveries could enable new designs (arrow 4). A design could be further explored (arrow 6) and this closes the research process loop 4-6-1. The loop of arrows 2, 5, and 6 represents a research process in which exploration brings more understanding leading to a design. The design triggers further exploration to improve the design as shown in Figure 5.
The loop 7-8-9 shows a research process from testing, explaining and designing. The research process signifies the improvement of design by making a sequence of changes in a design. The changes are then tested and the results have to be interpreted and explained. The loop 4-7-3 is a sequence in which tests are made resulting in discoveries, which are put into designs, which could be further tested. The loop 10-9-5 is a research process in which a phenomenon is explained to increase understanding, which results in a design (Schwaninger, 2007). The next sections show examples of how the holistic research process can be applied when describing the research that led to the Systemic-Holistic Approach (SHA) (Yngström, 1996), the Immune Digital System (Kim, 2002), the Socio-Technical System (STS) and the Security by Consensus (SBC) model (Kowalski, 1994).

1.2.3.1 Systemic Holistic Approach
In her research developing the Systemic Holistic Approach it appears that Yngström (1996) followed the research process loop explore -> understand -> design -> test -> discover, 1-2-5-7-
3, as outlined in Figure 6. Yngström explored IT security in relation to modern IT structures (arrow 2).

The research question was how to understand security in relation to modern living environments and modern information technology. Yngström developed the Systemic Holistic Approach (arrow 5), as shown in Figure 7 (Yngström, 1996), for investigating, studying, structuring, specifying, evaluating IT security problems and possible solutions. SHA is based on the General Systems Theory (von Bertalanffy, 1956), Cybernetics theory (Wiener, 1948) and General Living Systems Theory (Miller, 1978). The Systemic-Holistic model is composed of two components: a systemic module and a three dimensional framework. The dimensions in the framework include the levels of abstraction, the context orientation, and the content area as shown in Figure 7.
The dimension of the levels of abstraction consists of design or research; theory or model; and physical construction. The context orientation dimension can be geographical space and time bound. The content dimension has technical issues and non-technical issues. Technical issues include processing, storing, communication, collecting and displaying information. Non-technical issues include operational, managerial, legal, ethical, social, and cultural. The Systemic-Holistic Approach is used for analyzing and studying security problems, for governing design, operation, management, and evaluation of secure systems. The Systemic-Holistic Approach can be used to study a system as a whole or in detail and to study an environment of a system. Different aspects of a security system can be defined, investigated, evaluated, and analyzed at any design, theoretical or construction level, and in any time dimension. Yngström tested the approach on academic IT security education (arrow 7). Yngström discovered that the holistic approach facilitates the understanding of IT security problems and helps students develop knowledgeable attitudes useful on the labor market,
which is arrow 3. The Systemic-Holistic Approach has been used in implementing and conducting bachelor and master programs in information security in computer science. In the next section, the author describes the Security by Consensus model and Socio-Technical system.

1.2.3.2 The Security by Consensus Model and Socio-Technical System
Kowalski (1994) appears to have followed the research process loop explore->discover->design->explain->test->discover, 1-4-9-8-3, in the holistic research process (Schwaninger, 2007) as shown in Figure 8.

![Figure 8: The Holistic Research Process in Developing SBC Model and STS System](image)

The insecurity problem as associated with IT systems was explored as an emergent property of socio-technical systems (arrow 1). The social and technical measures were discovered to protect information adequately and developed (designed) the Socio-Technical system, Figure 9, which is arrow 4 in the holistic research process. The Socio-Technical System was developed to study and analyze all levels of IT systems security. When any of the components of the Socio-Technical System change, the other components change too in order to keep the balance. When a new machine is introduced in an organization, it could affect the methods for using the machine, structure, and culture in the organization. For example when a smart card system is introduced in the organization, it could affect the current operating system. It could require new legal security measures. The new legal security measures could affect the ethical and operational security measures, which could necessitate a change in the current ethical controls. The author of Socio-technical system also developed (designed), arrow 4, the Security by Consensus (SBC) (Kowalski, 1994). The SBC model considers the static and dynamic
characteristics of IT systems security. The static characteristics are considered as a layered framework containing the social and technical measures in an IT system.

Social security measures include the ethical-cultural, legal, administrative-managerial-policy, and operational. Ethical-cultural measures include all informative and educational measures taken to clarify particular ethical and cultural problems relating use of IT. Legal measures include informing people the laws and the punishments that could be imposed to the breaker. Administrative/managerial include management prevention measures, monitoring and control of personnel, and formulation and control of IT security policies and regulations. Operational and procedural measures involve creating prevention procedures. The technical security measures include the mechanical/electronic; hardware; operating system; application; data, store, process, and collect information. The social measures are considered as day-to-day IT security measures while the technical security measures are referred to as emergency IT security measures. The dynamic characteristics result in applying the layered framework to the problem of securing communication in a system and between systems. The SBC model was applied in analyzing and comparing European and North Americans evaluation criteria.

FIGURE 9: A SOCIO-TECHNICAL SYSTEM
Figure 10 outlines semantic and syntactic chains of the SBC model in the social and technical mechanisms. The chains imply that the semantics of one layer in a social-technical system are used to give meaning to the next layer. For example, semantics of ethics are supposed to give meaning to syntax of the law layer. The semantics of the law layer are to give meaning to the syntax of the layer of policies. These semantic and syntax chains can be used to develop secure systems for exchanging information. For example, two people in different countries exchanging information have to agree on the ethical, law, policy, procedural and technical protocols to exchange information. A secure model for a patient medical record and an online security handbook were also developed. The SBC and Socio-technical systems were tested in organizations in Sweden and Canada (arrow 7), in Figure 8. The results of tests were interpreted, analyzed, and explained (arrow 8). After describing the Socio-Technical system and SBC model the author briefly describes the immune system.

1.2.3.3 The Immune System and Digital Immune System
A number of researchers (Forest, Hofmeyr, & Somayaji, 1997; Kim, 2002) of digital immune systems have followed the research process loop explore -> understand -> design -> test -> explain, 1-2-5-4-7-8, in the holistic research process (Schwaninger, 2007). They have explored and discovered the principles of the immune system that could be applied to secure information systems. The researchers have designed systems, tested the principles, and explained the results of the tests.
The immune system has features that make a human being survive in different environments. This system protects the human body from many different threats such as viruses. It has two main layers, the outer layer, and the adaptive layer. The outer layer consists of skin, pH, inflammatory responses, etc. The adaptive layer of the immune system has white blood cells called lymphocytes (Kim, 2002). These white blood cells produce antibodies, which attack and destroy foreign cells. There are two main types of lymphocytes: B-cells and T-cells. B-cells are developed in the bone marrow while T-cells are developed in thymus. B-cells are antibody cells and they are supported by T-cells in discovering viruses that are hidden inside cells. Several chains of DNA represent the B-cells and T-cells because these cells have special genetic structures. B-cells mutate at a higher rate than T-cells. B-cells have more receptors than T-cells. In the bone marrow and thymus there are different types of gene libraries (DNA) and the libraries contain different expressions for candidate B-cells and T-cells.

The expressions for B-cells and T-cells are selected randomly. Before being released in the body to start functioning, they must pass a test called negative selection algorithm. These cells have as a function to detect cells or viruses that do not belong to the body. When they detect viruses, they are supposed to bind to them and kill them. The negative selection algorithm is used to test whether the cells detect correctly, meaning that the organisms that were detected indeed do not belong to the body. Therefore, this algorithm tests these cells whether they incorrectly bind to ‘self’ cells, which belong to the body. Those cells that bind incorrectly are killed. Those B-cells and T-cells that pass this negative selection algorithm are released into the body. When a B-cell monitors in the body and discovers an antigen it can bind to it with strong affinity, which is above a certain threshold, or with less affinity below a certain threshold. If this B-cell binds to an antigen with less affinity then the T-cell will help to activate this B-cell. The cells that produce good results are cloned. During the period of activation, B-cells produce memory cells with properties to remember the previous antigens that were detected (Forest, Hofmeyr, & Somayaji, 1997). The digital immune system was designed by (Forest, Hofmeyr, & Somayaji, 1997) and was applied for virus protection (Symantec, 2001). The next section describes the application of the holistic research process (Schwaninger, 2007) in this research.

1.2.3.4 APPLYING THE HOLISTIC RESEARCH PROCESS IN THIS THESIS
The author divided the research into mini-studies. The results from the mini-studies were reported in papers, which were presented in international conferences and then published in the proceedings of the conferences. In this research the author followed research loop explore --> understand --> design -->test --> discover--> design, 2-5-7-3-4, in the holistic research process (Schwaninger, 2007), as shown in Figure 11.
The author explored the adaptation systems and critical systems for information security systems. The author also explored the cultural, traditional, ethical, and other social issues and their effect on security of systems as discussed in the paper IV, *Sketch of a Generic Security framework based on the Paradigms of Systemic-Holistic Approach and the Immune System* (Mwakalinga & Yngström, 2005b). The economical factor was also explored in relation to the IT markets of security products (Kowalski, Nohlberg & Mwakalinga, 2008). The author also explored how to model an adversary of IT as described in the paper X, *Modeling the Enemies of an IT Security System - A Socio-Technical System Security Model* (Kowalski & Mwakalinga, 2011).
The author came to better understanding of the systems and features required for making information systems learn to adapt to environments. A framework for adaptive information security systems was designed as reported in the paper VIII, A holistic and immune system inspired security framework (Mwakalinga, Yngström & Kowalski, 2009a). A methodology for applying the framework for adaptive information security systems was designed as described in the paper VII, Methodology for considering environments and people in developing systems and application of holistic and immune security framework (Mwakalinga, Kowalski & Yngström, 2009c). The author also designed the security framework for software agents that provide security services in the framework for adaptive information security systems. This was reported in the papers V and VI, Securing Mobile Agents for Survivable Systems (Mwakalinga & Yngström, 2005a), and Framework for Securing Mobile Software Agents (Mwakalinga & Yngström, 2006b). The author designed different components of the security framework. The first component is the authorization system for providing authorization in the security framework as reported in the paper I, Authorization system in open networks based on attributes certificates (Mwakalinga, Rissanen & Muftic, 2003). The author also developed an architecture for implementation of the adaptive information security systems as described in paper XII, Architecture for adaptive information security systems as applied to social networks (Mwakalinga & Kowalski, 2011c). The second component is the integrated security system for identity management and provision of security services in the framework as reported in the paper II, Integrated security administration in a global information system (Mwakalinga & Yngström, 2004a). The integrated security system component was applied in designing a security for e-government system as reported in the paper III, Integrated security system for E-government based on SAML standard (Mwakalinga & Yngström, 2004b).

Thereafter the holistic and immune inspired security framework was tested (validated). The adaptive framework was validated in three dimensions. The first dimension was validation by checking how the framework for adaptive information security systems mapped with the international security standards given that they should reflect reality of information security systems. The second dimension was validating the framework by using a panel validation model (Beecham, et al, 2004) by interviewing experts in information security because they know the reality of information security systems. The third dimension was validation of the framework to reality of information security by doing an autopsy of the reported ICT crimes cases as described in the paper XI, ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security (Mwakalinga & Kowalski, 2011). In addition, the publications in this thesis were extensively reviewed by reviewers of international conferences. Validation is described in chapter 2.

The author discovered how to minimize the gap between the capabilities of information security systems to control abuse and the needed capabilities of information security system. The next section describes synthesis, which is the next step in the thinking process.

1.2.4 SYNTHESIS

The sixth step in the thinking process (Armstrong, 2006) is the synthesis. In this section, the author will describe the integration of the different results from the mini-studies of the research. In the first section, the author will present the framework for adaptive information security services. In the second section, the author will present the architecture for implementation. The author applied the epistemological principles to integrate the different results from the mini studies.
Epistemology is the theory of knowledge, from philosophy of science, which is concerned with the nature and limitation of knowledge. It studies what knowledge is and how it is acquired, what people know, what people do not know, and how people know what they know. Knowledge, according to Plato, is a subset between truths and beliefs (Popper, 1972). “The more we learn about the world and the deeper our learning, the more conscious, specific, and articulate will be our knowledge of what we do not know, our knowledge of our ignorance. For this, indeed, is the main source of our ignorance — the fact that our knowledge can be only finite, while our ignorance must necessarily be infinite” (Popper, 1972). What we know, knowledge, is just a small percentage of what we do not know, which is ignorance, because ignorance is infinite.

The author also applied ontological principles to integrate the different results of the research. In information science security, “ontology is a constructed model of reality, a theory of the world-more practically, a theory of a domain. In still more practical terms, it is a highly structured system of concepts covering the processes, objects, and attributes of a domain in all of their pertinent complex relations” (Neirenburg & Raskin, 2001). In this research, the framework for adaptive information security systems was divided into three domains as shown in Figure 12.

![Figure 12: Structuring Knowledge in This Research](image)

The first domain contains basic cybernetic concepts such as inputs, processes, outputs, and feedback controls. The author applied the Cybernetics’ third order feedback mechanism to
regulate and control the outputs of the processing (Schoederbek & Kefalas, 1990). The Cybernetic feedback mechanism has functions to transform the disturbances that come in the form of inputs so that they should cause no harm to an information security system. The second ontological domain consists of a set of five functions of deterrence, prevention, detection, response, and recovery. The third domain is an iteration of domain one into domain two. This research produced knowledge, which was structured into domains in accordance to the ontological principles. The relationship between domains was studied as outlined in Figure 12.

1.2.4.1 THE FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS

In this section the framework for adaptive information security systems, which is the basic model for the Framework for adaptive information security systems, is presented. Figure 13 outlines the framework for adaptive information security systems. The author uses the Systemic-Holistic Approach (Yngström, 1996), the Immune system (Forest, Hofmeyr, & Somayaji, 1997), the Security by Consensus model (Kowalski, 1994), and the Socio-Technical system (Kowalski, 1994) as fundamental concepts. The author explored the principles required for the framework for adaptive information security systems. The author identified the principles required from the Systemic-Holistic Approach. The principles include the holistic view, analysis of technical and non-technical factors that affect information security, analysis of environments where information security systems run, securely store, process, display, and transmit information. The principles that were necessary from the immune system were then identified. These principles include adaptability, autonomy, multiple level, identification, memory, diversity, distribution, and dynamic coverage. Thereafter the principles that were needed in the security model from the Socio-Technical system and Security by Consensus model were identified. These principles include assessing the effects of culture to information security, analyzing the threat agent, studying security levels, and how to apply social and technical security measures required to strengthen the vulnerabilities that were created by culture. Thereafter the author identified the critical systems that should be present in an information security system.

According to Miller (1978), 19 critical systems must be present in every living system for it to survive in different environments. The author believes that there are critical systems or functions that should be present in every framework for adaptive information security systems analogous to living systems. The author identified the critical systems that should be present in every framework for adaptive information security systems. The critical functions are integrated into the security value-based chain. These functions include the deterrence, prevention, detection, response, and recovery (Kowalski & Boden, 2002; Eschenbrücher et al., 2004). Kowalski developed the Value-based chain for security (Kowalski & Boden, 2002) from the Value chain model (Porter, 1985). The Value chain model was first established by Porter (1985) to describe the concept of value adding activities in a company. The Value chain model was aimed at maximizing value creation at minimum costs.
Security value in the deterrence, prevention, detection, response, and recovery functions is added in the following way. In any framework for adaptive information security systems there has to be measures to scare away attackers in the deterrence function. If one fails to deter attackers then one should have measures to prevent attacks in the prevention function. If one fails to prevent attacks, the next step is to detect the attacks in the detection function. If one fails to detect attacks, the next step is to respond to the attacks. If one fails to respond properly to attacks the next step is to recover from attacks. The idea of adding values is to make it very
difficult and more expensive for the attacker to attack the information security system. In every critical value-based chain-function, there is a feedback mechanism. For every disturbance to the critical system, there is a regulator. This is in line with the Law of Requisite Variety (Ashby, 1956) that states that the “Quantity of regulation that can be achieved is bounded by the quantity of information that can be transmitted in a certain channel” (Umpleby, 2008). Therefore, the number of regulators must be equal or greater than the possible disturbances expected from the changing environments. The aim is to maintain stable states on the critical systems. This feature is borrowed from the immune system that keeps all the essential variables in a body within acceptable states or in Ashby’s (1956) terminology Homeostasis.

The framework for adaptive information security systems applies the Cybernetic feedback mechanism, fault tolerance measures and adaptability principles to keep an information system in a state of homeostasis independent of the environmental and internal disturbances. One of the properties of living systems is goal seeking (Schoederbek & Kefalas, 1990) and the framework for adaptive information security systems seeks to keep entropy of an information system as low as possible. Information systems suffer natural entropy because adversaries of IT constantly develop new strategies for attacking systems; most information systems do not learn to adapt to changing environments; and technology changes (Kings, 2008). The second level in the framework for adaptive information security systems, according to the ontological principles, is a set of the critical subsystems, which builds on the input, process, outputs, and feedback controls. The third level is the framework for adaptive information security systems, which according to the ontological principles is the management section for managing attributes, relationships, and communication among the different components.

1.2.4.2 ARCHITECTURE FOR IMPLEMENTATION

There are many different ways to describe computer system architecture. The computer system architecture describes the structure and behavior of the components of the system. This section briefly describes the architecture for implementation as outlined in Figure 14. The architecture is organized based on the Viable system model (Beer, 1984) as described in the paper VIII, A holistic and immune system inspired security framework (Mwakalinga, Yngström & Kowalski, 2009a). The next sections describe the different components in the architecture.

SYSTEM MANAGER AND INTEGRATED SECURITY FRAMEWORK

The first component is the system manager. This is the only component that has access to all the components. The system manager creates rules, identities, goals, and security policies of operations and monitors the behavior of all the components in the security framework. The system manager activates the security framework and initializes all the components of the framework. The integrated security system performs identity management and provides security services in the whole framework. The integrated security system is the commanding and coordinating system. All components of the security framework request specialized software agents for providing security services in the security framework.
THE AGENT CREATOR
The agent creator generates software agents as shown in figure 14.

FIGURE 14: ARCHITECTURE FOR IMPLEMENTATION
The software agents are created based on the prior knowledge of adapting principles. This knowledge is stored in the database of gene libraries. This gene library contains genes that have been predetermined based on a priori knowledge (Kaneshige & Krishmakumar, 2007). The genes combine to form different solutions like the way one combines Lego blocks to form some solution. The gene libraries provide information for the agent creator. The agent creator acts like a bone marrow in the human body that creates B-cells. The agent creator combines genetic expressions from the database of genetic expressions and artificial immune algorithms from the database of artificial immune system algorithms to create agents. The agent creator gives security agents specialized principles for the deterrence, prevention, detection, response, and recovery and send the agents to the respective subsystems as shown in Figure 14. These
mobile agents provide security services to all the components of the security framework and the information system.

The bone marrow contains the gene library, which is the DNA (Kim, 2002). The gene library rearranges the genes to create pre-detectors, which are future B-cells. These pre-detectors are tested using the negative selection algorithm (Kim, 2002) before leaving the bone marrow to determine whether they detect ‘non-self’ foreign cells and whether they do not detect the ‘self’ cells that belong to the body. The agent creator represents the bone marrow of the body. Those that pass this test go to the body and start monitoring in the human body. The agent creator applies the a priori knowledge to create different normal and abnormal profiles for the deterrence, detection, prevention, response, and recovery sub systems. The agents that pass the test are allowed to monitor in security framework.

The agent creator applies the Negative selection algorithm to test the agents for deterrence, detection, prevention, response, and recovery sub systems (Kim, 2002). The agent creator trains all the agents before releasing them into the real environment. The components monitor the performance of agents, record the agents, and inform the agent creator the principles of the most successful agents, according to policy specified criteria. The successful agents are cloned using the clonally selection algorithm (Kim, 2002). These principles are stored in memory. The agent creator applies these principles to improve the principles of next generation of agents.

**Deterrence, prevention, detection, response and recovery sub systems**

The next component is the deterrence system, which is responsible for scaring away attackers as reported in the paper IV, *Sketch of a Generic Security framework based on the Paradigms of Systemic-Holistic Approach and the Immune System* (Mwakalinga & Yngström, 2005b). It applies the principles of cybernetics feedback mechanisms, principles of immune system and other systems to deter attackers. It applies software agents to perform detection and deterrence of surveillance attempts, attacks, and intrusions and take action based on the security policy. The prevention system applies the Cybernetic feedback mechanisms, principles from the immune system, the Systemic-Holistic Approach (Yngström, 1996), Socio-Technical system (Kowalski, 1994) the Security by Consensus model (Kowalski, 1994) and other systems to provide social and technical measures for preventing attacks to the security framework. The detection system applies neural networks, fuzzy logic, Cybernetic feedback mechanisms, principles from the immune system to provide measures for detecting attacks and intrusions to the attacks. The detection system also uses the Systemic-Holistic Approach (Yngström, 1996), the Socio-Technical system (Kowalski, 1994) the Security by Consensus model (Kowalski, 1994) to provide measures for detecting attacks and intrusions. The response system applies the software agents to respond to different attacks and intrusions to the security framework. The recovery system is responsible for putting the security framework back to normal operation after attacks and intrusions. The security functions are applied at the application, transport, internet, and link layers.

**Adaptation services**

The next component is the adaptation system, which provides adaptation services. The adaptation system is divided into three sub-components.

ENVIRONMENT ANALYZER
The first sub-component is the environment analyzer, which provides measures for making an information security system learn to adapt to environments. Ashby (1956) proposed two types of adaptations. The first type is to make the system adapt to an environment. The second type is to make the system learn to adapt when the environment changes. The Cybernetics feedback mechanisms (Wiener, 1948), digital immune system, variety and regulation (Herring, 2002) and Cybernetic structural models (Howland, 1990; Herring, 2002) are applied for the first type of adaptation. The Viable System Model (Beer, 1984) is applied for the second type of adaptation. Analyzing environments where an information security system operates, involves identifying the local environment, embedded environment, total environment, and predicting future environments. It also involves classifying the environments, analyzing the levels of security of these environments. An observation is made over a period to study the inputs that are coming from the environments and affecting an information security system. This is described in the papers VII and VIII, Methodology for Considering Environments and People in Developing Systems and Application of Holistic and immune security framework (Mwakalinga, Kowalski & Yngström, 2009c) and A holistic and immune system inspired security framework (Mwakalinga, Yngström & Kowalski, 2009a). The analyzer collects data on environmental disturbances from all the components and stores them in a database. The analyzer applies the collected data to create probabilistic models and to forecast the future environmental disturbances and thereby foresee how the framework will react to those future disturbances. This is described in the paper IV, Sketch of a Generic Security framework based on the Paradigms of Systemic-Holistic Approach and the Immune System (Mwakalinga & Yngström, 2005b).

PEOPLE’S VALUE ANALYZER
The second sub-component is the People’s value analyzer, which applies the informal cultural model (Mwakalinga, Yngström & Kowalski, 2009a), the Socio-Technical system (Kowalski, 1994) the Security by Consensus model (Kowalski, 1994) to analyze culture and other social issues of users. The effects of culture and traditions on users are assessed in the following way. The author predicts the behavior and preferences of users in different cultures using the informal cultural model (Mwakalinga & Yngström, 2005a). Some behaviors and preferences of users of different cultures can create vulnerabilities in the framework for adaptive information security systems. Vulnerabilities are analyzed.

ANALYZING THE VULNERABILITIES CREATED BY CULTURAL BEHAVIOR AND PREFERENCES IN THE FRAMEWORK
The author applies the Socio-Technical system (Kowalski, 1994) to analyze the vulnerabilities created by cultural behavior and preferences in the framework for adaptive information security systems. The vulnerabilities that were created by cultural behavior and preferences are dealt with by applying social and technical security measures (Kowalski, 1994). The Security by Consensus model (Kowalski, 1994) is applied to remove the vulnerabilities as described in the paper VII, Methodology for Considering Environments and People in Developing Systems and Application of Holistic and immune security framework (Mwakalinga, Kowalski & Yngström, 2009c).

APPLYING SOCIO-TECHNICAL MEASURES WHERE CULTURE AND TRADITIONS CREATE WEAK LINKS IN INFORMATION SECURITY
The Socio-Technical system (Kowalski, 1994) is applied to analyze the weak security links created by cultural behavior and preferences in the framework for adaptive information
security systems. Thereafter the Security by Consensus model is applied to strengthen the weak security links as outlined in Figure 15.

Apply the informal Cultural model to predict behavior of users
Apply the Socio-Technical system to analyze the weak security links created by cultural behavior and preferences in the holistic information security model
Apply the Security by Consensus model to remove the weak security links

FIGURE 15: ANALYZING THE WEAK LINKS CAUSED BY CULTURE.

For instance, Chaula (2006) conducted a study on the effect of human behavior on systems security. It was found that people with low uncertainty avoidance tend to lack holistic approaches to security. This implies that they lack security in depth measures and they lack attention to details. In the framework for adaptive information security systems, the security policy will specify the holistic security measures to take care of these vulnerabilities. People with low uncertainty avoidance tend to perform inaccurate risk assessment, because they have poor assumption about motivation, opportunity and methods, lack of information classification, and use metrics poorly (Chaula, 2006). In the framework for adaptive information security systems, procedures and security policies will be created so that there should be good risk assessment and information classification. Cultures where people have low future orientation have ineffective contingency planning. This affects prediction of disasters and preparation if an attack or a disaster was to occur. The framework for adaptive information security systems will put effective contingency and continuity plans through the security policies, procedures, and designs. Cultures where power distance was high result in poor communication on security issues between upper level management and employees and technicians. The framework for adaptive information security systems will enforce policies and procedures, which require continuous communication on security issues between upper level management and employees and technicians. Surveys were made to understand the effect of culture of users on decisions regarding the importance of value-based chain functions as described in the following sections.

THREAT ANALYZER
The last sub-component of the adaptation system is the threat analyzer, which applies the socio-technical, and economical model (Kowalski, Nohlberg & Mwakalinga, 2008) to analyze the tools and methods that attackers apply to attack an information security system. The Social-technical-economical model is used for addressing security problems at different levels and perspectives. Analysis is undertaken to understand the model that an adversary of IT applies to attack information security systems. The adversary of IT investigates the tools and methods that an information security system is applying to defend in the deterrence, prevention, detection, response, recovery, and other components. The adversary is using a model related to the socio-technical and economic model (Kowalski, Nohlberg & Mwakalinga, 2008) to attack information systems as described in the paper VIII, a holistic and immune system inspired security framework (Mwakalinga, Yngström & Kowalski, 2009a). After gathering the
information on tools and methods used to defend a system, the adversary of IT decides whether it is economical to attack an information security system or not. This is further described in Chapter 2. The next components in the architecture are the fault tolerance, security manager, and special analysis.

**Fault Tolerance, Security Manager and Special Analysis**

The next component provides fault tolerance services. This component performs fault tolerance services in every component of the security framework. The component is responsible for error detection measures, damage assessment measures, damage confinement measures, error recovery measures, fault treatment, locator, and continued service measures in the *holistic and immune system inspired security framework*. The security management component uses the recovery sub system to perform the risk management, security policy management, compliance management, and continuity planning management services for the security framework and the information system. The special analysis performs special analysis of unknown and abnormal inputs as requested by the sub-systems. The next section presents the themes and values of papers where the results of the mini studies are reported.

1.2.5 THEMES AND VALUES OF PAPERS

This section briefly presents the themes and values of papers as shown in Figure 16.
The study was divided into mini studies. The results from the mini studies are presented in papers that were presented in international conferences and the papers were published in proceedings of the conferences. The author explored the adaptation systems and critical systems for information security systems (Papers IV & VIII); explored cultural and other social issues and their effect to security (paper VII); explored social-technical and economical (Kowalski, Nohlberg & Mwakalinga, 2008); explored modeling the adversary (Papers VIII) as outlined in Figure 16.

Then the author understood the features and principles required for making information systems learn to adapt (Papers IV & VIII). Thereafter the author designed a global integrated security administration system (Paper I); designed an authorization system (Paper II); developed integrated security system for E-government (Paper III); developed a holistic and immune system inspired security framework (paper VIII). The author designed a methodology for applying the holistic information security model (Paper VII); developed a security framework for software agents (Papers V & VI); developed an architecture for adaptive information security systems (Paper XII). The author validated the framework by applications to e-learning system (Paper IX), and telemedicine system (Mwakalinga, Kowalski & Yngström, 2009d).

FIGURE 16: OVERVIEW OF CONTRIBUTIONS
immune system inspired security framework (paper VIII); designed a methodology for applying the holistic information security model (Paper VII); and developed a security framework for software agents (Papers V & VI). The author developed an architecture for adaptive information security systems (paper XII). Then the author tested (validated) the framework using a panel validation model as reported in paper VIII. The framework was validated through external reviews of the publications. The framework was further validated by mapping to security standards. The framework was also validated by analyzing reported ICT crimes as presented in paper XI, ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security. The framework was applied to secure e-learning systems (Paper IX) and telemedicine systems (Mwakalinga, Kowalski & Yngström, 2009d). It was discovered how to minimize the gap between the capabilities of information security systems to control abuse and the needed capabilities as outlined in Figure 16. The themes and values of every paper are briefly described in the following sections.

1.2.5.1 Paper I - Authorization System in Open Networks Based on Attribute Certificates

Themes of the Paper
The theme of this paper (Mwakalinga, Rissanen & Muftic, 2003) was to investigate ways of providing authorization in open networks and for the different components of the Framework for adaptive information security systems. The aim was to learn how to separate authorization from authentication because the same authority does not always manage these two services. The theme included studying: how to identify users and assign globally recognizable roles; how to match user roles with authorization attributes like security labels; how to delegate authorization; and how to enforce privileges.

Values of the Paper
The authors designed the system and implemented the system in C language. This system is applied to provide the authorization security service for the deterrence, prevention, detection, response, recovery and other components of the Framework for adaptive information security systems. The separation of authorization from authentication was achieved by applying the attribute certificate standard. However, this separation was only achieved partially because the users must be authenticated before being authorized. Therefore, the authors needed to bind attribute certificates to the authentication certificates but different authorities can do these security services. The system is flexible and interacts with other sub systems of the Framework for adaptive information security systems. The next mini study was to study measures for securing a large system like an e-government system.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in designing the system for authorization in the framework of adaptive information security systems. This was the report on the first mini – study of the thesis. He also developed how the system could be applied in the deterrence, prevention, detection, response, and recovery systems.

1.2.5.2 Paper II - Integrated Security Administration in a Global Information System
THEME OF THE PAPER
The theme of this paper (Mwakalinga & Yngström, 2004b) was to study ways of integrating certification, authorization, registration, and smart card systems in a global security system. The theme was also to design a system for integrating and managing the components of the Framework for adaptive information security systems.

VALUES OF THE PAPER
This paper is as a spin-off of the licentiate thesis (Mwakalinga, 2003). The authors designed a global security system that integrated the certification, authorization, smart card and registration systems. This system was implemented in Java language. The system provides database services, identity management, digital certificates, attribute certificates management, smart card services, and authorization services in the holistic and information security model. The system also provides fundamental security services (confidentiality, integrity, non-repudiation).

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in designing the system, programming, and providing the integration to the framework for adaptive information security systems. The second author provided discussions and guidance for the full paper.

1.2.5.3 PAPER III- INTEGRATED SECURITY SYSTEM FOR E-GOVERNMENT BASED ON SAML STANDARD

THEME OF THE PAPER
The theme of this paper (Mwakalinga & Yngström, 2004b) was to study ways of applying the integrated security system in securing complex systems such as online e-government systems. The theme was also to study how to make the global security system scale. The theme was also to understand how to provide security services for users with low levels of e-literacy.

VALUES OF THE PAPER
The e-government security provides measures for making the Framework for adaptive information security systems flexible and scalable. The system also provides measures for integrating the framework with existing information systems that had no security when they were created. This feature is very attractive because many information systems have information security systems as add-ons. The limitation of this e-government system is that it was not adaptive to environments. This inspired the author to make a study on how to make information security system learn adapt to environments. It was also noted that the system lacked fault tolerance measures to enable it to continuously operate even if some parts of subsystems failed. The author decides to explore holistic measures of making information security systems learn to adapt to environments and culture. The next mini study was to explore the functions for making a security system learn to adapt to environments and to culture of individuals. This is described in the next section.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in developing the e-government security system, analyzing, providing security measures in e-government systems, and integrating with other information systems. The second author provided discussions and guidance for the full paper.
1.2.5.4 PAPER IV - SKETCH OF A GENERIC SECURITY FRAMEWORK BASED ON THE PARADIGMS OF SYSTEMIC-HOLISTIC APPROACH AND THE IMMUNE SYSTEM

THEME OF THE PAPER
The theme of the paper (Mwakalinga & Yngström, 2005b) was to sort in functions inspired by the immune system and Systemic-Holistic Approach that are useful for securing information systems. The work aimed at using systems holistic approach to study ways of securing information systems. Another theme of this study was to explore the factors required to be included that relate to design, development and operation of information security systems.

VALUES OF THE PAPER
This study laid foundation for the framework for adaptive information security systems. After analyzing the first three mini studies, the results indicated the need for applying a holistic approach to consider different factors that affect information security. Technical and non-technical factors that could affect information security systems were considered. The authors apply the Systemic-Holistic Approach (SHA) and the principles of the immune system to provide security to information systems. From the SHA the following principles were applied: the holistic view, analysis of technical and non-technical factors that affect information security, analysis of environments where information security system run, securely store, process, display, and transmit information. The principles that were necessary from the immune system were then identified. These principles include adaptability, autonomy, multiple level, identification, memory, diversity, distribution, and dynamic coverage. A model was created comprising of five critical sub-systems for every information security system. All inputs to the sub systems are processed in order to take out poison in the inputs by applying the Cybernetics feedback systems. The immune system cells are applied to detect viruses and foreign cells in the body. In analogy, software agents were applied to provide security services and perform different function in the security framework. The software agents must be protected before being allowed to perform different tasks in the security framework. The next section describes general methods of securing software agents for survivable systems.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in sorting out the necessary principles from the SHA, immune system, and Cybernetics for laying the foundation of a framework for adaptive information security systems. Mwakalinga created the basic model for the adaptive information security systems. Louise Yngström provided the initial ideas and directions of applying the SHA including the principles from the immune system.

1.2.5.5 PAPER V - SECURING MOBILE AGENTS FOR SURVIVABLE SYSTEMS

THEME OF THE PAPER
The theme of the paper was to study ways of securing software agents, which are used to perform different tasks in survivable systems. The theme was also to understand how to secure software agents through all the phases of agents’ creation, certification, owning, launching, traversing, and returning to the owner. The theme was also to study measures for protecting agent platforms in survivable systems that can be applied to framework for adaptive information security systems.
VALUES OF THE PAPER
In this study, the threats and attacks in different types of agent communication among the agents and agent platforms were identified. Thereafter the requirements and security services were identified to meet the identified threats. A general methodology for securing mobile agents was created. Security measures were provided for preventing an agent from attacking an agent server. Security measures were also provided for preventing an agent server from attacking an agent and an agent from attacking another agent. Security measures were also provided to prevent an agent server from attacking another agent server. Communications between agents and agent owners and agent servers were protected. Integrity of agents and data is provided through signatures. The next section describes a framework for securing software agents that are specific to the framework for adaptive information security systems.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in developing the methodology for securing mobile agents for survivable systems. Mwakalinga also provided security measuring for protecting agents, agent server, agent communication, and tracing. The second author provided discussions and guidance for the full paper.

1.2.5.6 PAPER VI - FRAMEWORK FOR SECURING MOBILE SOFTWARE AGENTS

THEME OF THE PAPER
The theme of this work (Mwakalinga & Yngström, 2006b) was to study ways of using mobile software agents to deter attackers, protect information systems, detect intrusions, respond to the intrusions and attacks, and to produce recovery services to systems after attacks for the framework for adaptive information security systems. The theme was also to study measures for making the framework for adaptive information security systems adaptive to environments using mobile software agents.

VALUES OF THE PAPER
In this work, specific measures for securing mobile software agents for the framework for adaptive information security systems were provided. Security measures were also provided to protect communication between different components in the security framework. Methods were studied for providing specific software agents for the deterrence, protection, detection, response, and recovery sub-systems. The agents provide authentication, confidentiality, integrity, non-repudiation, and authorization security services. The training of agents during their creation based on the immune negative selection and clonally selection algorithms, genetic algorithms, and neural networks. The agents make decision based on the fuzzy logic. A prototype was created but it reflects only part of the framework that deals with maintenance. The next mini-study was to study how to consider environments and culture in developing information security systems.

Jeffy Mwakalinga contributed in all sections of the paper and gave the main contribution in designing the framework for securing mobile software agents. Mwakalinga provided specific security measures for the deterrence, prevention, detection, response, and recovery systems. The second author provided discussions and guidance for the full paper.

1.2.5.7 PAPER VII - METHODOLOGY FOR CONSIDERING ENVIRONMENTS AND CULTURE IN DEVELOPING INFORMATION SECURITY SYSTEMS
The theme of this paper (Mwakalinga, Kowalski & Yngström, 2009c) was to study how to create a methodology for considering environments where information systems operate. This included how to involve people and consider what cultures aspects affect their decisions. The study focused on how to apply the framework for adaptive information security and how to better understand who defined the boundary between a system and its environment.

The authors established a methodology for considering environments and people in the development of systems. Factors that set the boundary between an information system and an environment were discussed. Information system designers and developers and enemies of IT (Kowalski, 1994) tended to set the boundary between a system and an environment for users without asking their cultural values. Users of information systems do not own information systems because they cannot control them (Kowalski, 1994). One cannot own something if one cannot defend it (Kowalski, 1994). Cultural values of users and geographical factors should set the boundary between a system and its environment. An environment of an information system was outside of the control of an information security system. There are hostile and friendly environments and different strategies should be used to process inputs from hostile and friendly environments. The next mini-study was to understand the effect of economics perspective of information security and specifically to explore telecommunication markets.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in developing the methodology for considering environments and people in the development of systems. Mwakalinga studied how different cultural preferences and behaviors could create vulnerabilities in information security systems. The second author provided the framework to describe cultures from a security perspective and the third author provided discussions and guidance for the full paper.

1.2.5.8. Paper VIII - A HOLISTIC AND IMMUNE SYSTEM INSPIRED SECURITY FRAMEWORK

The theme of this paper (Mwakalinga, Yngström & Kowalski, 2009a) was to explore the adaption systems that are most appropriate for application to information systems security. The theme was also to study measures for analyzing exploring cultural, traditional, ethics, and other social issues essential for inclusion in the framework for adaptive information security systems. The theme was also to find measures for strengthening weak links that are created by culture and other social issues. Another theme was to validate the Framework for adaptive information security systems. Another theme was to study how the security framework could handle the dynamic changes from environments.

The paper addresses adaptability issues in information security systems. The adaptability system was developed for providing measures to make the system and its subsystems learn to adapt to environments. It consists of the environmental analyzer, people’s value analyzer and threat analyzer. The communication of different components in the framework for adaptive information security systems was designed. The security framework was validated through interviews, questionnaires, and criteria from different international security standards. The next
mini-study was about how to apply the Framework for adaptive information security systems to secure large systems like an e-learning system.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in developing the holistic and immune system inspired security framework. Mwakalinga studied how to provide adaptability measurers to environments and culture of people. The second and third authors provided discussions and guidance for the full paper.

1.2.5.9. PAPER IX - SECURING E-LEARNING SYSTEM USING A HOLISTIC AND IMMUNE SECURITY FRAMEWORK

THEME OF THE PAPER
The theme of this paper (Mwakalinga, Kowalski & Yngström, 2009b) was to apply the framework for adaptive information security systems to secure a large system like an e-learning system. The theme was also to understand the challenges when applying the Framework for adaptive information security systems in real environments.

VALUES OF THE PAPER
The paper examines the social and technical security measures for helping an e-learning system learn to adapt to environments and to culture of e-learning users. Multiple security service schemes are provided to accommodate users with different computer literacy levels and cultural backgrounds. The mobile agents provide security services in an e-learning system. Methods were studied on provision of security measures in the most common scenarios in e-learning: teacher centered, evaluation centered, and collaboration centered. The next step in the thinking process is reflection.

Jeffy Mwakalinga contributed in all sections of the paper. He gave the main contribution in designing the securing the e-learning system based on the holistic and immune security framework. Mwakalinga analyzed e-learning system architectures and how to integrate with the immune security framework. Mwakalinga studied how to provide adaptive security measures for e-learning systems. The second and third authors provided discussions and guidance for the full paper.

1.2.5.10. PAPER X- MODELING THE ENEMIES OF AN IT SECURITY SYSTEM - A SOCIO-TECHNICAL SYSTEM SECURITY MODEL

THEME OF THE PAPER
The theme of the paper was to study how to model the enemy of an IT system. In order to defend from the attacks and intrusions of the enemy of IT, it was necessary to understand the tools and methods that an enemy uses to attack information systems.

VALUES OF THE PAPER
The paper proposes a way of modeling an enemy of IT. The enemy of IT uses scans a large number of computers to find out the tools and methods that a defender is applying to defend information systems. The enemy of IT analyses how an information system deters attacks, prevents attacks and intrusions, and detects intrusions and attacks. The enemy tries to analyze how the defender responds to the attacks and intrusions. The aim of the enemy is to understand the different vulnerabilities that could be exploited. The enemy of IT appears to use the Socio-technical security model to attack an information system at the living, abstract and concrete
layers. The enemy of IT could find out that the deterrence subsystem is the weakest and attack the information system through the deterrence subsystem. As a defender, this model could help to analyze the subsystem or the point in the information system that has weakness and strengthen it. A security manager could use this model to determine the potential victims in a company by analyzing all the computers and information systems in a corporation. The results of the analysis should indicate in which systems to add security measures.

Jeffy Mwakalinga contributed in all sections of the paper. Mwakalinga gave the main contribution in proposing a methodology for modeling an enemy of IT. Mwakalinga analyzed different tools and methods that hackers use when attacking information systems. Mwakalinga studied how the hackers were organized. Stewart Kowalski provided the original idea and guidance how to do social-technical modeling.


Theme of the Paper
The theme of the paper was to validate the adaptive framework for information security systems to reality. The aim was also understand how to detect potential IT victims so that we could provide security measures.

Values of the Paper
The paper examines 41 reported ICT crimes. The crimes occurred because of the absence of deterrence socio-technical measures. In addition, the prevention and detection measures were weak which enabled the attacks to take place. In addition, response security measures were lacking or weak, which enabled the ICT criminals to succeed. We recommended that every information system should have the deterrence, prevention, detection, response, and recovery security measures. We also recommend that the security measures should include both social and technical security measures. This is because the hackers use both social and technical measures in attacking or in gathering information before the attacks. The hackers use social engineering to gather information. We also recommended that security administrators to detect potential victims by checking whether the deterrence, prevention, detection, response, and recovery security measures are present and their strength. These functions could act as crime prevention features in ICT products and systems.

Jeffy Mwakalinga contributed in all sections of the paper. He gave the main contribution in analyzing the reported ICT crimes and performing an autopsy of these crimes. He also gave recommendations on how information systems should provide crime prevention measures. The second author provided the original idea, discussions, and guidance for the full paper.

1.2.5.12 Paper XII – Architecture for Adaptive Information Security Systems as Applied to Social Networks

Theme of the Paper
The theme of this paper was to develop an architecture for adaptive information security systems for implementation. The theme was also to study how to apply the architecture to secure social networks.
VALUES OF THE PAPER
The paper examines the requirements for security architectures and the development process of security architectures. The security architecture is to be developed by a team. The development process includes planning, designing, implementing, operating, and maintaining it. The authors analyzed two related architectures one for computer systems and the other for mobile networks. The architecture was applied to secure social networks.

Jeffy Mwakalinga contributed in all sections of the paper. He gave the main contribution in developing the architecture for adaptive information security systems. He then studied how to apply the architecture in securing social networks. The second author provided discussions and guidance for the full paper.

1.2.6 REFLECTION
In this section, the author reflects on the relationship of the expected end product, the research problem, and the contributions as outlined in Figure 17. The expected end-product was a framework for adaptive information security systems. The research problem was how to minimize the gap between the capabilities of information security systems to control abuse and the needed capabilities. The research problem was divided into five research questions. The first research question required identification of the critical systems for adaptive information security systems in analogy to Miller’s (1978) 19 critical systems must be present in every living system for it to survive in different environments. The identified critical systems are the value-based chain systems. The value-based chain systems include the deterrence, prevention, detection, response, and recovery as reported in the paper IV, *Sketch of a generic security framework based on the paradigms of Systemic-Holistic Approach and the immune system* (Mwakalinga & Yngström, 2005b). The second research question required investigation of the adaptation systems for making information security systems adapt to environmental and cultural changes. The first identified adaptation system was the immune system whose principles provide internal adaptation measures in the components of the security framework as described in the paper VIII, *A holistic and immune system inspired security framework* (Mwakalinga, Yngström & Kowalski, 2009a). The immune system applies cells to defend the body. In the framework for adaptive information security systems software agents are applied to provide security services and perform different tasks. The software agents have to be secured before providing security services. This is reported in the paper V, *Securing mobile agents for survivable systems* (Mwakalinga & Yngström, 2005a) and in paper VI, *Framework for security mobile software agents* (Mwakalinga & Yngström, 2006b).

The second adaptation system was the Viable system model (Beer, 1984), which was applied to provide measures for adapting to the environments as described in the paper VII, *Methodology for considering environments and culture in developing information security systems* (Mwakalinga, Kowalski & Yngström, 2009c). The third adaption system was the Cybernetic structural model (Herring, 2002), which was applied to provide external adaptation measures as described in the paper VIII, *A holistic and immune system inspired security framework* (Mwakalinga, Yngström & Kowalski, 2009a).
The expected end product: a framework for adaptive information security systems

The research problem is how to minimize the gap between the capabilities of information systems and the capabilities of information security system that control them

First research question: What are the critical systems for adaptive information security systems?

Critical systems are deterrence, prevention, detection, response and recovery – paper IV

Second research question: What adaptation systems are needed to making information security systems adapt to environmental and cultural changes?

Adaptation systems are the immune system, viable system model and Cybernetic structural model – Paper VIII
Methodology for considering environments and culture in developing information security systems - paper VII
Securing mobile agents for survivable systems - papers V and VI

Third research question: How can identity management be provided in adaptive information security systems?

Integrated system for security administration and an authorization system – papers I and II

Fourth research question: What models are IT adversaries using to attack information systems and how can these be circumvented?

The socio-technical security model was developed to study the models that are used by an IT adversary – paper X
The economical perspective of information security systems (Kowalski, Nohlberg & Mwakalinga, 2008)

The fifth research question: How can these results from the investigation be applied to protect information systems?

Application to Security for e-government system – paper III
Application to security for an e-learning system- paper IX
Application to security for a telemedicine system (Mwakalinga, Kowalski & Yngström, 2009d).
Application to secure social networks - paper XII

FIGURE 17: REFLECTION BETWEEN THE END PRODUCT, RESEARCH PROBLEMS, AND QUESTIONS
Thereafter a study was made to understand how to provide adaption measures in information security systems for adapting to environments and culture as reported in the paper VII, *Methodology for considering environments and culture in developing information security systems* (Mwakalinga, Kowalski & Yngström, 2009c). The third research question required determining ways to provide identity management in information security systems. The first study was how to provide authorization in the framework as reported in the paper I, *Authorization system in open networks based on attributes certificates* (Mwakalinga, Rissanen & Muftic, 2003). Then another study focused on how to manage identities and provide security services as reported in the paper II, *Integrated security administration in a global information system* (Mwakalinga & Yngström, 2004a).

The fourth research question required analysis of the models that an IT adversary is using to attack information systems. In order to understand how to defend information systems it is necessary to understand the methods and tools that an enemy is applying to attack information systems. The socio-technical economic model was developed to study the models that are used by an IT adversary. The adversary of IT analyzes how economical it is to attack an information system by checking how an information system defends itself. This was reported in the paper VIII, *A holistic and immune system inspired security framework* (Mwakalinga, Yngström & Kowalski, 2009a) and paper XI, *Modeling the Enemies of an IT Security System - A Socio-Technical System Security Model* (Kowalski and Mwakalinga, 2011). The socio-technical economic model was also applied to understand the economical perspective of information security system (Kowalski, Nohlberg & Mwakalinga, 2008). The model is also applied for studying the tools and methods that an adversary of IT uses to attack information security systems.

The fifth research question required analysis and application of the results from the investigation to protect information systems. Studies were made on how to apply the results of the investigation. The first application was on security for an e-government as reported in the paper III, *integrated security system for E-government based on SAML standard* (Mwakalinga & Yngström, 2004b). The second application of the results was on security for an e-learning system as reported in the paper IX, *Securing e-learning system using a holistic and immune security framework* (Mwakalinga, Yngström & Kowalski, 2009b). The third application was on security for a telemedicine system (Mwakalinga, Kowalski & Yngström, 2009d).

**1.2.7 RESULTS - A FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS**

The next step in the thinking process is the results, which is a Framework for adaptive information security systems as displayed in Figure 18.
Have we solved the problem?
The research problem was stated in section 1.2 was stated as how to minimize the gap between the capabilities of information security systems to control abuse and the needed capabilities.
FIGURE 19: APPLYING THE VALUE-BASED CHAIN FUNCTIONS FOR SOCIO-TECHNICAL CONTROLS

The gap was filled by applying the value-based chain for socio-technical controls as outlined in Figure 19 (adopted from Kowalski, 1994 p 57). The adaptive framework for information security systems was developed and it provides adaptive social and technical security measures to environments and culture in the framework. These socio-technical measures are provided in the critical sub-systems, which include the deterrence, prevention, detection response, and recovery.

1.3 LIMITATIONS

This framework for adaptive information security systems is behaving as a ‘Cybernetic living’ (Yngström, 1996) which implies that it takes care of dynamic changes in open system environments and changes in different sub systems. However, the security model cannot take care of indefinite large changes, like occurrences of fire and earthquakes where systems operate, in the open environments. The behavior of the framework for adaptive information security systems when indefinite changes occur in open environments is unpredictable.
Implementation is not part of this work. Some parts of the framework for adaptive information security systems may not be implementable by today’s technology. The surveys were conducted to the information security experts and master students who had good knowledge of the holistic view and system thinking theory. Therefore, in validating the security framework the author applied the expert panel and mapping of the framework against the criteria of existing security standards, which takes as axiomatic that these standards are valid which might not be the case. The publications of the mini studies do follow the research plan chronologically because of early mistakes in planning the research. In analyzing environments, the author did not cover infrastructural environments like electric power (failure, over-voltage, noise interference), heating, humidity, cooling, earthquakes, fire, floods, and so on. The system depends on the effectiveness of algorithms that are used in the sub-systems for mobile agents.

1.4 Organization of Chapters

CHAPTER 2: VALIDATION OF THE FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS

This chapter presents three approaches to validate the framework for adaptive information security systems. The first approach is a theoretical analysis where the framework is mapped against a number of existing security standards. The second validation approach applies the panel validation method proposed by Beecham (Beecham, et al, 2004). The third validation approach was achieved by analyzing ICT crime cases using the framework.

2.1 VALIDATION APPROACH 1: THEORETICAL ANALYSIS

This section presents the results of mapping the framework for adaptive information security systems against the criteria from existing security standards. Security standards should to a large extent reflect or react to reality of information security systems because they were established to map the reality as shown in Figure 20.

FIGURE 20: VALIDATION APPROACH 1: MAPPING OF THE SECURITY FRAMEWORK TO SECURITY STANDARDS
The aim of the theoretical analysis was to assess how closely the framework aligns with the security standards. The author mapped the framework to the Common Criteria (Common Criteria, 2006) and the ISO 27001 (ISO27001, 2006) standards. In order to cover the security problem range of the framework, which is both Information Technology security and Information System security, two of the most widely used and representative security standards were selected. For the IT area the Common Criteria was selected and for the IS area the ISO 27001 was selected. From the Common Criteria, the security functional requirements were used. These include Security audit, Communication, Cryptographic support, User data protection, Identification and Authentication, Security Management, Privacy, Resource utilization, Target of Evaluation (TOE) access, Trusted path/channels, Protection of target of evaluation of security functions (TSF). The ISO 27001 consists of the following requirements: Establish Information Security Management Systems (ISMS), Implement ISMS, Operate ISMS, Monitor ISMS, Review ISMS, Maintain ISMS, Improve ISMS, Management responsibility, Internal ISMS audits, and Management review as shown in Table 2. The first column indicates the criterion.

**TABLE 2: MAPPING THIS FRAMEWORK AGAINST COMMON CRITERIA AND ISO 27001**

<table>
<thead>
<tr>
<th>Criterion</th>
<th>Presence in security Framework</th>
<th>Strength of the criterion</th>
<th>Social security measures</th>
<th>Technical security measures</th>
<th>Multiple mechanisms provision</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security audit</td>
<td>1</td>
<td>3</td>
<td>28%</td>
<td>72%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Communication</td>
<td>1</td>
<td>4</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Cryptographic support</td>
<td>1</td>
<td>4</td>
<td>45%</td>
<td>55%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>User data protection</td>
<td>1</td>
<td>4</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>ID &amp; Authentication</td>
<td>1</td>
<td>4</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Security Management</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Privacy</td>
<td>1</td>
<td>3</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Resource utilization</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>TOE access</td>
<td>0.5</td>
<td>2</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Trusted path</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Protection of TSF</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>CC</td>
</tr>
<tr>
<td>Establish ISMS</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Implement ISMS</td>
<td>1</td>
<td>2</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Operate ISMS</td>
<td>1</td>
<td>4</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Monitor ISMS</td>
<td>1</td>
<td>4</td>
<td>28%</td>
<td>72%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Review ISMS</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Maintain ISMS</td>
<td>1</td>
<td>3</td>
<td>30%</td>
<td>70%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Improve ISMS</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>70%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Management Resp.</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Internal ISMS audits</td>
<td>1</td>
<td>4</td>
<td>28%</td>
<td>72%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
<tr>
<td>Management review</td>
<td>1</td>
<td>3</td>
<td>31%</td>
<td>69%</td>
<td>1</td>
<td>ISO27001</td>
</tr>
</tbody>
</table>

The second column indicates whether the criterion is present or absent in the framework. If the criterion is present in the framework then the value is 1, if the criterion is absent in the framework then the value is 0. The third column indicates the strength of the criterion, classified as maximum strength, medium strength or minimum strength. For example,
authentication has maximum strength if there is mutual authentication, which implies that a
server authenticates a client and the client authenticates the server. In addition, they are both
using strong authentication measures for example using digital certificates. If the server and the
client use mutual authentication but they were not using strong authentication measures then
the strength would be value 3. If authentication is one way that is only the server authenticates
the client using a strong authentication measure then the strength is value 2. If they use weak
authentication measures like passwords then the strength is value 1. Value 4 indicates
maximum strength, value 3 indicates medium, value 2 indicates minimum strength, value 1
indicates poor strength, and value 0 indicates no strength. The fourth column indicates the
percentage of the social security measures in the socio-technical security measures that can
provide the criterion. As described before, social security measures could be ethical, legal,
political, managerial, and operational (Kowalski, 1994). If the criterion can be provided by
social security measures the value is 1 otherwise the value is 0. The fifth column indicates the
percentage of the technical security measures in the socio-technical security measures that can
provide the criterion.

A desktop survey was made to understand how much social and technical security measures
users would allocate to the deterrence, prevention, detection, response, and recovery functions.
The idea of the survey was to ask respondents how much percentage out of 100 % would they
allocate on social, and how much out of 100 % would they allocate on technical security
measures for each function. The average results are shown in Figure 21.

![Technical and social security measures](image)

**FIGURE 21: AVERAGE OF RESULTS FROM THE SURVEY ON TECHNICAL AND SOCIAL
SECURITY MEASURES ALLOCATION ON THE VALUE-BASED CHAIN FUNCTIONS (N=60)**

The results show that 55 % of the total security measures would be allocated to technical
security measures while 45 % would be allocated to social security measures in the deterrence
function. 70 % of the security measures for prevention function could be allocated to the
technical security measures while 30 % could be allocated to social security measures. For the
detection function, 72 % could be allocated to the technical security measures while 28% could
be allocated to the social security measures. For the response function, 57% could be allocated for providing technical security measures while 43% could be allocated to providing social security measures. 69% of the security measures for recovery function could be allocated for providing technical security measures while 31% could be allocated for providing social security measures. The criteria are assigned to the categories of deterrence, prevention, detection, response, and recovery. For example, identification and authentication are assigned to the prevention category, which implies that 31% of the security measures could be used to provide the criterion while 69% the security measures could be used to provide technical security measures. Awareness and training are assigned to the deterrence category, which implies that 45% of security measures could be social while 55% of the security measures could be technical security measures. These criteria are used in columns for social security measures and technical security measures in Table 2.

The sixth column indicates whether the criterion could be provided by multiple security mechanisms. If the criterion could be provided using multiple security mechanisms then the value is 1 otherwise the value is 0. The last column outlines the source of the standard, the component of security framework that provides the criterion. The author starts by mapping the framework against the criteria from the Common criteria in the form of security functional requirements (Common criteria, 2006). There are eleven classes of security functional requirements in Common Criteria as described in details in appendix F. The mapping of the framework for adaptive information security systems against security standards indicate all functions are present except the Target of access as shown in the first column of Table 2. Therefore, to some extent it could be said that the framework has the necessary functionality. To decide, however, if the framework has both the necessary and sufficient functionality we will use the other two validations approaches.

2.2 Validation Approach 2: Panel Validation Model

The panel validation model was applied as the second approach where the author followed the steps proposed by Beecham (Beecham et al, 2004).

2.2.1. Objective, Chosen Criteria, and Evaluation Processes

The objective of this holistic investigation was to explore, understand, explain, design, test, and discover how to minimize the gap between the ability of information systems to adapt to environments and culture changes and the information security systems ability to adapt to these same changes. We validated the framework for adaptive information security systems by interviewing information security experts. These experts understand the reality of information security systems and therefore we asked them how valuable the security framework would be in the organizations as shown in Figure 22.
The second process was to list the success criteria identified during the initial stages of the model development. These criteria are outlined in Table 3. The third process was to explore alternative methods for testing how the criteria are reflected in the model. One method to test the security criteria would be to implement them in an organization and then make an inquiry on how the security framework meets the identified success criteria. The success of these criteria depends on the information security knowledge that employees have and the results will not be the same as of the security experts.
TABLE 3: IDENTIFIED SUCCESS CRITERIA

<table>
<thead>
<tr>
<th>Success Criterion</th>
<th>Purpose</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usefulness</td>
<td>To understand how useful is the framework for adaptive information security system in organizations</td>
<td>System theory, Systemic-holistic approach, Socio-technical system and immune system</td>
</tr>
<tr>
<td>Adaptable to environments</td>
<td>To provide measures for making information security systems learn to adapt to environments</td>
<td>System theory, Systemic-holistic approach, Socio-technical system and immune system</td>
</tr>
<tr>
<td>Adaptable to culture of users</td>
<td>To provide measures for making information security systems learn to adapt to culture of users</td>
<td>System theory, Systemic-holistic approach, Socio-technical system and immune system</td>
</tr>
<tr>
<td>Strength to resist attacks</td>
<td>The security framework should have the ability to resist attacks</td>
<td>Socio-technical system and immune system</td>
</tr>
</tbody>
</table>

2.2.2 DESIGN OF VALIDATION INSTRUMENT
The next process was to design a validation instrument to test the success criteria. The author designed the questionnaire and validation instrument. The table 4 outlines the success criteria, the questions, and the components of the security framework.

2.2.3 SELECTING PANEL EXPERTS
The next process was to select the security experts. The author sent requests to many information security experts who had good knowledge of the fundamental principles in the thesis but only six experts had time to participate. Six information security experts in industry and academia were interviewed on the usefulness and applicability of the security framework. All experts were academics or research students with some experiences from industry. The experts were also selected based on their knowledge and experiences in the information security and their holistic view of this area.
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Questions</th>
<th>Components of the Framework</th>
</tr>
</thead>
</table>
| Usefulness of the security framework in organizations | Question 1  
Can this security framework and its subsystems be applied / useful in your organization? | Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework      |
| Degree of usefulness of the framework in organizations | Question 2  
How useful would this holistic and immune security framework and the subsystems can be to your organization? | Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework      |
| Adaptability of framework to environments           | Question 3  
How satisfied are you with the adaptability features of this security framework to environments? | Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework      |
| Adaptability of framework to culture               | Question 4  
How satisfied are you with the adaptability features of this security framework to the values of the people using the information security systems? | Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework      |
| Strength of the framework to resist attacks         | Question 5  
How satisfied are you with strength of the framework to resist attacks. | Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework      |
The results of this survey are also found in appendix D.

2.2.4 Present results of the validation
The author presents here the results of validation from the expert panel.

2.2.4.1 Usefulness and applicability of the holistic and immune security framework
Table 5 presents the results.

**TABLE 5: CAN THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK AND ITS SUBSYSTEMS BE APPLIED / IMPLEMENTED / USEFUL IN YOUR ORGANIZATION? (N=6)**

<table>
<thead>
<tr>
<th>Can it be implemented?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NOT SURE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Need more information</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

**TABLE 6: HOW USEFUL WOULD THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK AND ITS SUBSYSTEMS BE TO YOUR ORGANIZATION? (N=6)**

<table>
<thead>
<tr>
<th>Degree of usefulness</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>75%</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>50%</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25%</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

The results are shown in Table 6.

2.2.4.2 Adaptability features of the security framework to environments
The respondents were satisfied with the adaptability features outlined in the Table 7.

**TABLE 7: HOW SATISFIED ARE YOU WITH THE ADAPTABILITY PRINCIPLES OF THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK TO ENVIRONMENTS? (N=6)**

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Somewhat satisfied</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Not too satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Not at all satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2.4.3 ADAPTABILITY PRINCIPLES OF THE SECURITY FRAMEWORK TO VALUES OF USERS

Table 8 outlines the results of adaptability survey.

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Somewhat satisfied</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Not too satisfied</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at all satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The author also discussed with two of the respondents about the strength of the framework to resist attacks, specifically in relation to the degree of preventing the enemy from attacking the framework. The two respondents expressed the opinion that the deterrence, detection subsystems, and the whole framework security framework could be successful in preventing the enemy from attacking information by 75%. One respondent commented that the prevention subsystem could prevent the enemy from attacking the information system by 75%.

2.2.5 RELATION OF RESULTS TO SUCCESS CRITERIA

The next process in the panel validation model is the relation of the results to other success criteria in order to gain an impression of strengths and weaknesses. The next section presents the comments and discussions with the respondents. The fourth information security expert commented, “Based on the information I have seen, this seems to be one of the few frameworks that take cultural behavior as an integral part of the design context. Since human behavior is one of the main sources of computer insecurity, I think that integrating this into the security framework should lead to much better results than just designing security systems from a strictly technical perspective.” The expert commented that security of agents needed to be addressed. The software agents need to be secured before being given the ability to defend others and trained before being allowed to protect the information systems. This is reported in the papers V and VI, *Securing Mobile Agents for Survivable Systems* (Mwakalinga & Yngström, 2005a), and *Framework for Securing Mobile Software Agents* (Mwakalinga & Yngström, 2006b).

It was also recommended to create a selling package process for the framework in a form of guidelines of how to work with the framework. This would help the organizations to have a good starting point when applying the framework. In this regard, the author developed guidelines for applying the security framework as reported in the paper VII, *Methodology for considering environments and people in developing systems and application of holistic and immune security framework* (Mwakalinga, Kowalski & Yngström, 2009c). The fourth information security expert pointed out that, an adaptive framework like this would be very useful in a university environment where changes happen rapidly. The first information security expert commented that assuming that all the people’s values are known then the adaptability measurers would be effective. As for the detection subsystem, people’s behaviors
are dynamic and it is not easy to predict people’s behavior. The first expert also added that theoretically, the adaptability principles to environments were sound but it was hard to evaluate effectively the principles until applied in their organizations. Theoretically, adaptability principles to the culture, traditions, ethics, and other social issues of users are good but it is hard to say exactly how effective they would be when applied in the companies. The fourth respondent expressed the opinion that adaptability was the main quality and characteristic of the whole framework. The second respondent commented that the framework could be useful in an organization to structure the security work. It is a good framework for technical organizations. The expert added that there were many technical solutions but there was no framework that could make them fit together which would make this framework useful in fitting the different technical solutions together. The framework could be applied as a benchmark to see whether all the information security areas are covered in an organization such as control, centralized login, etc. The security framework could be useful for small and large organizations.

The first information security experts suggested the following architecture for implementation using software mobile agents as shown in Figure 23.

The architecture has the following components. The identity management server (IDMS) manages identities of the security framework. The certification Authority (CA) server would be used for managing digital certificates of the security framework. The Policy Decision Point (PDP) would be applied for making decisions about authorizations in the security framework. The Universal Description Discovery and Integration (UDDI) server would be used for creating software mobile agents and registering their services using the Service-Oriented Architecture (SOA, 2009). The Extensible Access Control Mark-up Language (XACML) would provide access control services in the security framework (SOA, 2009). The Magnet platform was an agent platform where one could enquire available services at the UDDI server. If the agent providing the required service were available at the UDDI the server would launch the agent from agents’ repository and the magnet platform. If the required agent were not available at the UDDI, the server would notify the magnet manager to create an agent. When probes appear, we need to detect and respond by deterrence. When attacks come, we need to
detect them. When intrusions come, we need to detect them and protect/prevent them. When penetration occurs, we need to detect them and recover from damages. We validated the framework for adaptive information security systems with security experts. In this case, students acted future experts. Surveys were made on master international master students in information security that had knowledge of holistic approach, system theory and social technical systems, which are the fundamental concepts in this thesis. The first group of 11 master students was given a brief description of the security framework and then they answered the questionnaire. The second group had 60 students, the third had 27 students, and the fourth had 37 students. The following section presents the result of this survey. The results are briefly described in the following sections but the details are found in appendix D.

2.3 VALIDATION APPROACH 3: ANALYSIS OF REPORTED ICT CRIME CASES

The adaptive framework for information security systems was further validated towards reality of information security systems by doing an autopsy of 41 ICT crime cases as outline in Figure 24.

![Diagram of Validation Approach 3: Analysis of Reported ICT Crimes]

FIGURE 24: VALIDATION APPROACH 3: ANALYSIS OF REPORTED ICT CRIMES
An analysis was made of 41 computer crime cases as described in the paper XI, *ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security* (Mwakalinga & Kowalski, 2011a). These computer crime cases were analyzed (US Justice, 2010) to study the cause of compromised systems in relation to the deterrence, prevention, detection, response, and recovery measures. Out of 41 cases, no system that was attacked had strong deterrence measures to scare away attackers. Seven systems had weak deterrence measures, which could not scare away attackers. 34 systems had no deterrence measures. When it came to prevention measures, 40 systems had weak prevention measures, which could not prevent attackers. One system had no prevention measures at all. 31 systems had no response measures at all, while 10 systems had weak response measures. As to the recovery systems, 34 systems had no recovery measures while 7 had weak recovery measures as outlined in Table 9.

**TABLE 9: VALUE-BASED CHAIN FUNCTIONS IN THE REPORTED ICT CRIME CASES**

<table>
<thead>
<tr>
<th></th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Weak</td>
<td>7</td>
<td>40</td>
<td>37</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>None</td>
<td>34</td>
<td>1</td>
<td>4</td>
<td>30</td>
<td>34</td>
</tr>
</tbody>
</table>

18 of the cases had weak confidentiality measures. In 31 of the cases authentication security service was not strong. In 32 cases, access control was not strong enough. 23 cases had breaches in integrity security service. Nine cases had breaches in privacy security services. Criminals appear to use both social, like social engineering, and technical measures to attack information systems. Criminals used social attacking measures in 26.8% of the crimes. In 31.7% of the crime cases criminals used both social and technical attacking measures. The criminals used technical attacking measures in 41.5% of the crime cases. Details are described in the paper XI, *ICT Crime Cases Autopsy: Using the Adaptive Information Security Systems Model to Improve ICT Security* (Mwakalinga & Kowalski, 2011a) and in the appendix G. The Socio-Technical model was applied to analyze the methods and tools that the hackers applied in attacking the information systems. The structure or organization of criminals is presented in paper XI. The methods that criminals used in the 41 crime cases included stealing credit cards and identities, installing Trojan horses, reconfiguring networks, redirecting traffic, deleting and modifying records. Other methods include impersonation, stealing program codes, diverting salaries, distributed denial of service, SQL injection, stealing secrets and formulas from companies and Web defacing. The method of stealing identities and credit card information and selling the information was applied in ten crime cases. The method of stealing secrets from companies like trade secrets, formulas, and new product designs was used in five crime cases. The method of distributed denial of service was applied in four crimes cases. The SQL injection method used in two of the crime cases.
Web defacing method was used by criminals in two crime cases. Another method used in one of the crime cases was selling the botnet army to other criminals using the state web sites. As regards machines, it is not easy to understand the exact machines that they used to conduct their criminal activities. However, it appears that they were using powerful computers and fast ubiquitous internet access. The same goes to culture of the criminals they tend to come from different cultural backgrounds.

The ICT crimes occurred because of the absence of deterrence socio-technical measures. In addition, the prevention and detection measures were weak which enabled the attacks to take place. In addition, response security measures were lacking or weak, which enabled the ICT criminals to succeed. The author recommends that every information security system should have the deterrence, prevention, detection, response, and recovery security measures. The author further recommends that the security measures should include both social and technical security measures. This is because the hackers use both social and technical measures in attacking or in gathering information before the attacks. The hackers use social engineering to gather information. We also recommend especially to security administrators to detect potential victims by checking whether the deterrence, prevention, detection, response, and recovery security measures are presence and their strength. These functions could act as crime prevention features in ICT products and systems.

2.4 SUMMARY OF VALIDATION

The results show that to some extent that the framework has the necessary functions. The results show also that the framework provides the adaptive security measures to environments and culture of users. The results show also that ICT crimes occur because of lack of necessary deterrence measures and weak prevention, detection and response security measures.

Could the results of this thesis be generalized? A research finding can be generalized if the results of an investigation can be extended. It is normally results obtained under quantitative settings that researchers could generalize (Patton, 2002). The research methodology applied in this research was holistic research process and qualitative. Whether to generalize the results is an open issue at this stage. The author believes that more studies should be conducted before generalizing the results. Could the results of this investigation be transferable? Results of an investigation can be transferable if they are detailed enough to be carried to other settings (Patton, 2002). We need to conduct more studies to make it to be transferable because it is a framework and by nature a framework does not include details. However, the validation process conducted indicates that even though implementation details and specifications were not spelled out, the analyses, descriptions and discussions with the information security experts resulted in positive assessments of future realizations of the framework including also a suggested architecture of implementation.
CHAPTER 3 CONTRIBUTIONS AND CONCLUSIONS

3.1 CONTRIBUTIONS

3.1.1 FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS

The framework is based on the five critical systems that should be present in every adaptive information security system. This was adopted from Miller’s theory of nineteen critical systems needed to be present in every living system. The five critical systems of the adaptive framework are the security value-based chain functions called deterrence, prevention, detection, response, and recovery. The critical systems allow the framework to defend information security systems at five layers. In the first layer, the framework deters attacks and intrusions using the deterrence system. If a system fails to deter attacks and intrusions, it will use the second layer, prevention system, to prevent the attacks. If the information security system fails to deter and prevent attacks and intrusions, it will use the third layer, detection system, to detect the intrusions and attacks. If the information security system fails to deter, prevent, and detect the attacks and intrusions it will use the fourth layer, response system, to respond to the intrusions and attacks. If the information system fails to deter, prevent, detect, and respond then it will use the fifth layer, the recovery function, to recover from the intrusions and attacks. The framework for adaptive information security systems provide the adaptability measures using the principles of the immune system, the Viable System Model, the Cybernetics structural model and Cybernetic feedback mechanisms. The author also suggested an architecture for implementing the framework for adaptive information systems security.

3.1.2 METHOD OF CONSIDERING CULTURE, TRADITIONS, ETHICS, AND OTHER SOCIAL ISSUES OF USERS WHEN DEVELOPING INFORMATION SECURITY SYSTEMS

A methodology for considering culture and other social issues when developing information security systems was developed. The first step of the methodology is to assess the effects of culture and other social issues on users of the security system. An informal cultural model (Mwakalinga & Yngström, 2005a) is applied for predicting the behavior and preferences of users in different cultures, which may create vulnerabilities in information security systems. Therefore, the Socio-Technical model (Kowalski, 1994) is applied to analyze the weak security links and vulnerabilities created by cultural behavior and preferences in the framework for adaptive information security systems. The next step is to take care of these vulnerabilities by applying social and technical security measures. The Security by Consensus model (Kowalski, 1994) is applied to remove or handle the vulnerabilities. For instance, a study by (Chaula, 2006), found that users of culture with low uncertainty avoidance tend to lack holistic approaches to security. This implies that they lack security in depth measures and attention to details. In the framework for adaptive information security systems, a security policy would specify the social and technical security measures to remove these vulnerabilities. Another weakness found by Chaula (2006), is that users of culture with low uncertainty avoidance tend to have poor risk assessment, poor assumptions about motivation, opportunity and methods; they tend to ignore to classify information, and use metrics poorly. In the framework for adaptive information security systems, procedures and security policies would be created so that there should be good risk assessment and information classification. A further weakness with users from cultures with low future orientation is that it leads to ineffective contingency planning. This affects continuity plans and preparation if an attack or a disaster was to occur.
The framework for adaptive information security systems would put effective contingency and continuity plans through the security policies, procedures, and designs. Further, users of cultures where power distance is high result in poor communication on security issues between upper level management and employees and technicians. The framework for adaptive information security systems would enforce policies and procedures, which require continuous communication on security issues between upper level management and employees and technicians.

3.1.3 Model for Understanding the Methods of an Adversary of IT
The socio-technical security model was applied to analyze the threats and to understand tools, methods and processes that an adversary of IT applies to attack information systems (Kowalski & Mwakalinga, 2011a). The adversary of IT investigates the tools, methods, and processes that an information system is applying to defend in the different subsystems like deterrence, prevention, detection, response, and recovery. This information will help the adversary of IT to determine weaknesses in the different sub systems. The information gathered so far would assist the adversary of IT to decide whether it was possible and worthy to attack an information security system. Adversaries of IT appear to be organized in groups in the following way. The first group is of researchers who investigate systems to find vulnerabilities in applications, operative systems, frameworks, and in different products (Kowalski & Mwakalinga, 2011a). The next group is software coders, who write intelligent malicious toolkits and programs like Trojans for monitoring, capturing, retrieving information, and covering their activities. The next group is of botnets army keepers, which maintain and increase the army of botnets. The next group consists of attackers, which include all kinds of hackers that perform the attacks. Some attackers use botnets, which they hire at prices that are set by botnet army keepers to gain information. The next group consists of consumers who use the stolen information and translate it into money. Consumers use the stolen information by creating fake credit cards, transferring money from victims’ online banking accounts. The helpers’ group includes mules and entities who offer free hosting servers for storage of stolen information. Money mules are a network of people who transfer stolen money from banks in one country to other countries at commissions.

3.1.4 Principles for Securing Mobile Agents
Measures for securing mobile software agents in the holistic and immune security framework were studied. The author learned how to secure communication using mobile agents and how to secure information carried by software agents. Specific software agents for deterrence, protection, detection, response, and recovery sub-systems were created. Specialized mobile agents for registering, authentication, confidentiality; integrity, non-repudiation, and authorization were created.

3.1.6 Principles for Securing E-governments
The author investigated the measures for securing e-government systems. Most e-government systems use one form of authentication, one form of access control in all types of services without considering the different sensitivity levels of the information in the e-government systems. Multiple authentication methods are provided. Some e-government services require simple authentication while other highly classified transactions demand strong authentication. Multiple authorization schemes, information integrity schemes and digital signature schemes are also provided. The principles accommodate different e-literacy levels of users of an e-government system. Countries have different levels of e-literacy and users with low levels of e-
literacy do not understand some e-government security systems. These schemes could be configured to accommodate different e-literacy levels. The system integrates registration, certification, authorization, and smart card systems. The principles support an integrated e-government system with other private organizations like transport, banks, manufacturing, and other organizations.

3.1.7 CULTURE AND SECURITY VALUE-BASED CHAIN FUNCTIONS
Two surveys were made to understand how culture affects users’ decisions on prioritizing the security value-based chain functions deterrence, prevention, detection, response, and recovery. The complete results of the survey are in appendix D. Although the surveys were only done on university students it appears that people of different cultures put different priorities on the security value-based chain functions. The results also indicate that there appears to be a difference in the way men and women put priority on the security value-based chain functions. Men and women agree that prevention is first priority but differ in percentages allocated to the prevention sub system. For women deterrence function has second priority while for men deterrence function has fourth priority. Both men and women put the least priority on the response function. Another aim of the survey was to understand the ratio of social security measures in comparison to technical security measures that users from different countries apply in the security value-based chain functions. There appears overall to be more emphasis on using technical security measures than social security measures. The biggest differences were in the prevention and detection functions where it is almost 70 to 30 % split in favor of technical security measures. However, it is difficult to generalize on security culture from these surveys at this stage and more studies need to be made.

3.1.8 APPLICATION OF THE FRAMEWORK TO SECURE E-LEARNING AND SOCIAL NETWORKS
The adaptive framework for information security systems can be used to secure small and large information systems in small and large companies. This was illustrated when the framework was applied to secure an e-learning system as described in paper IX (Mwakalinga, Kowalski & Yngström, 2009b) and social networks as reported in paper XII (Mwakalinga & Kowalski, 2011c).

3.2 CONCLUDING REMARKS
The goal of this holistic investigation was to explore, understand, explain, design, test, and discover how to minimize the gap between the capabilities of information security systems to control abuse and the needed capabilities. The framework for adaptive information security systems was developed to achieve this goal. The developed framework presents a methodology for making information security system adapt to changing environments and changing cultures. The developed framework lays down a methodology for applying also including non-technical factors like culture, legal and other social issues when developing information security systems. The thinking process according to (Armstrong, 2006) was applied to plan and to guide the research, together with the holistic research process according to (Schwaninger, 2007). In order to solve the research questions, research was divided into mini studies, the results of which were reported at 11 international conferences and one journal. The major research problem of filling the gap, was divided into five research questions. The first research question required the identification of critical systems for adaptive information security systems, in analogy to Miller’s theory (1978) of 19 critical systems for living system to survive in different environments. The identified critical systems for adaptive information security systems are deterrence, prevention, detection, response, and recovery.
The second research question required an investigation of the adaptation systems for making information security systems adapt to environmental and cultural changes. The first identified adaptation system was the immune system whose principles provide internal adaptation measures in the components of the security framework. In the framework for adaptive information security systems software agents are applied in analogy to cells in the immune system to provide security services and perform different tasks. The software agents have to be secured before providing security services. The second adaptation system was the Viable system model (Beer, 1984), applied to provide measures for adapting to the future, embedded, and local environments. The third adaptation system was the Cybernetic structural model (Herring, 2002), applied to provide external adaptation measures and a study how to provide adaption measures in information security systems for adapting to environments and culture.

The third research question required the identification of a method to provide identity management in information security systems. An integrated security system for identity management was designed for this reason. The fourth research question required a study of the models that an IT adversary was using to attack information systems. The Social-technical security model is aimed at addressing security problems at different levels and perspectives at the living; abstract; and concrete. This model could also be used by the security administrators to detect potential victims in a network indicating where to put more attention. The study also examined how to increase the ratio of the states that could be controlled by an information security system. Security can also be defined as the ratio of the states known and unknown that could be controlled by the enemy of IT to the states that can be controlled by the information systems. The smaller the ratio of the states controlled by the hacker to the states that are controlled by an information system the harder it is to succeed when attacking. If this ratio is high it is easier for the attacker to succeed the information system and difficult to control the information system. The results also include the way the hackers are organized which helps to understand how to respond during attacks and intrusions. The fifth research question was to study on how to apply the results from the investigation to protect information systems. The researcher applied the framework to secure an e-learning system and a telemedicine system.

3.3 Future Work

This thesis has covered research in theory of Information System security and information Technology security, and Information Technology security practice as outlined in Figure 25 (on the left hand side). The plan of future is to cover research in practice in information system security as shown in Figure 25 (right hand side). Knowledge is applied to understand, to explain, to predict, and to control. The knowledge acquired from this research would be applied at the individual, organizational, and national levels as accordance to the system thinking. The framework would be used first, at the individual level to protect a workstation or wireless devices like mobile phones. Then the framework would be applied at the organizational level and then at the national level. This framework for adaptive information security systems offers a solution for systems but it will also use point security solutions like intrusion detection systems and virtual private networks. According to hype cycle for information security (Gartner, 2006) it takes between 1 to ten years for point security solutions to mature it is predicted that it could take five years for this framework to mature.
FIGURE 25: FUTURE PLANS OF THEORY AND PRACTICE IN IS AND IT SECURITY
REFERENCES


Enabling Tomorrow Conference. Co-sponsored by IFIP and the IEEE Systems, Man and Cybernetics Society (SMCS) Chapter, a chapter of the IEEE South Africa Section


PAPER I
Authorization System in Open Networks Based on Attribute Certificates

Jeffy Mwakalinga¹, Eric Rissanen², Sead Muftic³

¹Department of Computer and System Sciences, Royal Institute of Technology, Kista, Sweden
Fax: +46 8 703 9025 Tel: +46 8 16 1721
²Swedish Institute of Computer Science, Kista, Sweden
³Department of Computer and System Sciences, Royal Institute of Technology, Kista, Sweden and Computer Science Department; The George Washington University, Washington DC, USA.
[jeffy@dsv.su.se, erik.rissanen@bredband.net, sead@gwu.edu]

ABSTRACT
This paper describes a security system for authorization in open networks. Authorization means authority to access certain resources, to perform certain operations, or to use certain system functions. In this paper, the authorization system bases on use of attribute certificates. An attribute certificate is a signed object containing authorization attributes of a user. Before checking whether a user is authorized to perform an action or to access an object, the identity of the user must be verified. The identity verification system bases on public key certificates. We separate authorization system from authentication system because the same authority does not always establish authorization and authentication information. However, these two systems must be combined and that is done by including the serial number of the user’s public key certificate as a field in the users attribute certificate, which carries authorization information.

The topology of the authorization system comprises authorization authority servers issuing attribute certificates to users, application clients handling those certificates, and application servers verifying user access rights based on attribute certificates. Furthermore, all these components are themselves certified by standard PKI certification authorities, thus supporting mutual authentication and cross-domain scaling.

Keywords
Certification authority, attribute certificate, attribute authority, authorization and access control models.

1 INTRODUCTION
1.1 GENERAL PRINCIPLES
This paper describes a generic system for authorization in open networks based on attribute certificates. Authorization means authority to access certain resources, to perform certain operations, or to use certain system functions. Authorization addresses three major problems: identification of users and assignment of globally recognized roles; matching of user roles with authorization attributes like security labels; enforcement of authorization privileges and making decisions. Today organizations run Web servers and resources of these servers should be accessed globally only by authorized people. For instance, companies have IT
resources, only accessed by customers who subscribe for them. In most cases, the system gives a user name and a password to a customer, who subscribes for resources, and can log in using these tokens to the servers. A user should be able to access the resources from any machine in the global network. A customer may decide to pass the username and password to friends. Friends can then access the resources without having paid for them. Authorization systems have to provide a mechanism for minimizing this risk. An authorization system should make it possible for a client to verify whether the signer of a cheque has authority to do so. In all these cases, a secure and global system of authorization is required. Authentication of clients comes before authorization to access or perform a task. The first task of an authorization system is therefore to authenticate clients. So how can the system reliably authenticate clients in an open network?

There are two types of authentication schemes: simple authentication and strong authentication. In this system, we use using strong authentication and clients and servers mutually authenticate each other. It bases on public key certificates. A client is required to present her public key certificate for authentication to the server. The second task of an authorization system is to check whether the authenticated client has authority. We describe this in section 4.2. What are the requirements of an authorization system in open networks?

1.2 REQUIREMENTS

We must combine authorization in open networks with authentication system. This is so because authentication comes before authorization to access resources or perform certain functions. Separate systems should provide authentication and authorization because the same authority does not usually create authorization and authentication information. The system must be secure so that people can trust it. It should be possible to delegate rights and privileges to other entities. It should be easy to administer which implies that an authorization system should have a user-friendly interface. The system should be scalable and efficient, because it is for global systems where delays are not acceptable. It should support distribution of authorization elements. Authorization in open networks should be flexible supporting alternative authorization policies.

1.3 AUTHORIZATION POLICIES

An authorization system bases on authorization policy of an organization. An authorization policy specifies rules for accessing objects or performing certain actions. We could specify this policy in terms of access control lists, capabilities, or attributes assigned to subjects, objects or both. Access control models usually describe policies. An access control model is an abstract description of an access control system and its main goal is preventing unauthorized access to resources of a computer or information system. An access control model comprises the following items: a target, which is the object to be accessed; an initiator, which is an entity wishing to access the target and an access control function, which uses access control information to decide whether a subject can access a target. Access control function passes its decision to an enforcement function, which provides access to the target information or prevents it based on the output of the decision function.

Organization of Sections

Section 2 covers current approaches. Section 3 deals with the principles of an authorization system in open networks. Section four describes a prototype of the
authorization system. Section five briefly discusses conclusions.

2 CURRENT APPROACHES

2.1 SOME SOLUTIONS ON RESTRICTING ACCESS

Authorization in open networks could base on IP addresses and domain names [4]. In this case, a server examines the incoming request and grants or denies access depending on the IP number or domain name. IP-based authorization is not suitable for mobile clients and it does not accommodate dynamically allocated or shared IP addresses. This type of authorization is not secure, because today it is relatively easy to forge IP numbers. The system is vulnerable to DNS spoofing and IP spoofing where an attacker takes control of the DNS host-names’ lookup system. As a result, one leads a server to believe that it is talking to a trusted host. How can one verify whether an IP address is genuine? One way is to extract the IP address and then double-check with the DNS system of the client. The system could make a request to the DNS to return the host name of the IP address and then the system checks this IP address. The system makes another request to the DNS system to return the IP number of the host name returned in the previous request. If these match then the IP address is most likely genuine.

It is also possible to minimize the problem by using firewalls, which use reliable DNS lookup. However, how can one determine whether a DNS lookup is reliable? Are there any trusted and reliable DNS lookups today? Can firewalls be trusted? We configure these systems properly in order to function correctly and not all firewall administrators are competent in this area.

Authorization bases on certificates. When a user requests a service, she presents a digitally signed certificate together with the request. A server grants access if certificate is valid. To be valid means, the system validates the chain of certificates.

2.2 ROLE–BASED ACCESS CONTROL (RBAC) SYSTEM FOR SECURING A WEB-BASED WORKFLOW

Ahn, Sandhu, Kang and Park [2] describe a way to add a RBAC system to an existing web-based workflow system. A web-based workflow system consists of an interface for clients, a gateway to external services, a tool for protocols, and workflow tool for descriptions and enforcements, where the work performs activities in coordination. Different servers execute different tasks. These systems provide only low-level security services such as simple authentication. Authentication and authorization security services bases on public key certificates. The system uses HTTP protocol for client–to–server communication and uses CORBA’s network addressing protocol for server-to-server communication. The system attaches different roles to each task. Users’ identities are verified and then checked whether authorized to perform tasks, which they request Role–Based Access Control (RBAC) model in this system have a set of roles, a set of permissions, and users. This model supports role hierarchies. The system assigns permissions to roles and users may have different roles. Users can have one or more roles. A role can be assigned one or more permissions and vice versa.

RBAC system consists of three major components: a workflow design tool, a role server, and a Web-based workflow system. The administration of the system applies the workflow design tool for generating roles, building role hierarchies, assigning roles to tasks, specifying flows of information and relationships among tasks, and for passing information to the role server. The role server has two
components: a user-role assignment component and a certification server. The functions of user-role component include assigning users to roles, and creating and managing role hierarchies and databases. The certification server is responsible for verifying users’ identities, fetching users’ information from databases, and issuing certificates with users’ role information. The workflow system contains Web-based task servers. A task server approves authorization to a client based on the information found in user’s certificate. The system gives authorization to the client during the establishment of SSL session between a client and a task server. The Web server asks for a client certificate during SSL handshaking procedures. Client sends a certificate to the server. The server verifies the identity of the client. The server extracts authorization information from the client’s certificate and checks whether this client has authority.

The advantage of this system is that the administrator makes very little changes on the server side and no changes on the browser’s side. If one of Web servers is manipulated, it does not cause the system to stop, because servers are doing multiple and different tasks. The disadvantage of this system is that both authentication and authorization information are based on public key certificates. Different authorities could set and update authorization and authentication information. It is also inconvenient with respect to policy management, because different authorities can have different policies. Validity of authorization information and authentication can also be different.

2.3 ONE-SHOT AUTHORIZATION SYSTEM USING SMART CARDS

Au, Looi, and Ashley [1] present an authorization system based on smart cards. This system could provide services in coordination with any existing authentication system and it can authorize clients across multiple domains. In one domain, the system consists of three components: a client workstation, a security server, and an application server. The system connects the client workstation to client’s smart card reader. On this workstation there is a program called Authorization Token Manager. This program communicates with an application server and the administrator of the application server installs it on the client side. This program retrieves one–time authorization tokens, verifies them, and stores them in the smart card together with private keys and other information. Client’s smart card authenticates remote servers, verifies authorization tokens, and creates session keys. After using these one-time tokens, the program renews them. Security server contains two modules: an authentication server and an authorization server. An authentication server verifies identities of clients. An authorization server performs authorization services. The security server communicates with an application server to get initial and updated authorization information. It also communicates with the workstation to exchange authentication information. The application server maintains an access control list, a valid token ID list, and accesses the information list.

The advantage of this system is that authorization tokens are one-time, which solves the problem of replay. The disadvantage of the system is that it creates heavy traffic, because it issues one-time authorization tokens. Another shortcoming of this system is that it is not explained how the messages are protected while in transfer, so it is difficult to determine how secure the messages are during this process.
3 USE OF ATTRIBUTE CERTIFICATES FOR AUTHORIZATION IN OPEN NETWORKS

3.1 ATTRIBUTE CERTIFICATES
An attribute certificate (AC) is a signed object containing authorization attributes of a subject. Attribute Authorities (AA) are the components responsible for issuing attribute certificates. The serial number of the client’s PKI certificate, which is used for authentication purposes, is inserted in a field called holder. Fields of an attribute certificate according to [6] are:
- Attribute certificate information
- Signature algorithm identifier, which is an algorithm used to sign the AC
- Signature value, which is a signature of the issuing AA

The fields in the attribute certification information include:
Version: This field contains the version of the attribute certificate (AC).
Holder: This field contains the identity of the holder of the certificate. It has the serial number of the owner’s public key certificate, general names of the AC’s owner, digest information, which can include public key, public key certificate, digest algorithm and so on.
Issuer: It contains the identity of the issuer of the attribute certificate.
Signature: This contains the algorithm that was used for signing the attribute certificate.
SerialNumber: It has a serial number of the attribute certificate.
AttrCertValidityPeriod: This field contains the validity period of the attribute certificate in the form of two dates defining a time interval.
Attributes: This field contains the actual attributes and this field is specified by the issuer of the attribute certificate. These attributes include service authentication information, access identity, charging identity, group, role, clearance etc.
IssueUniqueID: This field contains additional information to help locate the issuer.
Extensions: Extensions contain some additional information about the attribute certificate: audit identity for audit trails. Other extensions are attribute certificate targeting, which is used to specify the number of targeted servers or services; authority key identifier, which is used to assist in verifications of the signature of the attribute certificate; authority information access, which is used for checking revocation status of a certificate; and CRL distribution points, etc.

Attribute certificates are stored in the same way as public key certificates: in global repositories or in directory systems. Attribute certificates can be revoked. However, in cases when their lifetimes are too short, revocation may not be necessary. Revoked attribute certificates can be stored in attribute certificates revocation lists. This is a list of AC’s serial numbers. It must be possible to verify the authority of the issuing AA, i.e. there is a valid chain of public key certificates containing the extensions asserting AA’s authority. In inter-domain environments, there should be a way of translating attributes issued by other domains into the domains responsible for validating the ACs. Attribute certificates should keep all or some of its attributes confidential if so desired by clients. Attribute certificates are useful in supporting delegation.

3.2 AUTHENTICATION OF CLIENTS AND ASSIGNMENT OF ROLES
When a client connects to an authorization server for the first time, a client is authenticated by presenting her public key certificate. This certificate is verified by
validating certification chain from the authority, which issued the certificate to the top certification authority in the hierarchy. A check is also made to verify that the certificate in question is not revoked. If the certificate is found to be valid then an attribute certificate is issued to the client. Roles and clearances are given to the client and they are written in the client’s attribute certificate. These roles and clearances specify authorization of the client and these specifications are stored in the policy file of the attributes authority. A reference to the client’s public key certificate is also included in the attribute certificate in the field called holder. In this attribute, there is a sub field called baseCertificateID and this sub-field holds the serial number of the client’s public key certificate. After populating all the fields of the client’s attribute certificate, the certificate is signed by the issuing AA. A client can protect some fields of the attribute certificate using secret keys. The attribute certificate is then stored in the X.509 Directory or in a global database. A copy of this attribute certificate is sent to the client.

3.3 SYNCHRONIZATION OF ROLES AND AUTHORIZATION ATTRIBUTES

When a client makes a request to access resources of a secure Web server, she presents her public key certificate. This certificate is validated as described in section 3.2. If validation is successful then the serial number of this public key certificate is used to pull the client’s attribute certificate from the directory or from the global database. If client’s AC is not found at the server or if the database or X.500 directory is down, then the client is requested to send her AC to the Web server. Every resource in the secure Web server has a security label. Labels are attached to resources by using S/MIME. S/MIME is a standard for encapsulating MIME documents and provides services like confidentiality, integrity, and authentication. Confidentiality is a security service, which protects resources from illegal read, illegal access, deletion, sabotage and so on. Integrity is a security service that protects resources from illegal modification, deletion etc. The resources are stored in the security Web server in encapsulated forms. The security labels that are attached to resources specify in the policy file which roles and clearances can access the corresponding resources. The security label has a list of all roles, which can be granted access. The policy file contains information on security classifications and categories. It can contain information mappings among different security policies. If a policy of a company changes then it is enough to update the policy file without needing to change other modules. A Policy Creation Authority (PCA), which is a trusted entity, signs the policy file. Security labels and clearances have policy identities, which are references to the policy files in which they are specified. The policy file contains lists of security classifications and categories and all allowed combinations of them. All messages between a client and a secure Web server are protected using S/MIME, SSL or other secure protocols.

3.4 ENFORCEMENT IN THE AUTHORIZATION SYSTEM

Decisions to grant access to the secure Web server’s resources are based on the policy of the AA. This policy is created by the Top or Root certification authority and all the entities under this root certification authority use this policy. Roles, clearances, ranks, security labels and other attributes and information are specified in this policy file. The attribute certificate of the client is
pulled from the global database or from the X.509 Directory. The security Web server must verify the attribute certificate by verifying the signature of the attribute certificate. The validity of the AC must also be checked. The subject in the attribute certificate, the AC’s issuer, and the complete certification chain is validated. A local certification authority, as explained in section 3.5, certifies the AA. The client’s AC contains clearances or roles of the client. These attributes specify the authority of the client. Access control decision function takes as parameters, a policy file, a security label, and an authorization set and this set includes a clearance, a role and other parameters. Access is granted if the client’s attribute certificate is verified and if the client has a clearance or a role that matches the security label of the requested resources.

3.5 MANAGEMENT INFRASTRUCTURE

The system uses the X.500 authentication framework. This system uses certificates-based authentication. Clients are required to have public key certificates before being authorized to access or perform actions in the authorization system. Certification authorities (CA) certify attributes authorities (AA), which issue attributes certificates. The complete system is shown in Figure 26.

At the top, there is a trusted root certification authority. Below this root CA there is one or more intermediary certification authorities depending on the complexity or size of the organization. The last CA in the hierarchy is a local CA. This is responsible for certifying the Attribute authority, managing public key certificates to clients, managing keys, revoking certificates and so on. At the root CA there is a Security Policy Information File (SPIF) for the entire system. This file contains the policy for the whole system. Every certification authority has a certificate, which contains an extension called cAClearanceConstraints. This extension enables authority to act as an Attribute Authority (AA). The root CA issues a self-signed certificate to itself. It then issues certificates to the lower entities. If the root CA belongs to a company then this company can have middle certification authorities in different countries where it has offices or its business. Certificates

**FIGURE 26: MODEL OF SYSTEM COMPONENTS**
issued to lower entities have to be verified by checking the signatures of certificates. The whole chain up to the root CA has to be validated. The local CA issues a certificate to the AA, which in turn issues an attribute certificate to the end entity. The policy file, SPIF, has to be signed by the root CA so end entities must verify the signature before using it. In cases where there are different root certification authorities and belong to different organizations then root certification authorities are required to cross certify each other so they have to issue certificates to each other and these certificates will contain the corresponding cAClearanceConstraints extensions.

3.6 DELEGATION OF ATTRIBUTES

Delegation of attributes is done with the help of a field called attribute in the attribute certificate and with the help of an extension in the AC that is called authority information access. Authority information access has an IP address of the directory where the issuer of the attribute certificate may be found. This extension can also store an IP address of the directory that has the AC of the upper entity that delegated attributes to the lower entity. When the Web server receives a request, from a user it can authenticate her as described in section 3.3 and if authentication of the user is successful, the Web server will retrieve the user’s AC and check its validity as discussed in section 3.4. If attributes are delegated then the attribute’s value will be delegated set of attributes. The Web server will thereafter get the AC of the delegating entity from the directory whose IP address was in the authority information extension. The AC of the upper entity will be verified as discussed in section 3.4. The user will be authorized if the AC of the delegating entity is valid.

4 IMPLEMENTATION OF A PROTOTYPE

This prototype bases on geotronics [7] library suite. The RBAC is implemented using access control library in the following way. It is specified in the policy file, SPIF file, as described in section 3.4, so that all the roles are given security categories. Categories are authorities to perform different functions or access different objects in the secure Web server. Every security label has a list of roles, which are authorized to access certain resources or perform the desired actions. Every clearance in the attribute certificates contains a list of the roles, which can be granted access.

4.1 THE ACCESS CONTROL LIBRARY SUITE

This authorization system uses the access control library [3] and it consists of the following libraries.

SNACC - This is a high performance ASN.1 to C/C++ Compiler. This library contains an ASN.1 compiler for encoding and decoding data structures.

S/MIME Freeware Library (SFL) - this library provides support for cryptographic functions like signing, verifying signatures, protecting messages and so on.

Certificate Management Library (CML) - this is used to verify the certification paths.

The Storage and Retrieval Library (SFL) - this library is used for maintaining the database for certificates. SFL is used for providing functions for parsing, generating, protecting, and verifying SMIME messages.

Access Control Library (ACL) - this library takes care of access control decisions basing on S/MIME security labels, X.509 certificates, and attribute certificates.
4.2 IMPLEMENTATION

There are three components in the prototype: An administration tool, a SPIF generator, and a certification manager. An administration tool, AdminTool (Figure 30), is used for managing roles and S/MIME documents. The SPIF generator is used for generating policy files, SPIF.

The administrator chooses an item to be generated from the interface in Figure 27. The administrator can choose to generate an SMIME document, an attribute certificate, or a new Security Policy Information File (SPIF), see Figure 28:

![Figure 27: Choosing an item to generate](image)

The administrator of the system creates a policy file as explained in section 3.4, enforcement in the Authorization System. She/he does this by activating the SPIF generator and a panel shown in Figure 28 will be displayed. In the SPIF generator, one has to specify the policy ID and a version of this policy file. Then roles have to be created. After creating the roles, SPIF file must be signed using the private key belonging to the issuer of the policy file.

![Figure 28: SPIF generator](image)

To issue an attribute certificate as discussed in section 3.2, recognition of clients and assignment of roles, an administrator selects option attribute certificate from the interface in Figure 29. Thereafter the administrator selects the policy file and public key certificate for authentication purposes as described in section 3.2. Different fields like serial number, validity,
roles, etc, are populated in the attribute certificate. The attribute certificate is then signed. Before storing the attribute certificate to the database, trusted certificates must be added to the database or to the directory system. These certificates are necessary for certificates chain validation as discussed in section 3.2. This is done using Certificate Manager Interface, shown in Figure 29. Attribute certificate can then be added to the database or to the X.500 Directory.

The next step for security administrator is to attach security labels to resources (in this case Web documents) as described in section 3.3. To add documents to the Web server, the administrator selects SMIME Document option from the AdminTool panel and this panel shown in Figure 30. Then he/she selects a document to be encapsulated and the corresponding SPIF to be used. The administrator then specifies the roles, which can access this document. The private key for signing the security label must be specified.

When a client requests to access a site on the Web server, the server expects client’s public key certificate The Secure Socket layer [8] is used for establishing secure sessions between the client and Web server. SSL is a system for securing messages while in transfer. The server checks whether client is public key validates the client’s digital signature as discussed in section 3.2. It also checks whether today’s date is within the certificates validity period. It also checks whether the CA that issued client’s certificate is a trusted CA and whether the public key of client’s certificate issuer validates the issuer’s digital signature. The server checks whether this certificate corresponds to the serial number in the attribute certificate. Then the Web server checks with the ACL to decide whether an incoming request is authorized to access the site. Web server loads the Publish dynamic library and passes the name of the selected document as a parameter to the access method of the extension. Documents are stored on the server in S/MIME format and contain security labels as described in section 3.3. The extension function fetches user’s attribute certificate from the X500 Directory and compares the role in it with the security label of the requested document. If the client is assigned the roles contained in the security label of the document, the document will be transferred to the client. If the client is not authorized to access the file, he/she will get an http “404 Not found” response.
5 CONCLUSIONS
This system is flexible and interacts with other systems like PKI certification system, X500 directory system, and smart card systems. Attribute certificates support delegation through an ordered sequence of attribute certificates with references to certification authorities. Attribute
certificates can be used for non-repudiation services making it possible to extend authorization systems to support this service. The system separates authentication security service from authorization making it possible for authentication and authorization decisions to be made by different authorities when necessary.

REFERENCES


PAPER II
ABSTRACT
This paper describes an integrated security administration for global organizations and electronic government systems. It integrates certification systems, authorization systems, registration systems and smart card systems. Many organizations today are having departments all over the world. Employees, employers and customers have to access information located in different countries. This complicates management of security systems for the organizations. The challenges that the organization face include providing authentication, authorization, protection of information, non-repudiation, integrity, privacy and other security services in the global environment. Today, organizations usually install certification, authorization, smart card, and registration systems and apply them separately without sharing common data and without any common security administration procedures. Thus, a new employee or citizen, who needs registration services, a smart card, a public key certificate, and authorization attributes must usually identify herself multiple times and must perform registration procedure at four different administration stations. In this research, we designed an integrated security administration procedure for all four-security systems, where we register users only once and the four security systems share all relevant security data and procedures. Therefore, the new integrated security administration is more efficient than existing procedures and it is simpler to manage and saves administration costs. This system bases on the Security Assertion Markup Language (SAML). SAML is an XML-based framework for exchanging security information. The research has achieved two goals: functional integration of data and security administration procedures and visual integration through a common security administration interface. These results are of high interest and importance when managing different components of an integrated security system. 

KEYWORDS
PKI System, authorization, SAML, Directory system, smart card system, certification authority and attribute authority.

1 INTRODUCTION
The goal of this paper is to describe a generic management security system for open environments. This system is also suitable for governments that are transforming manual government services into electronic services. The system also
applies to organizations that are supplying services to global markets. The government and organizations have to identify customers, employees, employers, citizens in global environments. This management system bases on the Security Assertion Markup Language (SAML) [10]. SAML is an XML-based framework for exchanging security information.

**Organization of Sections**

Section two covers related work and section three discusses Integration. Section four describes the prototype of the system. Section five briefly discusses conclusions.

**2 Related Work**

**2.1 Smart Card System**

Today smart card systems are managed in the following way [1]. The system consists of a central card management component, a card-personalizing component, a printer, an integrator, an enrolment component, a cardholder database, a logical access control component, a physical access control component and a certification authority server. At an enrolment component, a cardholder registers her information. With the help of a digital camera, a normal scanner, a biometric scanner and other equipments, cardholder’s photograph, signature and other data enter the enrolment component. The enrolment component sends information to an integrator. The integrator takes physical and logical privileges from the physical and logical access control components respectively, and combines them with the data from the enrolment component. The integrator sends this information to the card management system. This is responsible for updating the cardholder’s database. The database stores information about expired, lost, and stolen smart cards, copies of the cardholder’s information, etc. This component takes cardholder’s certificate, data from the card management system, and other data and personalizes the card. The system prints and issues the smart card to a cardholder.

**2.2 Role–Based Access Control (RBAC) System for Securing a Web-Based Workflow**

Ahn, Sandhu, Kang and Park [3] describe a way to add a RBAC system to an existing web-based workflow system. A web-based workflow system consists of an interface for clients, a gateway to external services, a tool for protocols, and workflow tool for descriptions and enforcements, where the workflow performs activities in coordination. Different servers execute different tasks. These systems provide only low-level security services such as simple authentication. Authentication and authorization security services bases on public key certificates. The system uses HTTP protocol for client–to–server communication and uses CORBA’s network addressing protocol for server–to–server communication. The system attaches different roles to each task. The system verifies users’ identities and checks whether authorized to perform tasks, which they desire. The Role–Based Access Control (RBAC) model in this system has a set of roles, a set of permissions and users. This model supports role hierarchies. The system assigns permissions to roles and users have different roles. Users can have one or more roles. A role can be assigned one or more permissions and vice versa. The system consists of three major components: a workflow design tool, a role server, and a web-based workflow system. The administration of the system applies the workflow design tool for generating roles; building role hierarchies; assigning roles to tasks, specifying flows of information and relationships among tasks and for passing information to the role
server. The role server has two components: a user-role assignment component and a certification server. The functions of user-role component include assigning users to roles, and creating and managing role hierarchies and databases. The certification server is responsible for verifying users’ identities, fetching users’ information from databases, and issuing certificates with users’ role information. The workflow system contains web-based task servers. A task server approves authorization to a client based on the information found in user’s certificate. The client is given authorization during the establishment of an SSL [7] session between a client and a task server. The Web server asks for a client certificate during SSL handshaking procedures. Client sends a certificate to the server. The server verifies the identity of the client. The server extracts authorization information from the client’s certificate and checks whether to authorize the client.

The advantage of this system is that the administrator needs to make very little changes on the server side and no changes on the browser’s side. If one web server is compromised, it does not cause the system to stop, because servers are doing multiple and different tasks. The disadvantage of this system is that both authentication and authorization information are stored in public key certificates. Different authorities could set and update authorization and authentication information. It is also inconvenient because different authorities can have different policies. Validity of authorization information and authentication can also be different.

3 INTEGRATION
This section describes integration of security management functions and procedures of the directory system, PKI system, smart cards system, and authorization system.

3.1 METHODOLOGY
The procedures of the components were analyzed first. Procedures were analyzed to determine which of them were common in all the systems and the result is shown in Table 10.

Security management procedures of the directory, PKI, smart card, and authorization systems are integrated in such a way that an administrator does not need to perform the same action four times for each individual security system as indicated in Table 10.

Registrations of users, identification of users, and verification of users’ identities are performed once for each user. Data are then shared by individual security systems and are available to each of these systems. When a public certificate is issued, it is stored in user’s smart card, in the directory system, and in the certification authority’s database at the same time. When authorization attributes are issued to a user, they are stored in user’s smart card, in directory system, and in authorization system at the same time. All shared data and procedures are integrated through a single graphical user interface, available to the security administrator. Data and procedures are displayed and available in a user-friendly form. The administrator can view data belonging to individual security systems and may register and update entries from the same interface.

3.2 DESIGN OF THE SYSTEM
The directory, X.500 [2], Public key Infrastructure (PKI), authorization, and smart card systems provide the basic ISO security services: authentication, access control, data confidentiality, data integrity, and non-repudiation. The security platform, that contains libraries and security mechanisms, supports this system. We
apply the Lightweight Directory Access Protocol (LDAP) [4] for accessing the X.500 directory. LDAP has methods and interfaces for communicating with the X.500 directory but these interfaces are not object-oriented and are very complicated for a normal user. In this work, we have created generic objects and object-based interfaces to solve the problem. We have developed a single PKI system [5] and it has objects and interfaces for certification, registration of users and organizations, management of certificates and keys, etc. The authorization system bases on the SAML [10]. The smart card system has objects and interfaces for formatting smart cards, creating file systems, for initialization, personalization of smart cards and other management procedures. We implement the US Government Smart Cards Architecture standard [8] in this research.
TABLE 10: ANALYSIS OF PROCEDURES

<table>
<thead>
<tr>
<th>Function</th>
<th>Smart cards</th>
<th>Directory</th>
<th>Authorization</th>
<th>PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration of Users</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Issuing Certificates (PKI, AC)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Creating a CRL</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Publishing Certificates</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification of users’ ID &amp; Data</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Storing Certificates</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Validation of Certificates’ Chains</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cross-certification</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Updating objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Submitting CRL</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Initialization of Cards</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personalization of Cards</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issuing Smart Cards</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Revoking objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SC Backups</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Stolen and Revoked SC</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Protection of objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Creating Roles</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Delete Object</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Setting ACL</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Loading Applets</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Display object</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Adding objects</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Recovery Operations</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

FIGURE 31: SECURITY ASSERTION MARKUP LANGUAGE

Figure 31 shows the integrated system. A company for example can have integrated security systems in different departments, which could be located in different cities and different countries. Secure Multiple Internet Extension (SMIME) [9] and Public...
Key Cryptographic Standard (PKCS) [10] will protect communication among these departments.

3.3 THE GENERAL MODEL OF THE SYSTEM

The system comprises the PKI system, the Authorization system, the Smart card system, a Policy decision point, the Directory system, the SAML [10], a client, and a web server as shown in Figure 31. SAML authorities as described in section 2.8 make SAML assertions. In this research, SAML authorities are PKI system, Authorization system, Smart card system, and Policy decision point. One administrator performs authentication, attribute, and authorization decision assertions. The web server has a policy decision point and a policy enforcement point.

3.4 REGISTRATION OF DIRECTORY OBJECTS FROM ONE INTERFACE

Representations from organizations, organizational units, countries, users, servers and other directory objects present their identities and other registration data to the administrator. The system sends applications for registration in the directory to the administrator. Public keys of the applying entities are included in the application forms. The system exchanges session keys for securing communication between them. The administrator of the directory sends to the applying entity a registration form and the public key of the directory. On the registration form, the user can indicate whether she desires to acquire a smart card, and/or certificate and/or an authorization attributes. The user may indicate whether she can personalize a smart card. The administrator of the system verifies the identity of the user the other registration data. If verification is successful, the administrator registers and writes the data into the directory system, into the smart cards system, into the PKI system, and into the authorization system at the same time.

Policies are stored in the directory system. The IETF’s [12] Policy Framework working Group is working on a model to represent policy information in the directories [11]. We describe the certification of entities in the following section.

3.5 CERTIFICATION OF CLIENTS

In this work, we are using a single PKI system. There is a top certification authority (TCA), a policy certification authority (PCA), a hierarchy certification authority (HCA) and a local certification authority (LCA). A client sends a certificate request to the LCA. The request includes among others a public key of the client. The administrator extracts data of this client from the directory system. The system processes and issues a certificate to the client. When the system issues the certificate, it stores it in the directory system, in the smart cards system, and in the authorization system at the same time. We apply certain extensions of a certificate that in this research. One such extension is Authority Information Access. We apply this extension to store an IP number of the directory that contains the certificate of the issuer. Another useful extension is CRL Distribution Points, which stores the IP number of the directory that contains the certificates’ revocation list.

3.6 SMART CARD SYSTEM’S ADMINISTRATION

The system performs the following steps in smart system’s administration: Creation of a file system, initialization of the smart card and personalization of the smart card to a specific owner.
3.6.1 Creation of File System of the Smart Card

An administrator starts by creating the directories in the smart card in accordance with the standard used. In this research, we are using the US Government Smart Cards Architecture standard [8] and it has one directory, called Government Smart card Architecture (GSA). Then the administrator creates files in accordance with the standard that the system implements. The US Government Smart Cards Architecture standard has the following files: card capability, general information, card information, personal protected information, access control, login information file, biometrics – X.509 certificate and PKI – Digital signature certificate.

3.6.2 Initialization of the Smart Card

In this process, the administrator extracts data of the smart card issuer from the directory. The system writes these data into the user’s smart card in a file that contains issuer’s data. In the US Government Smart Cards Architecture standard, the files are card information and general information. The system writes all fields of the card information file into the card during this process. In the general information file, we write the following fields into the card during the initialization process: organization, organizational unit, department number, department code, postal address, street address, physical delivery office number, locality, state or province, postal code, country and non-government agency.

3.6.3 Personalization of the Smart Card

The system extracts user’s data from the directory. The issuer or the cardholder may perform this process depending on the policy of the card issuer. The cardholder may update some or all personal data, while the administrator of the issuing organization updates some data, depending on the policy of the card issuing organization. The system writes data related to the cardholder into the smart card. In accordance to the US Government Smart Cards Architecture standard, we write data to the following smart card files: general information, protected personal information, Access control, Login information, Biometrics-X.509 certificate, and PKI – Digital signature certificate.

3.7 Authorization System

An administrator starts processing attributes of client by extracting client’s data from the directory. Thereafter an administrator extracts authentication information from the directory. In this research, the system uses a public key certificate of the client for authentication. After successfully authenticating the client, the administrator of the authorization system writes authorization information to the directory. The serial number of the public key certificate is part of this information. This serial number links the certificate to the authentication information to the authorization information. Authorization information can be stored in an attribute certificate or in attributes assertion.

3.8 Security Assertion Markup Language (SAML)

SAML [6] is a flexible Extended Markup Language (XML) based framework for exchanging security information about users on the Internet. SAML supports single sign on, which enables users to visit different sites without needing to login every time. The system represents the
security information in forms of assertions about subjects. Assertions contain authentication information, attributes of subjects and information about authorization decisions on resources. The SAML authorities manage and issue assertions, which include authentication authorities, attributes authorities, and policy decision points. Clients can request for assertions from the SAML authorities. Requests and responses are in the XML [15] formats. The protocol used for carrying the requests and responses is the Simple Object Access Protocol (SOAP) [14] over HTTP. SOAP bases on an XML based protocol and exchanges information in open environments. An assertion contains the following elements; major version, minor version, assertion ID, issuer, issuer’s instant, conditions, advice, XML signature [13], statement, subject statement, authentication statement, authorization decision statement and an attribute statement. The SAML architecture has the following components: a credentials’ collector, an authentication authority, an attribute authority, a policy decision point, a system entity (subject) and a policy enforcement point. The authentication authority, attribute authority, and policy decision points make decisions basing on policies. In this work, the PKI is an authentication authority, and authorization system is an authorization authority. A system entity logs in a domain and the authenticating authority authenticates the entity basing on the credentials supplied. The result of this process is stored in an authentication assertion as shown in Figure 31. The system creates a reference to this assertion, it is in the form of a ticket, and sends it to the entity. The entity can supply this ticket to different websites and will be authenticated basing on the ticket. If a website needs authorization information, the website contacts the attribute authority and requests for an attribute assertion. The system sends this assertion to the policy decision point, which issues the authorization decision assertion. The system then sends this assertion to the policy enforcement point on the website. The website will grant access to the requested resources depending on the authorization decision assertion.

4 PROTOTYPE
We have partly implemented this system and we briefly describe the prototype this section. The administrator starts by login into the security management system.

4.1 THE DIRECTORY SYSTEM
The administrator registers an organization, an organizational unit, or a user by selecting the directory from the interface. Then the administrator selects option Registration on the drop-down menu and then option register, then option organization, organizational unit, country or user on the interface shown in Figure 31. We fill the data into the registration forms and write these data into all the components of the system. When searching and retrieving data, the administrator selects the directory to search or retrieve data. Then an entity, organization, country, organizational unit, or user, is selected from which to search or retrieve data and the administrator enters the search string. The administrator updates information in the components by selecting option organization, organizational unit, country, or user and then selecting update from the menu. The update action enables data to be modified in all the components of the integrated system.
4.2 THE PKI SYSTEM
An employee or customer of an organization sends a certificate request to the administrator of the system. The administrator processes the certificate request by selecting Local CA from the PKI system in the interface, then organization and then certification. The administrator approves the certificate request of the organization by selecting certify and then choosing the request to be processed from the list of certificates’ requests. The certificate is then issued by selecting issue certificate in the menu. A certificate of a user is created in the same way as that of an organization. The issued certificate is then stored in the user’s smart card and in the directory system. To revoke a certificate an administrator selects option Certificate and then revoke and the certificate to be revoked. The administrator can perform other management actions like list certificate, delete certificate and so on.

4.3 SMART CARDS SYSTEM
An administrator creates the file system of the smart card. Then the administrator performs login session as shown in Figure 32 and then chooses option Smart Card from the drop-down menu and creates the file system by selecting Initialize Card. The first time this option is selected it activates creation of a file system of the smart cards, while the second selection causes initial data to be written to the smart card.

4.3.1 INITIALIZATION OF THE SMART CARD
An administrator selects smart cards system from the interface. Then the administrator selects option Initialize Card from the drop-down menu in the interface. In this process, the data related to the issuer of the smart card are written to the user’s smart card. Issuer related data are extracted from the directory system.

4.3.2 PERSONALIZATION OF THE SMART CARD
An administrator selects smart cards system, then option Smart Card and then option Personalize Card from the drop-down menu. In this process the personal data specific to the cardholder are written to the smart card. Personal data of the cardholder are extracted from the directory system.
5 CONCLUSIONS

This research has achieved integration of diversified security administration procedures through functional and visual integration. As a result, the integrated security administration system specified in this research simplifies user and administrator’s procedures. The user now goes to one administrator instead four different administrators. The system also simplifies activities of an administrator because she now performs administration from one interface on one machine. The administrator performs user’s registration once and data is shared by all the subsystems. From one machine, an administrator is able to visualize the whole system with all the components. The system reduces administration costs. The system uses SAML, an XML based framework, for exchanging security information between clients and web servers. This simplifies transfer of information because in one assertion we can have information about authentication of subjects, attributes of subjects and authorization decisions on resources.

It is expected that contributions and benefits of this research are the following:
- Easier administration of security system components;
- Easier reconfigurations, additions, and upgrades of the security system; and
- It is a flexible system and it is easier to extend with other components. A new component can be integrated with this system by performing an analysis of functions and data in the new component and then integrating the functions and data of the new component with the existing integrated system.

SAML is a flexible framework for exchanging security information and facilitates integration among different security components. Reduction of administration costs

Future work can include further extensions to the system to add notary system, trusted third party time-stamping system and to support conflict resolution services.
ACKNOWLEDGEMENT
Dr. Kasun De Zoysa, now at the Colombo University, Sri Lanka, for creating the security platform and for many advices
Chen Chen, at Computer Science Department, The George Washington University, Washington DC, USA, for participating actively in the development of the prototype.

REFERENCES
PAPER III
INTEGRATED SECURITY SYSTEM FOR E-GOVERNMENT

BASED ON SAML STANDARD

Jeffy Mwakalinga, Prof Louise Yngström

Department of Computer and System Sciences
Royal Institute of Technology / Stockholm University
Forum 100, S-164 40 Kista, Sweden
Email: jeffy@dsv.su.se, louise@dsv.su.se
Tel: +468 161 721
Fax: +468 703 90 25

ABSTRACT
This paper describes an integrated security system for electronic-government services. Many governments are transforming manual government services to electronic government services. This transformation is in most cases done without involving users of the services. This makes users of these services have little trust in the e-government. Security is in most cases not addressed from the early stages of e-government development. Some governments depend on security solutions from private vendors and these governments do not have full control of security. E-government services have different levels of classification and so they require different types of authentication and authorization methods. Most e-government systems today use one form of authentication in all types of services without considering the different sensitivity levels. All countries have different levels of e-literacy and users with low levels of e-literacy do not understand some of today’s e-government security systems. This security system provides multiple authentication methods. Some e-government services require simple authentication while other highly classified transactions demand strong authentication. This security system provides multiple authorization schemes, information integrity schemes and digital signature schemes. These schemes can be configured to accommodate different e-literacy levels. The system integrates a registration system, a certification system, an authorization system, and a smart card system. It bases on the Security Assertion Markup Language (SAML) standard, which is an XML-based framework for exchanging security information. The system can be integrated in existing e-government systems and can be built-in in new e-government systems. Information of different levels of classification can be stored in same websites and can be accessed through multiple authentication and authorization methods. This system enables the society to perform secure e-government transactions and accommodates different e-literacy levels.

KEY WORDS
Attribute certificate, integrated security system, e-literacy, assertion, and anonymity.
INTEGRATED SECURITY SYSTEM FOR E-GOVERNMENT

BASED ON SAML STANDARD

1 INTRODUCTION

Provision of electronic government services is one of the main goals of many governments in the digital world. It is cheaper to provide government services electronically than manually [1], and it reduces corruption practices, since one cannot bribe a server. An e-government service costs a government between US $1 and US $7, while a non e-government service costs a government between US $ 2 and US $ 200 [2]. The United Nations recommends development of e-government, in part three of the e-government handbook for developing nations [1], to consider the following challenges and opportunities in the design of e-government programs. These programs include “infrastructure development, law and public policy, digital divide (e-literacy and accessibility), trust (privacy and security), transparency, interoperability, records management, permanent availability and presentation, education and marketing, public/private competition/collaboration, workforce issues, cost structures and benchmarking” [1]. Privacy according to this handbook [1] involves protecting personal information that the government collects about individuals, while security is involved with protecting e-government sites from attacks and misuse. An example of laws involving personal information protection can be found in the Personal Information Protection and Electronic Documents Act [3]. This work is dealing with ways of providing security in e-government services.

There are different types of communications in e-government: government agencies to government agencies; government agencies to and from citizens; government agencies to and from business organizations [4], government agencies to and from international organizations and other countries. Willingness of citizens and other parties to use e-government services will depend on the trust that they have on the services. E-government services can be public or classified. There are four categories of e-government information and services [21] e-management, e-service, e-commerce and e-Decision making / e-democracy. An evaluation of the Australian local e-government indicated that there was progress in e-management but little progress in the e-service, e-democracy, and e-commerce areas. These services have different levels of classifications: high, medium, low, and these levels can in turn be broken into intermediary levels. The challenges in e-government services’ security [1][4] include identifying users, authenticating users, storing public and classified information in same websites, checking authorizations, auditing, signing transactions, resolving conflicts, keeping copies of information, and so on. Hence, e-government security systems should be able to meet the following requirements: should provide multiple authentication methods, authorization, credential issuance and revocation [5], audit, confidentiality, conflict resolution, accountability, availability, platform independent, privacy, information integrity, anonymity, scalability, single sign on and so on.
The challenges and requirements were analyzed to find ways of providing security services in e-government. The e-government security systems are to support small countries like Namibia with a population of about two million people as well as big countries like China with a population of over 1.275 (2003) billion people. Study was made to find ways of managing e-government services and information of different levels classifications. The study included the issue is e-literacy. There are different levels of e-literacy in every country. The different levels of e-literacy and services with different levels of sensitivity can be solved by having multiple authentication methods, authorization methods, privacy provision methods, conflict-resolution schemes, and so on. Different e-literacy levels may require complicated computation to be performed on the e-government websites and leave only light and user-friendly procedures on the e-government client’s side. A study was made of what the technology has to offer in these areas.

The remaining sections are organized in the following way:
The second section covers related work; the third section is about the e-government security system; section four briefly discusses the conclusions.

2 RELATED WORKS

This section discusses SAML [6] system, the integrated security system [14] and the challenges of an on-line authentication system.

2.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML) STANDARD

SAML [6] is a flexible Extended Markup Language (XML) based framework for exchanging security information about users on the Internet. SAML supports single sign on, which enables users to visit different sites without needing to login every time. The security information is represented in forms of assertions about subjects. Assertions contain authentication information, attributes of subjects and information about authorization decisions on resources as shown in Figure 33. Assertions are issued and managed by SAML authorities and they include authentication authorities, attributes authorities, and policy decision points. Clients can request for assertions from the SAML authorities. Requests and responses are in XML formats. The protocol used for carrying the requests and responses is the Simple Object Access Protocol (SOAP) over HTTP. SOAP [7] is an XML based protocol that is used to exchange information in open environments. An assertion contains the following elements: major version, minor version, assertion ID, issuer, issuer instant, conditions, advice, XML signature [8], statement, subject statement, authentication statement, authorization decision statement, and an attribute statement.

The SAML architecture has the following components: a credentials’ collector, an authentication authority, an attribute authority, a policy decision point, a system entity (subject) and a policy enforcement point. The authentication authority, attribute authority, and policy decision points make decisions basing on policies. A system entity logs in a domain and the authenticating authority authenticates the entity basing on the credentials supplied. The result of this process is stored in an authentication assertion. A reference to this assertion is created and it is in the form of a ticket and it is sent to the entity. The entity can supply this ticket to different websites and will be authenticated basing on the
ticket. If a website needs authorization information, the website contacts the attribute authority and requests for an attribute assertion. This assertion is sent to the policy decision point, which issues the authorization decision assertion. This assertion is then sent to the policy enforcement point on the website. The website will grant access to the requested resources depending on the authorization decision assertion.

![SAML Architecture Diagram]

**FIGURE 33: SAML ARCHITECTURE**

2.2 INTEGRATED SECURITY SYSTEM (ISS)

This is an integrated security system [9] of various individual security systems, which are often used as separate systems. The components of this system include a registration (X500) [19] system, a certification system, a smart cards system, and an authorization system as shown in Figure 34. This system is supported by a security platform, which has different security mechanisms, which can be updated or changed whenever necessary. The main functions of this system are to provide identification of users, users’ authentication, non-repudiation, confidentiality, delegation, information integrity, and authorization. Authentication is provided through public key certificates. Authorization and delegation are provided using attribute certificates [14]. An attribute certificate is a certificate that carries authorization and delegation information. It contains a reference to the authentication tokens for validation purposes. Non-repudiation is provided using smart card systems and signature schemes. Users in need of registration services, a smart card, a public key certificate, and authorization attributes usually identify themselves multiple times and perform registration procedure at four different administration stations in non-integrated security systems. In this system identification of users, verification of users’ identities and registration of users is done once per user and all relevant security data are shared among the four security sub-systems. The same administrator registers the
client, issues a digital certificate, and issues an attribute certificate and a smart card to the client. The administrator can visualize all the data and can perform updates and other management operations from the same interface. The system offers functional integration of data and security administration procedures and visual integration through a common security administration interface.

![Architecture of Integrated Security System](image)

**FIGURE 34: ARCHITECTURE OF INTEGRATED SECURITY SYSTEM**

### 2.3 The Challenges of an On-line Government Services

One of challenges of e-government according to [10] is providing user-friendly systems for e-government clients. Clients today in US are forced to keep multiple passwords that are needed just in a single session. The second challenge is that e-government in US [10] is depending on multiple systems from different private vendors. In some cases authentication systems of different forms, and authorization systems of different forms come from different vendors and administrators have to use different platforms. The third challenge is to provide multiple authentication schemes. Some services demand strong authentication while others demand simple authentication schemes. Today many government agencies are forced to use only one type of authentication for the different types of services. The forth challenge is that the security perimeter of the US government was formally “well defined as inside and outside” [10], but it is not the case today. This complicates the management of security of e-government because the security perimeter of the government is no longer well defined today. The reason for this change is the expansion of e-business technology, which makes the government deal with security in different platforms and in different applications like web services. The US government is planning to create a special net GOVNET [4] that will not be connected to the global Internet for government agencies. This is aimed at protecting government agencies from security problems that are present today in the Internet. It will be interesting to see how the e-government services will be provided to clients when e-government clients are using the normal global Internet while the government is using GOVNET that is not connected to the global Internet.
3 E-GOVERNMENT SECURITY SYSTEM

3.1 ARCHITECTURE OF THE SYSTEM

The system contains the following components: an e-government website, an integrated security system, a SAML server, a controller, an e-government client, an e-citizen system, an e-regional system and ministries’ systems as shown in Figure 35. The functions of the web site include directing e-government clients to different services, policy enforcements, protecting messages, informing the SAML server the required authentication and authorization types before accessing resources and before transactions, backup operations, and other administrative procedures. The integrated security system manages digital certificates, smart cards, attribute certificates, registrations, and policies. The ISS acts as an assertions’ authority [6]. The SAML server manages authentication assertions, attribute assertions and authorization decision assertions. The controller performs anonymity services. Anonymity can be provided when performing services like electronic voting, survey, e-democracy issues, and other issues.

FIGURE 35: ARCHITECTURE OF E-GOVERNMENT SECURITY SYSTEM

The controller performs operations like identifying and authenticating an e-government client. After user identification and authentication, the controller removes the original IP address and then sends the message to the desired destination servers with controller’s IP address as source [18]. Another function of the controller is to check the validity of requests. The controller collects credentials of clients. For every serious request, there is a denial of service cookie [11] that is a function of an IP address and a secret code of a client. This reduces non-availability (partially) problem of the e-government website.

E-citizen system offers a variety of public and classified e-government services to citizens. Public services require no authentication while classified services can require
simple or strong authentication with or without authorization. All transactions are protected using the configured security mechanisms. There is a policy file that specifies the types of authentication and authorization needed for each service. If a client desires to perform e-government services at a specific ministry, she will be directed to that ministry. Every ministry has a number of integrated security systems and SAML servers at different sections depending on the size of the ministry. Every ministry has its own policies basing on the sensitivity of the information and services it offers. E-regional is a system that deals with local e-government services. The regions or states are in turn divided into districts. All these regions and districts can have ISS and SAML systems to facilitate effectiveness in the management of services in local governments.

When an e-government client desires to access the e-government website, the controller collects credentials and sends them to the integrated security system. If it is the first time, the client performs identification and authentication procedures and if successful, she is registered in the directory. The information is shared by all e-government sub-systems. The client is then issued with a digital certificate, an attribute certificate [14] and a smart card if desired. A denial of service cookie [11] is sent to the client. If the client has already been registered, the controller checks whether the request is valid and then sends the credentials to the integrated security system. This system prepares authentication assertions, attribute assertions and authorization decision assertions. The assertions are signed by the integrated security system using XML signature [12] and then protected by XML encryption [8] and integrity. All the messages between the ISS and the SAML server are transmitted using the SOAP [7] protocol. The SAML server has to verify the signatures in the assertions from the ISS. The World Wide Web Consortium (W3C) has developed XML [15] Key Management Specification (XKMS) [16] for locating, validating and registering keys. This protocol is used by SAML to validate the keys used for signing and encrypting assertions from ISS. The reference to each assertion is in the form of tickets [13]. The tickets are then sent to the client who forwards the tickets to the e-government website. The website checks the validity of tickets with the SAML server before granting access. The client can use these tickets to access the resources on the different e-government servers without needing to sign in again. SAML provides single sign on. The decision to grant services will depend on the roles indicated on the tickets. The ticket that refers to the attribute assertion contains an attribute certificate [14] or just a username, a role and other attributes. The authentication assertion contains the following authentication tokens: a username, a challenge response value, an X509 certificate, a password or a combination of these.

3.2 SECURITY SERVICES

3.2.1 MULTIPLE AUTHENTICATION METHODS

This system supports simple authentication and strong authentication. The reason for supporting multiple authentications is that services have different levels of sensitivity and also to accommodate clients with different e-literacy levels. Services with low levels of sensitivity can be configured to require simple authentication. E-government services with high sensitivity levels can be configured to require strong authentication. Simple authentication can be password based, challenge-response based, or biometrics based. The default mechanisms for supporting password and challenge response in this system include Lamport’s hash and Encrypted Key Exchange (EKE) [11]. Lamport’s hash is a
password protocol in which a password is hashed \( n \) times and then sent to a server. The number \( n \) is specified in the policy file. One for every authentication reduces the number \( n \). When \( n \) is 0, a new password has to be set. EKE is a strong password protocol that bases on Diffie-Hellman [11]. EKE enables e-government clients and e-government websites to create session keys and mutually authenticate each other. Strong authentication bases on digital certificates and secret keys. Parties mutually authenticate each other by proving to each that they possess private keys and secret keys.

3.2.2 Multiple Authorization Methods
Authorization in this system is role based, identity based, or a combination of these types. Before checking whether a client is authorized to access a resource or to perform a transaction the client must be authenticated first. Authorization tokens have references that can be used to verify the identity of clients. Authorization bases on tickets and attributes certificates [14].

3.2.3 Multiple Non-repudiation Schemes
This system supports non-repudiation schemes with public key technology and also with secret key technology. The e-government website and the e-government client sign all the messages between them by using private keys. Providing non-repudiation using secret keys involves a third trusted party. In this system, the controller is configured as a default notary. However, it can be configured to use other trusted non-government agencies to act as third parties.

3.2.4 Multiple Integrity Schemes and Availability
This system supports multiple integrity schemes. It supports mechanisms that use secret keys as inputs and those that produce digests without taking keys as inputs. The default systems in this system are Secure Hash Algorithm -1 (SHA-1) [11] and HMAC [11]. SHA-1 takes a message and produces a message digest that is 160 bits long. HMAC takes a message and a secret key and creates message authentication code of 128 bits or 160 bits long. Availability is partially provided though the use of denial of service cookies.

3.2.5 Audit, Privacy, Confidentiality and Anonymity
All the signed transactions between the e-government websites and e-government clients are stored in the directory and in a backup database. Clients and e-government servers sign all the transactions. Transactions that are not signed are not processed and they are sent back to clients for signing. Timestamps are attached to all the transactions. These records are kept in this way to be used in conflict resolution and accountability matters. All the messages between e-government clients and e-government websites are protected by using the configured protocols. The default protocol is Secure Socket layer (SSL) [17]. In addition, in this protocol client authentication is mandatory in this security system. Anonymity is provided in cases of e-voting, survey projects and other specialized transactions. Anonymity is provided [18] as described in section 3. Client’s data will be protected in accordance with the personal information protection laws of the government.

3.3 Advantages and Validation of the System
This system enables a government to control of all the security services and does not depend on different private vendors as discussed in the related work section 2.3. It provides multiple authentication methods, authorization schemes, privacy protection methods, information integrity schemes, and non-repudiation methods. This makes
services with different levels of classification require different types of security services. This security system is platform independent. The system is scalable. The administrator can manage public key certificates, smart cards, authorization attributes, and users’ registration from one interface of the ISS, which is simple and efficient. This system is using standards and mechanisms that have been analyzed and tested by experts. X.509 certificate and strong password protocols are used for authentication for sensitive e-government services. The system is using multiple authentication methods and in some cases, it may be recommended to use authentication methods that are not very strong to accommodate clients that have low e-literacy levels, but this will depend on the government policies. The same applies to authorization schemes. Standardized algorithms provide digital signature schemes and encryption schemes and they can be replaced whenever necessary. The security platform supports updates and removal of undesired mechanisms. This security system is using standards like SAML, XML, and SOAP to provide platform independency. The system can be built-in in any e-government systems and it can also be integrated in already existing e-government systems.

3.4 LIMITATION OF THE SYSTEM

The system does not provide Denial of service security service. It does not support e-government wireless services’ security. The system has not yet been implemented and so there are no results on performance. It is assumed that the government using this security system supports the public key infrastructure.

4 CONCLUSION

This work has highlighted security issues that need to be considered in designing e-government security systems. E-government services have different levels of sensitivity and they should be accessed through multiple authentication and authorization methods. The e-government security system should accommodate all clients regardless of their e-literacy levels. The system can be applied to any e-government architecture with minor adjustments. Future work includes extension to wireless technology, implementation of the system, and analysis of the system’s performance.

REFERENCES


PAPER IV
ABSTRACT
Everything that we see can be changed. Internet is vulnerable because it was not designed as a whole system. Changing the way we think and approach the development of Internet can change this. Initial development of the Internet and other systems focused only on computer technology and communications protocols. Many systems are not secure today because most research has concentrated on securing parts of the systems. Hence, we can change this by viewing security of Internet and other systems holistically, by focusing not just on technology and protocols but by considering system’s environments, people using the systems, future of systems and other factors. In this paper we view and approach security of systems holistically. We discuss and suggest a methodology of securing systems based on the paradigms of the Immune system and the Systemic-Holistic approach. The Immune system is used to protect human bodies from for instance different types of viruses. The Systemic-Holistic Approach views and studies a system as a whole or in details at the theoretical, design, or the implementation level. It takes into considerations technical and non-technical aspects and the system’s environment. The generic security framework has been created for using functions inspired by the immune system and the Systemic-Holistic Approach paradigms to secure systems. The framework contains the deterrence, protection, detection, response and recovery sub-systems. These sub-systems will be generically protecting both at the border and internally in the system. This methodology will improve the way we design security systems by generically considering different factors and people using the system.

KEY WORDS
Immune system, Systemic-holistic, negative selection algorithm, clonally selection algorithm, deterrence, protection, detection, response, recovery, intrusion detection, software agents, and generic security framework.
1 INTRODUCTION

This paper describes a generic security framework aimed for sorting in functions inspired by the immune system and the Systemic-Holistic Approach paradigms useful to secure systems. Internet and computers are vulnerable because of the assumptions initially directing the developments of computers and communications protocols. In addition, it was overlooked that users have various reasons for communicating. To handle the security problems it has been assumed that all systems, static and dynamic, can be correctly verified with formal methods. [See for instance 1]. To verify formally that a static system does what it is supposed to do is expensive; to formally verify that dynamic systems are correctly implemented with formal verification methods is impractical [1]. In addition, it has been assumed that: security policies can be performed and followed perfectly; that programs, large and small, can be perfectly implemented; and that systems can be perfectly configured [1]. However, all these assumptions are not correct [1]. Conclusions to be drawn are that formal verification methods for systems are not enough and other or complementary methods are sought for [1, 2]. It is challenging to verify that static and dynamic systems are secure with the current technology. Therefore, we have to find other ways of designing security systems by generically considering as many factors as possible. This includes studying how nature protects natural living systems. In this work, we discuss a framework based on the mentioned paradigms, which eventually would inspire an adaptability view on securing systems. We do this because we think time might be ripe for marrying the Systemic-holistic approach, which has been used with us as a base to understand security in relation to IT since the mid-1980’s [2], with the Immune system paradigm [1, 14]. In addition, some other scientific paradigms/approaches are appearing to underline needs for including nature-oriented views into traditional engineering fields [11]. The Systemic-holistic bases on the General living Systems Theory [16, 8, and 2], Cybernetics [17, 10] and General Systems Theory [16, 15, and 2]. The approach is used for studying, investigating, designing security systems, analyzing security systems in three dimensions of a system as one whole system as discussed in section 2.1. The human’s immune system is distributable, multi-layered, autonomous, adaptable, dynamic, which seems very attractive to security systems. A number of researchers [3, 1, and 9] have developed computer security systems based on Immune systems. However, the human’s immune system cannot be directly applied to computer systems because human bodies are made of cells, most of which are created in the bodies, while computers consist of hardware and programs that can come from different sources. This implies that the analogy has to be carefully studied.
2 Basic Principles

2.1 Systemic-Holistic Approach

The Systemic-holistic Approach, SHA, was developed by [2] for analyzing and studying security problems. It bases on General systems theory, General Living Systems Theory and Cybernetics. Biologist Ludwig von Bertalanffy developed General System’s theory in 1956 [17, 2]. He understood the need for having a common research theory for guiding researchers in multi disciplines. The General Systems movement identified laws and principles applicable to various disciplines and which could be used for systems in general. James Miller developed the General Living Systems Theory was [16, 8]. Living systems are in seven categories [16, 2]: they can exist as a cell, as an organ, as an organism, as a group, as an organization, as a nation and as supranational (as European Union). According to Miller, the chain of complexity can be built on 19 generic critical subsystems. Out of these 19 subsystems [16, 8], eight deals with processing matter/energy, nine deal with processing information and two subsystems deal with processing both matter-energy and information. This theory helps researchers to link reality and theories. Cybernetics was first defined by a mathematician Wiener [18, 10] as a science of communication and control in animals and machines.

The Systemic-Holistic model is composed of two components: a systemic module and a three dimensional framework [2]. The dimensions in the framework include the levels of abstraction, the context orientation and the content area [2]. The dimension of the levels of abstraction consists of design or research; theory or model; and physical construction. The context orientation dimension can be geographical space and time bound. The content dimension has the following components: technical issues and non-technical issues. Technical issues include processing, storing, communication, collecting and displaying information. Non-technical issues include operational, managerial, legal, ethical, social and cultural. The Systemic-Holistic Approach is used for analyzing and studying security problems, for governing design, operation, management and evaluation of secure systems. This approach can be used to study a system as a whole and the environment of the system and in three dimensions. Different aspects of the security system can be defined, investigated, evaluated and analyzed at any design, theoretical or construction level, and in any time dimension: near future or distant future; and in any environment.

2.2 The Human’s Immune System

The human’s immune system, IM, is protecting the body from various bacteria and viruses. Most of the information in this section comes from [3, 1, and 4]. The Immune system consists of two main layers: the passive and adaptive layers. The passive layers consist of the skin, membranes, pH (potential Hydrogen of a liquid), temperature and inflammatory responses. The adaptive layers consist of cell mechanisms. All the organisms belonging to a human body are labeled as ‘self’. Those organisms that are identified as “non-self” are detected and destroyed by the immune system. The adaptive immune system reacts dynamically to foreign cells. There are two types of human cells that are used in detecting foreign cells. These are the B-cells and T-cells. B-cells are generated in the Bone marrow while T-cells are generated in a Thymus. T-cells are in turn classified as helper T-cells and killer T-cells. Helper T-cells help the B-cells detect
foreign cells hidden inside the human cells. Killer T-cells kill foreign cells. B-cells recognize foreign cells and create antibodies with the function to be attached to these foreign cells. Before B-cells are released from the bone marrow, they have to be tested whether they can detect correctly. They pass a stage called negative selection in which all B-cells that detect the ‘self’ labeled organisms are disqualified and deleted. Those B-cells that pass the test are released into the body. When a foreign cell is detected, detecting B-cells to remember the detected foreign cell creates separate memory cells. Memory cells store information about foreign cells that were detected in the past and these memory cells have longer life spans than normal B- and T-cells. T-cells are also tested using negative selection before being released from the Thymus. Different B-cells and T-cells detect different types of foreign cells. T-cells and B-cells undergo a process called mutation in the gene library. The gene library contains all the genes that are used to create different types of cells. The gene library continuously adapts and creates blueprints for making better antibodies that detect more and more varieties of foreign cells. The gene library evolves in a process called clonally selection. Those cells that have a higher detecting capacity are cloned. The genes are used to maintain diversity of antibodies by generating different gene expressions.

The human immune properties have the following principles that can be applied in designing better security systems:

Distributed – cells detect the presence of infections locally without any coordination (this can be modeled by having mobile agents act as cells).

Multi-layered – multiple layers are combined to provide overall immunity. (This is already applied in the security architectures).

Diversity – with diversity, vulnerabilities in one system are less likely to be widespread. (This can be achieved by having agents doing a variety of actions).

Disposability – no single system is the most important and any cell can be disposed. Cell death is balanced by cell production. (The technology is not yet ready to implement this feature but at the process / agent level, it is possible to implement this).

Autonomy – the immune system does not require outside maintenance or management. It autonomously classifies and eliminates foreign cells and it repairs itself by replacing damaged cells (This behavior is suitable but its implementation is challenging as technology still is not ready, though it could be modeled so that three or five agents vote for a decision).

Adaptability – the immune system is able to detect and to learn to detect new foreign cells and retains the ability to recognize previously seen foreign cells through immune memory. This feature is not new it in computer systems, though determining that a certain program is malicious with 100% is a hard problem.

No secure layer – no layer is considered more secure than the other is.

Dynamically changing coverage - The immune system cannot produce a large enough set of detectors at any moment, so it maintains a random sample of its detectors that circulates throughout the body. This is because there are approximately $10^{16}$ foreign cells and these have to be distinguished from approx. $10^5$ ‘self’-cells.

Identity via behavior – identity is also proved through the presentation of a behavior (similar to intrusion detection).
2.4 DIGITAL IMMUNE SYSTEM

Digital immune systems based on the human immune system have been developed. Symantec developed one of these systems [7]. It is used in antivirus systems. The system has a virus detection system, an administrator system, a gateway and a virus analysis center. When a virus is detected on the client side, it is sent to the analysis center through the administrator system and the gateway. The administrator system keeps the latest definition files of viruses. It also monitors the samples and results of analysis to and from the analysis center. The administrator system also updates clients’ anti-virus programs. The gateway is responsible for securing the network between the client and the analysis center. It controls the network to make sure that the network is not flooded. It is also making sure that only one copy of every sample is sent to the analysis center. When samples of viruses arrive at the analysis center they are put into different classes depending on the languages, file types, versions of viruses and behaviors. The supervisor at the center allocates samples to different machines and human analyzers. The results of the analysis are used to create definition files for different operating systems and for different versions. The definition files are then tested to see if they detect viruses, disinfect files and verify signatures and so on. In some cases, the results are not enough to create definition files because the technology of detection is not available for that type of files. This digital immune system is however not effective in detecting polymorphic viruses and power point viruses.

2.5 GENERATION OF SOFTWARE AGENTS

In this work, we are using software agents to perform different tasks during deterrence, protection, detection and other actions. According to [22], “An agent is an encapsulated computer system situated in some environment and capable of reactive, pro-active, and autonomous action in that environment in order to meet its design objective.” An agent consists of three main components [23]: header, code, and a database. The header contains identity of the agent, agent attributes, signatures, travel paths, level of trust, ownership and other related information. The code section contains a system of programs performing the specific tasks of the agent. The database contains internal and the collected data while traversing in different environments. Agents are generated from an agent platform like Java Agent Development Framework (JADE) [24]. An agent has to be tested to see if it detects correct. There are a number of algorithms for testing and cloning agents of the digital immune systems, but in this work, we discuss only two algorithms.

2.5.1 NEGATIVE SELECTION ALGORITHM

In the first stage of this algorithm, normal behavior of programs, users and processes of the system is defined. In the second phase, patterns of this normal behavior are created. In the third phase, detector agents are created. These agents are then released to monitor the normal programs, users, network traffic or processes. Those agents that detect the normal behavior patterns are deleted, because they are supposed to detect only abnormal patterns. Those detector agents that do not detect the normal patterns are kept.

2.5.2 CLONALLY SELECTION ALGORITHM

This algorithm [3] is shown in Figure 36. The immature agents that passed the test during the negative selection algorithm are tested using abnormal behavior. Those agents that
pass the test are considered mature and they are released to monitor in real environments. These agents are also monitored to check whether they detect anything. Those agents that do not detect anything are deleted. Those agents that detect abnormal behavior are kept. In every agent, there is a parameter for counting the number of detections, age of the agent and also the type of detections. When the number of detections is less than a specified threshold, the age of the agent is checked. If the age is, more than a specified life span the agent is deleted. If the age is not more that the life span, then the agent will continue to monitor. When the number of detections is more than a specified threshold and if a human security officer acknowledges that the detected are foreign cells, the agent is cloned and the abnormality is deleted.

3 Methodology of Securing a System

3.1 System Model

According to the Systemic-holistic, a system can be viewed and analyzed at the model, design and implementation levels. In this section, we analyze the model of the system, which is shown in figure 37. The design of the generic security framework will be described in the methodology of securing a system section. The model bases on the Systemic-Holistic Approach and the human’s immune system. From the Systemic-holistic approach, we apply the principles: analysis of the technical and non-technical aspects; analysis of the environment in which the system will be operating; generic view and time factors. The technical aspects include how to securely store, process, transmit, collect and display information. In this regard, we consider technology, software and engineering issues. We check whether the current technology is ready to securely store, process, transmit, collect and display information. Software is concerned with the analysis of security services in the system. It is also concerned with the interfaces, the speed of the operations.
Non-technical aspects include operational, managerial, legal, ethical, social and cultural, people, and information. An analysis has to be made to check whether people can accept the system. Systems interact with people and it is not easy to separate people from operational procedures, managerial, cultural, ethical, social, legal issues. There are different laws in different countries. In some countries, a signature can be accepted as evidence in a court only if it is qualified. This means that one can prove the identity of the signer and prove that only he/she signed. The law requires that the keys involve in signing be stored in safe tokens like smart cards. While in other countries, it is sufficient to prove that there was an intention to sign some information.
Information can exist in different forms: as protected or unprotected signals; as unprocessed and protected or unprocessed-unprotected message: as processed and protected or processed and unprotected message: as protected or unprotected knowledge. Knowledge refers to information that has some meaning to the reader. Information can be further classified as being ethical, legal, according to the security policy, as politically correct, in accordance to a specified culture. Information could be further classified into sensitivity levels (green, orange, red, etc), quality of service required (high, medium, low; emergency, etc). As [13] points out ethical, laws, policy, standard operation procedure headers can be added to information and messages have to be approved before being sent to other parties. Considerations have to be made regarding time, environment, political and security policies. With time, technology changes and so considerations have to be made about how future can affect the system. Room has to be given for extensions of the system. According to [20] “The observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the near future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months.” This law has so far proved to be working even though the software is not developing at the same speed as hardware. It is possible to design many transistors theoretically, but it is completely another issue to have that many transistors in one chip. Another example is that PC manufacturers are aware that PCs have to interact with TV sets, stereos, mobile and non-mobile phones and other home and office appliances. If these factors were considered by PC manufacturers, from the beginning, the current PCs would be accommodating these principles and the prices of the PCs would have been relatively low. However, manufactures have to redesign PCs to meet the new requirements. In the near future, the PCs will be acting as databases for storing stream videos, pictures, music and other media. These media will have to be transferred to TVs and stereos. This can be done using wires or without wires and so, the PCs have to be equipped with the capability of doing this. These examples and Moore’s law show that we can predict future applications in today’s system designs. From the Immune system, the following principles are applied in the model: Adaptability; autonomy; multiple layers, identification; memory; diversity; distribution; dynamic coverage as shown in Figure 37. The principles in this model, Figure 37, that are based on SHA and IM are combined to form a system with five main sub-systems: deterrence, protection, detection, response, and recovery.
3.1.1 Deterrence Sub-System

Deterrence sub-system is aimed at scaring off attackers (like how a cat scares off attackers by increasing its size and through fierce screams). When criminals plan to rob a bank in the physical world they do surveillance of the bank to determine whether it is possible to attack, take what they want and get out without being caught and without living evidence. In the digital world, the attackers do more or less the same. Before would-be attackers intrude a system, they do some kind of scanning to determine the operating systems and their versions, the ports that are open, the applications and versions that and on the victim’s system. Then the attackers do possibly also social engineering to understand the architecture of the system. There are many ways of doing this, from just asking the people working there to listening to conversations of system administrators there or secretaries working there. It is surprising how employees like to talk about their jobs during lunches and even dinners! From the results of scanning and social engineering, the criminals decide whether it is possible to attack the system, and get out without being caught and without living evidence. The attackers will not attack a system if it is considered too risky. Therefore, there has to be means of scaring the would-be attackers from attacking a system. The functions of the deterrence sub-system include: adapting to the new and unknown surveillance methods; organizing training to prevent social engineering; monitoring surveillance attempts; redirecting attacks to specialized environments (like honey pot system); handling replies to scanners (returning nothing, a warning, etc); auditing; tracing scanning sources.
3.1.2 Protection Sub-System
Protection is a sub-system for guiding the territory of a system and its entities. Home cats establish territories, a special place on a sofa, and put rules. Wild cats mark territories by using peculiar identifying items like natural scents. The protection sub-system provides the following security services: authentication, integrity, confidentiality, non-repudiation and authorization of entities and information during storage, transmission, processing, collection and display. Other principles of this sub-system include adaptability in which the system learns new protection ways by applying the latest standards; organizational, like configurations in accordance to the security policy; semi-autonomy in which the system makes some decisions without involving the management of the system, but the critical decisions must involve the system management. Another feature is multi-layer protection, where protection is provided at the boundary of a system and inside the system and sub-systems. Partial distribution – this is a feature in which protection is done locally while in some cases protection is coordinated.

3.1.3 Detection Sub-System
This sub-system is responsible for detecting the abnormalities, storing and protecting the log of events, analyzing the events, monitoring, management and interacting with other subsystems. Other principals include multiple-layer detection, adaptability of new ways of monitoring and detecting, semi-autonomous, and dynamic coverage, sending reports to the database and the administration. The normal behaviors of outgoing and incoming messages are defined. Software agents are used to detect the abnormal behaviors of incoming and outgoing messages, as cells are used to detect foreign cells in immune systems. All the entities that belong to a system are labeled as ‘self’ by being given special identities and being registered in a database. Software agents monitor a system to discover the non-self entities in a system.

3.1.4 Response Sub-System
This sub-system is responsible for incident management. It classifies incidents into false alarms, minor and major incidents in accordance with the security policy of the system. The response and speed of reaction depends on the classification. It makes decisions on how to respond for every incident. The decisions include disconnecting the affected sub-system from others, slowing, shutting down or restarting the affected system, etc. The sub-system also sends reports to the affected users, to the database and to the administration. Other functions of this sub-system include managing patches and adaptability, tracing the attack, mitigation of the attack and so on.

3.1.5 Recovery Sub-System
The recovery sub-system is for bringing an attacked system back to normal. The functions of this sub-system include managing back-ups, re-installing the programs, periodic and emergency vulnerability testing, restoring a system from back-ups, collecting and protecting evidence, fixing the vulnerabilities. The agents can help to define and test business continuity plans. This process can be very expensive and takes much time if done manually. At every moment, three types of the state of system and sub-systems and operations are stored: the original state the intended state and the actual state. When an incident occurs, the system can go back to the original state and flush all the rest. This feature could be partially or wholly implemented depending on the current technology and other back-up resources.
3.2 GENERIC SECURITY FRAMEWORK

The generic security framework is composed of five main sub-systems: Deterrence, protection, detection, response and recovery as shown in Figure 38. Every sub-system can be implemented using human, hardware or software [13] or combined, depending on: the decisions that have to be made; the time of decision; and also the sensitivity of the environment like whether it is for a nuclear plant, a military, a bank and so on. How much effort should be spent [13] on deterring, protecting, detecting, responding, recovering and the interaction with people depends on the environment. One telecommunications company uses 0% in deterrence, 70% in protection, 5% in detection, 5% in response, and 20% in recovery in form of insurance fees. The dictatorship governments use approximately 80% of the resources in deterrence; the rest 20% is used for protection, detection and response. This should be specified in a policy file. One example could be to put 10% of the effort on deterrence, 50% on protecting, 20% on detecting, 10% on response, and 10% on recovering.

The Immune system uses cells to detect viruses. This framework uses software agents to perform different specialized tasks. The agents are generated in the agent generation library using an agent platform like [24]. Every sub-system requests the agents it needs from this library. Agents are tested and sent to the requesting sub-system by using negative selective and cloning algorithms like those described in [3]. All the sub-systems have a controller, an inputs section, a processing section and an outputs section. The
deterrence controller interacts with the inputs, process and outputs sections. It also communicates with the protection sub-system and the agents’ generation library and database.

When surveillance attempts come to a system, they pass through the deterrence controller. The controller analyses them and sends them as inputs to the process or to the special analyzer for further analysis. The controller also sends these incoming surveillance attempts to the database. Before being sent to the database and to the special analyzer, the incoming surveillance attempts are encapsulated. All the other sub-systems have feedback mechanisms with the aim to learn and improve the processing. All the sub-systems interact with the agent-generating library and with each other to share the knowledge needed to learn and improve processing. There are three types of feedback mechanisms [18]: first order second-order and third order. The first-order mechanism does not improve a process. The second-order has a memory and can help in improving a process but it has a limited number of unchangeable feedback alternatives making it less dynamic. Third order has memory, many feedback alternatives and is more dynamic than the other alternatives. In this framework, we aim for the third-order feedback mechanism. The controller combines different inputs; modifies inputs; stores different types of inputs; and manages different operations for improving processing in every sub-system. For every stage, the processing can have a number of sub-processes like decision-making, searching, memory unit, selecting, re-combining different factors [2], etc.

Every sub-system has generic functions, which can be replaced or updated whenever necessary. The security level of every system bases on three types of factors: users of the system; the system policy; and the policy of the environment in which the system is located. This generic security system sets a minimum level of security for all systems regardless of the environment the system is running in. This level can be increased depending on the type of environment, the type of users and the system policy.

3.3 LIMITATION OF THE SYSTEM

The framework has not been implemented and so there are no results of performance yet. Some aspects of this framework may not be wholly implemented by today’s technology and it is highlighted as a challenge to the researchers to come up with the technology for implementing them.

4 CONCLUSION

The generic security framework provides a methodology for securing systems. It bases on Systemic-Holistic Approach and the Immune system. Security is not only about technology but also it about people using the technology and the environments in which the systems are operating. This paper has suggested a methodology of generically viewing security systems. Future work will include implementing the framework, which we have just started working on. Future work will also include developing algorithms that are more effective for the agents.

REFERENCES


PERMISSIONS

Jeffy Mwakalinga and Louise Yngström are the authors of this paper. This work is original and does not violate any copyrights, rights and privacy of others. We retain the right all or part of this paper in our future work. We grant the ISSA 2005 organizers the right to publish this paper in the ISSA 2005 proceedings
PAPER V
Securing Mobile Agents for Survivable Systems

Jeffy Mwakalinga, Louise Yngström
Department of Computer and System Sciences,
Royal Institute of Technology/Stockholm University, Kista, Sweden
Fax: +46 8 703 9025 Tel: +46 8 16 1721
[jeffy@dsv.su.se, louise@dsv.su.se]

ABSTRACT
We have what we have today because of the decisions and actions that we made in the past. Our lives and computer technology in the future will depend on the decisions and actions we make today about them. In future, it is very likely that we will be walking with Web servers in mobile phones, PDAs, or MP3 players or in whatever devices. There will be so much information from banks, insurance, government, health, nursery, and schools requiring instant response that will necessitate people to carry Web servers. People will be required to make different authorization and privacy decisions, which cannot wait. The amount of information and actions can necessitate the need for helping hands in the form of mobile software agents, which are forms of non-human computer secretaries. These can be used in diverse business areas like auctions, contract negotiations, stock trading, and money transfer. These agents will need to carry information and perform transactions securely. How do we secure software mobile agents? In this paper, we describe ways of securing mobile agents for survivable systems. We describe ways of protecting mobile agents and the information that they carry.

Keywords
Software mobile agents, survivable systems, agent platforms, agent certifier, and accountability.

1 INTRODUCTION
The aim of this work is to study ways of securing software agents, which are used to perform different tasks during deterrence, protection, detection, response, and recovery services in the survivable systems. According to [14], “An agent is an encapsulated computer system situated in some environment and capable of reactive, pro-active, and autonomous action in that environment in order to meet its design objective.” An agent consists of three main components [3]: header, code, and a database. The header contains identity of the agent, agent attributes, signatures, travel paths, level of trust, ownership and other related information. The code section contains a system of programs performing the specific tasks of the agent. The database contains internal and the collected data while traversing in different environments. Agents are generated from an agent platform like Java Agent Development Framework (JADE) [15].

There are already software agents for different purposes. When one wants to find the best, ticket through the Internet to fly to a specified location it can take a lot of time and energy. To save time and
energy one can send a software mobile agent instead to do the job. Manufacturers of different products can negotiate prices, delivery of goods, terms of delivery and other services with supplies through their respective agents [4]. Other services suitable for mobile agents include network management, intrusion detection, testing security of networks and so on. The use of mobile agents reduces network traffic because they perform actions at agent servers reducing the request/reply messages in traditional client-server transactions. Mobile agents have to perform transactions and carry information securely. In this paper, we describe how to secure mobile agents for survivable systems. Survivable systems are those that are required to run all the time like air traffic systems, banking systems, medical systems, radars, and different business systems. To be able to run all the time they are required to have fault-tolerance measures. The methodology for building security in survivable systems is described in [13]. The Systemic-Holistic Approach [2] and the Immune system [1] paradigms are used as foundations in building security in survivable systems. The Systemic-holistic paradigm is used for studying security of a system as a whole by considering the system, the environment of the system and by considering technical and non-technical factors. The Immune system is used for protecting human bodies from different viruses and helps humans to survive in different environments. We study how living systems, particularly humans, survive in open environments and apply the features of the immune system to make systems survive. We use mobile agents in survivable systems and there are a number of security threats for mobile agents.

1.2 SECURITY THREATS FOR MOBILE AGENTS

Before addressing security, we need to understand the different security threats for mobile agents. The parties that are involved in transactions include agents and agent servers (platforms). An agent can attack an agent server, an agent server can attack an agent, an agent can attack another agent, an agent server can attack another agent server, and other outside attackers can cause security threats to the agents and agent servers [4].

Attacks from agents to agent servers include masquerading, denial of service and unauthorized access. Masquerading is a feature of an agent to pretend being another agent in order to gain unauthorized access of resources or to damage the reputation of the other agent and the owner of the agent. In denial of service, an agent disrupts the services offered by the agent server by running programs that heavily exploit system vulnerabilities of an agent server to degrade the performance of the agent server. Agent servers accommodate many mobile agents from different organizations. Some of the agents may try to access information on the agent server that they are not authorized to.

Attacks from agent to agent include masquerading, denial of service, repudiation and unauthorized access. An agent can exploit the weaknesses of another agent and steal its identity. The agent can then masquerade and perform any actions under other agent’s identity. Agents can launch denial of service attacks against each to prevent them intentionally from finishing their tasks.
An agent can cheat another agent to sign a bad contract and then repudiate later from having done that. An agent can change the information or programs in another agent if they are not secured. An agent can even call another agent’s methods in an attempt to change the behavior of the agent.

An agent server can attack a visiting agent in many forms: by masquerading, by denial of service, by reading agents information or by modifying agent’s information and programs. An agent can be cheated into paying higher prices for items that are being sold by an agent server. Outsiders can attack agent servers and agents by masquerading, unauthorized access, denial of service and by coping agents or parts of the agent messages and replaying them. After discussing security threats, we will discuss security requirements for mobile agents.

1.3 Security Requirements for Mobile Agents

According to [4] security requirements on agent frameworks include confidentiality, integrity, accountability, availability and anonymity. Confidentiality is required so that all the classified information can be kept secret at agent platforms and while being carried by the agents. Communications between agents and between agents and agent servers should also be confidential. All messages’ flow should be kept secret so that the listeners should not be able to find out the number of messages nor analyze the traffic between agents and platforms. Even the location of agents should be confidential. Agents can choose to be public and in such cases, they should be allowed to be. The activities of agents should also remain confidential so the audit logs of their activities must be protected.

Integrity of agents’ code, state, internal data and collected data should be provided to ensure that unauthorized modification of code, state and data is not done. Agents should be able to detect when modification of their code, state and data is done. The agent server must also be provided with integrity. Access control should also be addressed so that only authorized agents should be able to access and perform the tasks on agent servers. Changes to agent servers should be made only by authorized users.

Accountability, according to [4], includes identification, authentication and audit of human users, agents and agent servers. This includes maintaining records of security related events of user/agent name, access to objects, time of access, type of event, success or failure of event. Audit logs will force users and agents to be accountable for their actions making it difficult for them to deny having performed the actions. Audit trails of agents should also be kept to help tracing activities in case of errors. Agents and agent server must authenticate each other before performing any transactions. Authentication could be strong or simple, depending on the classification of transactions. When agents are accessing public information, agent servers may not require any verification of identities of agents.

Availability of information and services to mobile agents must be ensured. The agent servers must support simultaneous access, allocate resources fairly, be able to recover from different failures and so they should have fault-tolerance measures. Agent servers should scale and be able to handle requests from many agents. When the agent servers are
not able to provide this service, they should notify agents about it. Denial of services attacks from malicious agents or other sources on the agent servers should addressed. Anonymity is another security requirement for mobile agents. This requirement is challenging to meet since some transactions require participants to be strongly authenticated before performing them. The agent server should have a balance of the need for the agent to be anonymous and the need for the platform to hold the mobile agent accountable for its actions. The agent server can keep the identity of an agent and its actions secret from other agents as long as the agent is behaving in accordance to the policies and security requirements of the agent server but when the agent crosses the red line it will be revealed to other agents.

1.4 ORGANIZATION OF SECTIONS
Section 2 covers related work. Section 3 describes the security architecture of survivable systems. Section 4 discusses agent security. Section 5 briefly discusses conclusions.

2 RELATED WORKS
In [3] a comprehensive security infrastructure for mobile agents is described. The infrastructure provides authentication, authorization, integrity, accountability and non-repudiation. Authenticity of agents is provided by giving identities to agents. The Agent identity has static, dynamic identity and other specific identities. Static identity comprises of agent author’s ID (author’s certificate), agent owners ID (owners certificate) and agents name. Dynamic identity consists of agent home ID and time of launch. To verify identities one verifies the certificates. Authorization of agents is provided through agent attributes, which contain level of trust, agent task specifications, constraints of agents, agent owner credentials. Constraints on agents include expire-time, maximum size, whether an agent can create children, and others extensions. Integrity is a security service for making sure that information is not modified when on storage or on transmission, Integrity of agents and agent servers is provided through digital signatures. The signatures that every agent must have include agent authors, agent owners, trusted appraisal’s, privilege authority’s, sender’s, agent server’s signatures. Confidential information that is carried by agents is kept secret from other agents.

FIGURE 39: MOBILE AGENT COMPUTING MODEL
The lifecycle of an agent includes creation, owning, launching, traversing, hosting and returning home as shown in Figure 39. The agent developer creates an agent signs it and attaches the digital certificate. The agent is then sent to the trust appraisal that verifies the signatures, tests the agent and then puts a level of trust on the agent. She signs the agent and puts her certificate. The agent is then sent to the owner who had requested it. The owner verifies the
signatures of the agent developer and the trust appraisal. If successful, she accepts the agent. The owner assigns agent identity to distinguish it from other agents.

Before launching the agent, the owner writes specifications on the agent, gives constraints to the agent of lifetime, maximum size and other specified properties. The owner then assigns the home address, destination server, time of launch. She then signs the agent, seals it with the destination server’s public key, and sends the agent.

The destination server opens the seal, verifies the signatures of the author, trust appraisal and of the owner. If verification is successful, she accepts the agent. The server-hosting agent protects its information that is classified from the visiting agent. The server monitors the actions of mobile agent. Information collected from the agent server is sealed by the owner’s public key and then it is signed. The hash of the state of the agent is sent to the state server. The agent can then be sent home or to another agent server and the procedure before sending an agent is the same as when the owner was sending the agent to the destination server.

When the agent arrives home to its owner, the signatures are verified the state of the agent is checked. If something has gone wrong, the owner extracts hashes of states from the state server and traces the whole communication. This system provides most of security services in accordance to the security requirements, which were discussed in sections 1.3, confidentiality, integrity and accountability. The limitation of this system is that it does not provide anonymity and availability requirements.

3 SECURITY ARCHITECTURE FOR SURVIVABLE SYSTEMS

In [13] we developed a methodology for security survivable systems and the architecture for these systems is shown is Figure 40. The components in the architecture of survivable system include the deterrence, protection, detection, response and recovery sub-systems. It also includes an administration component containing the agent generation library, a system manager, a database, an integrated security system, special analysis component and the system’s fault tolerance manager. The fault tolerance manager detects errors, assesses the damage, and confines the damage, performs error recovery measures, does fault treatment measures, locates the errors and performs measures for continued service. Every sub-system has sections: inputs, process, outputs, and fault tolerance manager. The sub-systems also have memory and feedback mechanisms for analyzing and modifying inputs when necessary.

3.1 DETERRENCE SUB-SYSTEM

The deterrence sub-system is aimed at scaring off attackers (like how a cat scares off attackers by increasing its size and through fierce screams). When criminals plan to rob a bank in the physical world they do surveillance of the bank to determine whether it is possible to attack, take what they want and get out without being caught and without living evidence. In the digital world, the attackers do more or less the same. Before would be attackers intrude a system, they do some kind of scanning to determine the operating systems and their versions, the ports that are open, the applications and versions that and on the victim’s system.
Then the attackers do possibly also social engineering to understand the architecture of the system. There are many ways of doing this, from just asking the people working there to listening to conversations of system administrators there or secretaries working there. It is surprising how employees like to talk about their jobs during lunches and even dinners! From the results of scanning and social engineering, the criminals decide whether it is possible to attack the system, and get out without being caught and without living evidence. The attackers will not attack a system if it is considered too risky. The functions of the deterrence sub-system include: adapting to the new and unknown surveillance methods; organizing training to prevent social engineering; monitoring surveillance attempts; redirecting attacks to specialized environments (like honey pot system); handling replies to scanners (returning nothing, a warning, etc); auditing; tracing scanning sources.

3.2 PROTECTION SUB-SYSTEM
Protection sub-system has measures for guiding the territory of a system and its entities. Home cats establish territories, a special place on a sofa, and put rules. Wild cats mark territories by using peculiar identifying items like natural scents. The protection sub-system provides security services: authentication, integrity, confidentiality, non-repudiation and authorization of entities and information during storage, transmission, processing, collection and display. Other features of this sub-system include adaptability in which the system learns new protection ways by applying the latest standards; organizational, like configurations in accordance to the security policy; semi-autonomy in which the system makes some decisions without involving the management of the system, but the critical decisions must involve the system management. Multi-layer protection is a feature where protection is provided at the boundary of a system and inside the system and sub-systems. Another feature is partial distribution – in which protection is done locally while in some cases protection is coordinated.

3.3 DETECTION SUB-SYSTEM
This sub-system is responsible for detecting the abnormalities, storing and protecting the log of events, analyzing the events, monitoring, managing and interacting with other subsystems. Other features include multiple-layer detection, adaptability of new ways of monitoring and detecting, semi-autonomous, and dynamic coverage, sending reports to the database and the administration. The normal behaviors of outgoing and incoming messages are defined. Software agents are used to detect the abnormal behaviors of incoming and outgoing messages, as cells are used to detect foreign cells in immune systems. All the entities that belong to a system are labeled as ‘self’ by being given special identities and being registered in a database. Software agents monitor a system to discover the non-self entities in a system.

3.4 RESPONSE SUB-SYSTEM
This sub-system is responsible for incident management. It classifies incidents into false alarms, minor and major incidents in accordance with the security policy of the system. The response and speed of reaction depends on the classification. It makes decisions on how to respond for every incident. The decisions include disconnecting the affected sub-system from others,
slowing, shutting down or restarting the affected system, etc. The sub-system also sends reports to the affected users, to the database and to the administration. Other functions of this sub-system include managing patches and adaptability, tracing the attack, mitigation of the attack and so on.

3.5 Recovery Sub-system
The recovery sub-system is for bringing an attacked system back to normal. The functions of this sub-system include managing back-ups, re-installing the programs, periodic and emergency vulnerability testing, restoring a system from back-ups, collecting and protecting evidence, fixing the vulnerabilities. The agents can help to define and test business continuity plans. This process can be very expensive and takes much time if done manually. At every moment, three types of the state of system and sub-systems and operations are stored: the original state, the intended state, and the actual state. When an incident occurs, the system can go back to the original state and flush all the rest. This feature could be partially or wholly implemented. This depends on the current technology and other back-up resources.

3.5 Other Components
The integrated security system is used for certificate management, managing authorization and provides smart cards, database and information protection services. The special analysis component is used for analyzing inputs and other objects that are not understood by the sub-systems. The system fault-tolerance manager is responsible for the overall fault-tolerance of the whole system. It also controls the fault tolerance managers of the sub-systems. The system manager is responsible for managing all the operations of the system. This includes configurations, communications with other systems, controlling the all the components. All these sub-systems have fault tolerance managers which have error detection measures; damage assessment measures; damage confinement measures; error recovery measures; fault treatment and locator and continued service measures.
FIGURE 40: GENERIC MODEL FOR SURVIVABLE SYSTEMS
FIGURE 41: AGENTS

FIGURE 42: AGENT STATIONS
4 AGENTS SECURITY

4.1 OVERVIEW
The lifecycle of software mobile agent starts at an agent author, then it goes to an agent certifier, thereafter it goes to an owner, and then it is launched to different servers to perform the tasks specified [3] as shown in Figure 4.2. The agent developer and owner could be the same but the agent certifier and author/owner are not the same. An owner sends a request to an agent developer with task specifications of the agent. The agent developer creates the agent, comprising of a header, code and data [3]. The header contains the identity, attributes, recipient information, travel path and signatures. The data section is divided into internal data and collected data. The identity of the agent has three main parts [3]: static identity; dynamic identity, and other specific identities. The static identity contains the author’s ID, owner’s ID and the ID of the agent. The dynamic identity contains the agent home and time of launch. Other specific identities can include digital certificates and other tokens. Attributes of the agent include level of trust, task specifications of the agent, constraints of the agent, and credentials of the agent owner.

Signatures include agent authors, certifier’s, privilege authority’s (this authority issues agent’s security credentials to users), agent owners, agent sender’s signatures, and agent server’s signatures. Collected information include is information from different servers where an agent has been visiting. Agents are created by an agent developer according the task specifications. The tasks are specified by the one requesting the services who then signs the agent.

4.2 PROTECTING THE AGENT SERVER
There are a number of technologies [4] for protecting agent servers. One of this is called Software-based Fault Isolation (sandboxing) [5]. This is when untrusted agents are isolated and monitored in a special environment. When other agents, which are not part of the protection system, come to an agent server they will be authenticated and put in different domains or sandboxed depending on the trust level of the agents. The second technology is known as Safe code Interpretation [4] that means that a command that is harmful can be made safe or denied execution. Many agents today are created in using interpretative programming languages, like java, that are platform independent and scripts to be able to run in all platforms. Another technology is called signed code in which agents and other objects are signed digitally by private keys. A digital signature enables the agent server to verify the identity of an agent, the origin of the agent and its integrity. Java applets can be signed, which enables them to perform actions in a wider range of platforms.

Another technique is called State Appraisal [6], which is a way of verifying the correct state of an agent before accepting the agent and before authorizing the agent to access objects. Path Histories [7] is another technology, which aims at making sure that the agent servers that were visited before the current platform are authentic and have agent servers sign the information collected by the agent. Another technology is known as proof carrying code [8], which is a way of forcing authors of agents to prove that they have included safe measures in designing and creating agents. The proof and the code are sent together to the consumer where it can be verified in a simple way without using complicated cryptographic measures and without needing any help.

In this work, we apply Signed Code, Path Histories, a form of State Appraisal and a form of Sandboxing. The agents are signed by both the creator of the agent, the verifier, the owner and the sender of the agent. In this way, we can verify the identity of the agent, the home platform, the sender and the verifier of the code. Path Histories’ method is used by having
the servers, where the agent is visiting, sign the information collected. State appraisal is done not by the agent server but by the certifier of the agent where a trust level is specified so that the hosting agent can decide in which category to put the agent. Sandboxing is applied to agents that are not from the protecting system. Next, we discuss how agents are protected.

4.3 PROTECTING THE AGENT
Protecting agents is different from protecting agent servers [4] because the agents do not have their own processors and they cannot extend the home platform, but have to rely on the environments provided for them. Protecting agents is more of a detective and deterrent manner while protecting agent servers is preventive, detective, and deterrent. There exist a number of technologies for protecting agents [4]. One of them is called Partial Result Encapsulation, in which the results from each visited agent server are encapsulated. This can be done by the agent or by the agent server. However, it is recommended to be performed by the agent itself. One way that can be applied is called sliding encryption [9] in which the agent seals information every time it collects it. The agent can use the public key of the owner to seal the information, so that only when the agent returns home that the collected information is unsealed.

Another technology is known as Mutual Itinerary Recording [10] in which two cooperating agents record and track each other’s movements by sending to each through a secure channel the last agent server, the current and the next agent server. The next technique is called Itinerary Recording with Replication and Voting [11], which is similar to Path Histories [7], but it has been extended with fault-tolerant measures. There are multiple copies of an agent doing the same tasks. This method is resource demanding. The next technology is called Environmental Key Generation [12]. This is a way of protection in which an agent generates a key and protects all the executables if some environmental conditions are true. In this work, we use Partial Result Encapsulation as described in section 4.7. Details of security services in different scenarios are described in the following sections.

The mobile agents that are performing fault-tolerance tasks have special security properties. They are authorized to access agents and inspect the agent headers, agent codes, and data to detect errors, assess damages and so on.

4.4 SECURITY SERVICES DURING AGENT CREATION
For survivable systems, the agent generation library, shown Figure 41, is the agent author. In future, agents could be purchased / requested from other qualified authors. The sub-systems deterrence, protection, detection, response and recovery are the agent owners. These sub-systems request agents from the agent generation library in accordance to their specifications as shown in Figure 41. The special analyzer acts as an agent certifier, but in future there could be an independent body for certification of agents. The sub-system, for instance Deterrence, verifies the agent generation library before requesting a mobile agent. After successful authentication, the denial of service cookies will be shared between the sender and the destination. These are functions of an address and a secret key. These will be part of all the communications between these parties. The aim of denial of service cookies is to reduce denial of service attacks. Communications that do not have denial of service cookies attached with specified properties are ignored. These cookies are not like the normal cookies that servers give to client browsers when visiting their sites.

The agent generation library verifies the identity of the particular sub-system. If the verification is successful, the sub-system requests the required agent for its tasks from
the agent generation library. Every sub-system has many different agents for doing diverse kinds of tasks in this sub-system. The agent generation library composes the code. The agent generation library calculates the integrity of the code and then the separate integrities of the header and the data and attaches its digital certificates. Note that the private keys of the agent’s author, certifier and owner are never stored in the agent. To provide authenticity of agents the agent generation library signs the agent. To provide confidentiality requirement, the agent creator seals the agent by using the public key of the special analyzer, which is acting as the agent certifier. The agent is then sent to the special analyzer. The special analyzer opens the message by the private key and verifies the signatures and the integrity of the agent. If successful the special analyzer checks whether the agent is behaving in accordance to the specifications. The certifier puts a trust level and its digital certificate. The analyzer signs the agent, protects it and sends it to the sub-system. The sub-system opens the message using its private key. It verifies the signatures of the agent creator and of the special analyzer. The sub-system then notifies the agent creator and the certifier that it has received the agent. The sub-system also puts authorization attributes like mobility, expiration time, size limit of data it can collect and whether the agent can create (spawn) children. The sub-system’s controller acts as a privilege authority and issues credentials like roles, group membership and monitoring attributes.

4.5 SECURITY SERVICES DURING AGENT LAUNCHING

The agent can be operating locally or it can be sent to deter, detect, protect at other locations of the system. Before being sent to the location, the sender does the following procedure. The sender specifies the tasks of the agent; Assigns the dynamic identity by adding agent home ID and time of launch for authentication purposes. The sender also attaches the digital certificate of the sender; the owner’s signature of the agent is added for providing integrity; Sends the state of the agent to the controller of the sub-system for audit trails.

The signature of the sender is calculated by putting the receiver’s address, adding the hash of the agents’ state, adding the timestamp and a random number. All this information is put in the recipient information field and is then signed. To provide confidentiality the whole message is sealed by the destination server’s public key. The sender and the receiver authenticate each other before sending the agent. After successful authentication, the denial of service cookies will be shared between the sender and the destination.

4.6 SECURITY SERVICES DURING AGENT HOSTING

According to [4] the agent server should provide separate domains for each agent that it is hosting, but in this work we don’t provide separate domains for the security agents because they are deterring, detecting and protecting the system and they are supposed to move freely. When the destination server receives the agent, it does the following procedure:

- Opens the agent using its private key.
- Verifies the agent generation library’s and certifier’s signatures to check for integrity.
- Verifies agent owner’s digital certificate
- Verifies agent owner’s signature
- Verifies agent sender’s signature
- Checks the time stamp, hash of state and intended recipient in the recipient’s information. If successful the server accepts the agent, monitors the agent to provide accountability requirement and the audit logs are protected by the agent server.

When the agent has done the tasks the agent server will sign the information and send the agent home or to the next agent server as described in section 4.7
The agents that are not from the security system will be sandboxed if they are not fully trusted. This will reduce the denial of service threat from these agents. In cases where denial of service is launched by outside attackers, the address of the agent platform will be temporarily changed until the problem has been solved. The agents that require anonymity will have their identities hidden from other agents.

4.7 Sending an Agent for Cloning
If the agent is very successful in deterring, protecting, detecting intrusions and other tasks in accordance to the specified criteria the agent will be sent to the agent generation library for cloning. In sending the agent, the following procedure will be followed:
The agent generation library and the sender will authenticate each other before sending the agent.
Attach owner’s digital certificate
Assign agent home ID and a time stamp which is the dynamic identity for authenticity purposes.
Create the owner’s signature for integrity requirement.
Create sender’s signature by putting the receiver’s address, adding the hash of the agents’ state, adding the timestamp and a random number. All this information is put in the recipient information field and is then signed.
The whole message is sealed by the agent generation library’s public key to provide confidentiality and then it is sent.
When the agent generation library receives the agent it will perform the procedure in section 4.6 and will then clone the agent and will send the agent back though the agent certifier as described in section 4.4. A copy of the agent is stored in the database of the agent generation library.

5 Conclusions
In this work, we have provided ways of securing agents for survivable systems. The security requirements confidentiality, integrity, accountability are met. Information carried by agents and that, which is stored at agent servers, is kept confidential. Communications between agents and agent owners and agent servers are protected. Integrity of agents and data is provided through signatures. Accountability is provided through monitoring, signatures and log files protection. Denial of service is partially addressed by using denial of service cookies and by sandboxing, untrusted agents. Anonymity is not complete; a mobile agent can be anonymous to other agents but not to the agent server. An agent server has the right to monitor an agent. Limitation is that availability and anonymity requirements are partially met. Future work will be to implement the agent security. Agents that are used for fault-tolerant have all the authority to access agents for inspection purposes.

References


PAPER VI
FRAMEWORK FOR SECURING MOBILE SOFTWARE AGENTS

Jeffy Mwakalinga and Louise Yngström

Department of Computer and System Sciences,

Royal Institute of Technology,

Forum 100, 164 40, Kista, Sweden

Tel: +468 161 721 Fax: +468 703 9025

jeffy@kth.se, louise@dsv.su.se

ABSTRACT

Information systems are growing in size and complexity making it infeasible for human administrators to manage them. The aim of this work is to study ways of securing and using mobile software agents to deter attackers, protect information systems, detect intrusions, automatically respond to the intrusions and attacks, and to produce recovery services to systems after attacks. Current systems provide intrusion detection, prevention, protection, response, and recovery services but most of these services are manual and the reaction time is usually from a number of hours to days depending on the complexity of the systems. There are efforts of using mobile software agents to provide these services automatically, thereby reducing reaction time, but the technology is not widely accepted due to security issues of mobile agents.

In this work, we have created a framework for securing mobile software agents in information systems. Communication security between platforms, protection of the baggage carried by agents, and protection of agents are provided. The framework has five components: deterrence, protection, detection, response and recovery sub-systems. The framework has been partially implemented and has an interface for administrators, monitored systems, NIST vulnerability database, patches’ database, sensors, and Secure Mobile agents Run-Time System. This framework provides security for mobile agents at different levels and this increases trust in agents’ technology. The response time, after intrusions are detected, is shortened. The framework helps systems to adapt by improving the performance of new generations of agents.

KEY WORDS

Software mobile agents, deterrence, neural networks, immune system, genetic algorithm, and feedback mechanism.
FRAMEWORK FOR SECURING MOBILE SOFTWARE AGENTS

1 INTRODUCTION

This work is aimed at studying the methodologies of securing mobile software agents. Software mobile agents are computer programs that perform tasks, like looking for the best airline ticket, buying shares in stock markets, and testing networks for vulnerabilities, on behalf of human beings. An agent consists of three main components [Cheng, 1997]: header, code, and a database. The header contains identity of the agent, agent attributes, signatures, travel paths, level of trust, ownership and other related information. The code section contains a system of programs performing the specific tasks of the agent. The database contains internal and the external information, collected while traversing in different environments. This work is part of the investigation of creating of a generic security framework of survivable systems based on the Systemic-Holistic paradigm [Yngström, 1996] and the Immune system [Somayaji et al, 1997]. The general aim of the investigation is to identify features that protect living systems that can be used to secure information systems. Particular attention is paid to the immune system that protects people from different negative conditions in ever changing environments. The immune system uses cells, B-cells and T-cells to protect the body. In this work, we use mobile agents in the place of cells in the immune systems.

According to [NIST, 2000] security requirements on agent frameworks include confidentiality, integrity, accountability, availability and anonymity. Confidentiality is required so that all the classified information can be kept secret at agent platforms and while being carried by the agents. Communications between agents and between agents and agent servers should also be confidential. The activities of agents should also remain confidential so the audit logs of their activities must be protected. Integrity of agents’ code, state, internal data and collected data should be provided to ensure that unauthorized modification of code, state and data is not done. Agents should be able to detect when there is modification of their code, state and data. Accountability includes identification, authentication and audit of human users, agents and agent servers [NIST, 2000]. Audit trails of agents should also be kept to help tracing activities in case of errors. Agents and agent servers must authenticate each other before performing any transactions. Availability of information and services to mobile agents must be ensured. The agent servers must support simultaneous access, allocate resources fairly, be able to recover from different failures and so they should have fault-tolerance measures. Agent servers should scale and be able to handle requests from many agents. When the agent servers are not able to provide this service, they should notify agents about it.

1.1 RELATED WORK

1.1.1 A DISTRIBUTED INTRUSION DETECTION SYSTEM USING MOBILE AGENTS

This system [Kannadiga et al, 2005] has components: the console for intrusion detection system, the mobile agents’ dispatcher (MAD), and hosts. The system uses mobile software agents. Alerting agents (AA) reside in the IDS console and are used for receiving alerts that are generated by mobile agents (MA). Mobile agents (MA) are responsible for gathering and analyzing evidences of intrusions and attacks from different hosts. Each mobile agent is specific for a certain type of intrusions. Static agents (SA) reside in hosts with responsibility to monitor in the hosts. Static agents create a number of threads and each one is responsible for different kinds of attacks. MAD manages the dispatching of mobile agents to handle the requests that were generated by static agents. The requests are stored in a list called victim host list (VHL). This system has been implemented and it covers doorknob-rattling attacks, chain/Loop attack, distributed port scanning, and distributed DOS attacks. In the doorknob
rattling attacks attackers try to log in a system using a few common usernames and passwords. In the chain/lop attack, an intruder uses different machines to hide her identity and it is challenging to trace the origin of the intrusion. In distributed port scanning a number of distributed machines are used for scanning making it difficult to detect the origin of scanning. The system is effective in analyzing incidents but it lacks security of the individual mobile agents that are involved in performing different tasks.

1.1.2 A SAFE MOBILE AGENT SYSTEM FOR DISTRIBUTED INTRUSION DETECTION
[Zhong et al, 2003] have created a system for distributed intrusion detection based on the mobile agents. The system has a manager, an assistant mobile agent, a response mobile agent, a host-monitoring agent, and three host-monitoring sub-agents. When an intrusion occurs, the host-monitoring agent will send an alert to the manager. The manager will dispatch an assistant mobile agent to the different hosts to determine whether the intrusion is distributed or not. The assistant mobile agent will bring a report and the manager will analyze the report and then send the response mobile agent to all the hosts to fix the incident. The sub-agents are monitoring network connections, size of packages, headers of packages and arriving times, different file operations and privilege operations. The results of the monitoring are sent to the intrusion analyzer where they are interpreted in accordance to the interpretation trees. The security of mobile agents, confidentiality, authentication and integrity, is discussed but not in details. It is not described how the agents can be traced in case some problems occur during the traversing of agents. Baggage security is not discussed either.

2 SECURITY FRAMEWORK FOR AGENTS
This framework contains the following subsystems: agent creator and database, system manager, integrated security system, general database, special analysis, deterrence, protection, detection, response, and recovery a shown in figure 44. The agents are generated in the agent creator component. The system manager is responsible for the overall administration. The integrated security system is responsible for managing and providing security services, managing digital and attribute certificates and database services. The general database is keeping the main records of the system. Special analysis is used for analyzing the different intrusions and abnormalities in the system. All the components communicate with other components in the system. The sub systems request mobile software agents from the agent creator. All agents are trained before being released into the real environment. In the first phase of the training, the agents pass a negative selection test [Kim, 2002]. The agents that pass this test go through the clonally selection test [Kim, 2002]. After this test, the agents are ready to be deployed in the real environment and they are sent to the sub systems that requested the agents. When agents are released in the real environments, they are monitored to record their activities. The features of the most successful agents, according to policy specified criteria, are recorded and used to improve the features of next generation of agents.

2.1 REGISTER SYSTEM
The function of this system is to verify the data of the entity with the administrator before issuing an ID, which is a mini certificate. After verification of the data, a role is given to the entity, location of operation and other authorization parameters. If verification is not successful, the entity is killed or sent to for analysis. If verification is successful, the mini-certificate is issued. An encrypted authentication key is bound to the mini-certificate. An attribute certificate is issued and a public key certificate is issued. Attribute certificates are issued depending on the policy of the system and on the sensitivity of the environment. The entity is then registered into the database. Thereafter a status, a timestamp and agent’s ID are recorded and a report is sent to the general DB. The message
authentication code of the contents is created and encrypted; a denial of service cookie is created and signed. The level of security in an environment has a minimum and no maximum. The owners of the system decide their maximum level of security depending on their environment.

2.2 MOBILE AGENTS

There is a system of mobile agents that are used for providing different security services in the sub systems. These include helper and killer agents, authentication agents, confidentiality agents, authorization agents, Non-repudiation and integrity agents, and third-order feedback agents system.

2.2.1 HELPER AGENTS AND KILLER AGENTS

The helper agent, Figure 43, is responsible for delivering messages among agents and subsystems.

They take as input a message and verify the ID and signature of the message. If verification is not successful, the message is deleted or taken for analysis. If verification is successful, the helper agent puts a status, a timestamp, and the agent’s ID. The message is then delivered to the requested destination and a signed and time stamped report is sent to the general database. Killer agents are responsible for terminating intruding programs or processes.

2.2.2 AUTHENTICATION AGENT

This agent is responsible for providing authentication security service in the system and sub systems. It verifies identities of entities in a system. It monitors the system and checks the identities of entities in the system, even as B-cells in the immune system check whether all cells that are in the human body are marked ‘self’. It verifies the mini-certificate of the entity and checks with the general database to see if it is registered. If the entity is not registered or if the ID is not correct, this agent kills the entity or sends it for analysis. If verification of the identity is successful then the agent puts the status, timestamp and agent’s ID. The agent then sends it to the authorization agent and sends a report of the action to the DB.

2.2.3 CONFIDENTIALITY AGENT

This agent provides confidentiality security service in the system, deterrence, protection, detection, response and recovery sub-systems. It first verifies the ID of the entity or message to be encrypted. It then verifies the authenticity of the sender, the authorization that the sender has. If verification of the message and the sender is successful then the agent encrypts the message or entity, put a status, a
timestamp and agent’s ID. Then, it sends the message to the requesting system. It also sends a signed report to the general DB for audit purposes.

2.2.4 Authorization Agent
This agent provides the authorization security service. It first verifies the identity of the entity. Then it checks in the database whether this entity is registered. Then it checks the signature. If verification is not successful, this agent kills the entity or sends it for analysis in accordance to the specified policy. The agent also checks the attribute certificate of the entity. The attribute certificate has fields like roles, time and place of operations, delegation. The attribute certificate is also bound to the public key certificate. If the attribute certificate is not appropriate, (expired, corrupted) the agent sends it to the registering system through the helper agent.

2.2.5 Non-repudiation and Integrity Agent
This agent is responsible for providing the non-repudiation and integrity security services in the system and sub systems. It takes as input an entity and it verifies the entity’s ID. If ID verification is successful, the agent signs or verifies the signature on the entity. If not the agent kills the entity or sends the entity for analysis via the helper agent. The agent puts the status, a timestamp and agent’s ID. The agent sends the entity to the requesting system. It also sends a report of the action to the general DB.

2.2.6 Third Order Feedback Agents System
There are a number of agents in the third order feedback system [Schoederbek et al, 1998]. The detector agent notifies the entity the value that needs to be changed. The effectors’ agent supplies the required change. The recall agent produces historical decisions that have been made in the past from the memory. The recombination agent produces a number of recombinations from the memory and the selection agent selects those that can be further modified. The system of decision agents makes decisions based on the fuzzy logic controller and the Neural Network’s Adaptive Resonance Theory (ART) [Dasgupta et al, 2001]. A report is then sent to the DB.

2.3 Deterrence System
This system is aimed at scaring away attackers from a system. It has sections: inputs, process, outputs, and a feedback mechanism. It takes as input traffic and processes it and the outputs are fed back and modified using the third order feedback system as shown in Figure 44. The deterrence system classifies the inputs. It then kills the categories or allocates the different categories to the proper agents in the process section. This subsystem has a number of agents depending on the policy of the system. Every deterrence agent specializes in different types of surveillance. The agents can decide to: trace the surveillance or scanning efforts; kill them; reply nothing or with a legal action message; or send for analysis if the type of surveillance is unknown. The sub-system also has: helper and killer agents; authentication agents; confidentiality agents; authorization agents; non-repudiation and integrity agents; and third-order feedback agents system. These agents are present in all the sub-systems.

2.4 Protection Sub System
This subsystem is responsible for providing the security services authentication, confidentiality, integrity, authorization, and non-repudiation. It has inputs, processing, outputs and feedback mechanisms. These security services are provided with the help of the integrated security system and software mobile agents. The integrated security system manages public key certificates, authorization, directory services, and smart cards through certification, smart card, directory and authorization systems. Software mobile agents perform authentication, integrity, authorization, non-repudiation,
and confidentiality security services. All the entities in a system are given identities even as all cells in the human body are marked as ‘self’. Cells patrolling in the body continuously check for cells that are ‘no-self’. The identities given to the entities in a system are in a form of a mini-certificate. The mini-certificate has the following fields: a unique ID; a group ID; Encrypted location; Encrypted authentication key; an encrypted key; Denial of service cookie; an encrypted certificate serial number of the entity; Encryption attribute certificate number; an encrypted attribute number of the entity; and a signature.

2.5 DETECTION SUBSYSTEM
This system has inputs, processing, outputs and feedback mechanisms as shown in figure 44. In this subsystem, we use the general mobile architectures. This sub system acts as a detection and prevention system since it detects and responds. The system takes as input traffic and classifies using the Adaptive Resonance Theory (ART) [Dasgupta et al, 2001] or kills the incoming traffic or closes the system. Agents make decisions basing on the fuzzy logic engine [Dasgupta et al, 2001] and genetic algorithms as described by [Pillai et al, 2004].
2.5.1 System Design for Network Intrusion Detection System Using Genetic Algorithm

Genetic algorithms are based on the principle of survival of the fittest and the goal is to find a set of parameters or values that maximize a certain fitness function. An example of a fitness function could be \( F(x) = y^3 + 2 \cos(3y) \). There is a set of all possible \( y \) values. In addition, the goal is to find a set of \( y \) values from this set that maximizes the fitness function. In the system [Pillai et al, 2004] a data set is created that specifies the normal and abnormal behaviors by analyzing traffic packets from a network sniffer, like a TcpDump or WinDump, which records traffic [Pillai et al, 2004]. This dataset can have data like source IP, destination IP, source port, destination port, and the protocol used and an
intrusion indicator [Pillai et al, 2004]. This data set is used for training a genetic algorithm. After training, the data set can be updated and connections added [Pillai et al, 2004]. The rule set is established in the form “if \{condition\} then \{act\}” [Pillai et al, 2004] and thereafter a genetic algorithm rule set is created in GA format. In the initial stages, the first part will function as search algorithm to get values for each rule to indicate the good rules. Thereafter the genetic algorithm is used as a fitness function to determine the fittest rules. The fitness function used in [Pillai et al, 2004] is  

\[ F = \frac{a}{A} - \frac{b}{B} \]

in which ‘a’ contains the value that the specific rule carries for the number of correctly detected intrusions. ‘b’ contains the value that the specific rule carries for the number of false alarms. A is calculated by adding the value of correctly detected intrusions from all the rules. B is the total number of connections in the dataset.” When an intrusion occurs, it is notified by a response mechanism. The response mechanism is a pop up window indicating the rule, and a message notifying that an intrusion has occurred. “[Pillai et al, 2004]

2.5.2 NEURAL NETWORK CLASSIFIER
The Adaptive Resonance Theory (ART) [Dasgupta et al, 2001] is used for classifying network traffic into normal and abnormal and in training the monitoring agents. ART is neural network classifier is an unsupervised neural network using competitive learning and it does not require human supervision. During the learning stage, a knowledge base is established in which network, system, user, process normal behaviors are recorded. Any other behaviors that are not in the knowledge base are categorized as intrusions [Dasgupta et al, 2001]. The detection subsystem recognizes normal patterns and any other unknown patterns are regarded as malicious. In the ART Neural network, there are two filters: one represents features; the other represents categories. The initial stage in the learning process is concerned with parallel searching scheme that updates itself adaptively [Dasgupta et al, 2001]. During this period, input traffic categories are assigned recognition codes. New networks are encoded by changing weights or long-term memory traces and when self-learning is stable search automatically stops [Dasgupta et al, 2001].

2.5.3 FUZZY LOGIC CONTROLLER
The decision agents are basing their decisions on the fuzzy logic controller [Dasgupta et al, 2001] and also from the agent creator library and database. Fuzzy logic is a concept in which objects or entities can partially belong to a set. The objects can for instance belong to a set A by 50%. The range of belonging is 0-100%. In classical sets, an object or an entity is either inside or outside a particular set [MMDS, 2003]. The fuzzy logic is used in detection system decisions because the differences between normal and abnormal behaviors in networks are not distinct but fuzzy [MMDS, 2003].

2.6 RESPONSE SUBSYSTEM
It has inputs, processing, outputs and feedback mechanisms as shown in Figure 44. This sub-system bases on [Carver, et. al]. It receives alerts from the detection sub system. Interface agents are responsible for keeping history of false positives and negatives generated by each intrusion detection entity [Carver, et. al]. These agents transform IDS specific messages into a generic message format like the Knowledge Query and manipulation Language (KQML) or the Common Intrusion Detection Format [CIDF]. This history is used to create a confidence metric of each monitor. This metric and the intrusion reports are sent to the master analysis agent. The master analysis agent determines whether this intrusion is new or whether it is a continuation of the existing intrusion [Carver, et. al]. If the incident is new then a new analysis agent is generated to create a response plan for this new attack. If the intrusion is part of the existing one then the confidence metric and the intrusion report are sent to the agent handling the attack. To work out a plan for response the agent gets help from the Response Taxonomy agent, which is used to classify the attack [Carver, et. al]. The Policy
Specification agent is also consulted to check the legal, ethical, institutional requirements and resource limitations. The decision made is sent to the Tactics agent by the analysis agent. The tactics agent species the action to be taken and then allocates the duty to the appropriate components of the Response toolkit. The logger agent records decisions made by the analysis and tactics agents [Carver, et. al]

2.7 Recovery System
This sub system is used for putting a system back to its normal state after an attack. It has the following agents: helper and killer agents; authentication agents; confidentiality agents; authorization agents; Non-repudiation and integrity agents; and third-order feedback agents system; installation agents; cleaning agents; forensics agents; on-line back-up agents; off-line back-up agents.

3 Security of Mobile Software Agents

3.1 Security Services in the Generation of Agents
The Agent creator and creates agents. The agents are given identities. After generation, the special analyzer must certify the agents locally, but in future, there could be an independent body for certification of agents. Every sub system requests agents from the agent creator. The agent creator and the requesting sub-system will mutually authenticate each other before communicating further. Every sub-system has many different agents for doing diverse kinds of tasks in this sub-system. To provide authenticity and integrity of agents the agent creator signs the agent. To provide confidentiality requirement, the agent creator seals the agent by using the public key of the special analyzer, which is acting as the agent certifier. The agent is then sent to the certifier. The certifier opens the message by the private key and verifies the signatures of the agent. The special analyzer checks whether the agent is behaving in accordance to the specifications. The certifier puts a trust level and its digital certificate [Cheng, 1997]. The analyzer signs the agent, protects it and sends it to the sub-system.

3.2 Protecting the Agents, Their Baggage and Securing Communication between Sub Systems
Agents carry baggage and this must be protected. During the handshake, the sending and receiving sub systems exchange session secret keys to secure communication. When agents are moving between deterrence, detection, protection, response and recovery sub systems are protected in the following way. The session keys are used to protect the agent and the messages between these sub systems. The agent and the baggage are also signed by the sending sub system. The receiving sub system verifies the integrity and authenticity of the agent and messages by verifying the signature. Protecting agents when they are visiting a sub system is different from protecting agent servers [NIST, 2000] because agents do not have their own processors and they cannot extend the home sub system, but have to rely on the environments provided for them there. The technology called Environmental Key Generation [NIST, 2000] is applied to protect all the executables if the environment is hostile. An agent generates a key and protects the executables if some environmental conditions are true. We also apply the Partial Result Encapsulation [NIST, 2000], in which the results from each visited sub system are encapsulated and signed. We also apply the sliding encryption [Young et al, 1997] in which the agent seals information every time it collects it. The agent can use the public key of the owner to seal the information, so that only when the agent returns home that the collected information is unsealed.
Protecting the Sub Systems

There are a number of technologies [NIST, 2000] for protecting agent servers. One technique is called State Appraisal [Farmer, 1996], which is a way of verifying the correct state of an agent before accepting the agent and before authorizing the agent to access objects. In this work, agents are signed using the private keys of the agent creators and dispatchers. The sub-system opens the message using its private key. It verifies the signatures of the agent creator and of the special analyzer. The sub-system also verifies the authenticity of all the agent servers that were visited before the current sub-system in accordance to the Path Histories [Ordille, 1996]. The sub-system then notifies the agent creator and the certifier that it has received the agent. All the agent servers sign the information collected by the agent.

3.4 Sending an Agent for Cloning

If the agent is very successful in deterring, protecting, detecting intrusions and other tasks in accordance to the specified criteria the agent will be sent to the agent creator for cloning. In sending the agent, the following procedure will be followed: the sending sub system and agent creator will authenticate each other before sending the agent; the sender creates a secret key and protects it with the public key of the agent creator, the sending sub system then signs it. When the agent creator receives the agent, it will verify the signature of the sending sub system. The agent creator will then clone the agent and will send the agent back though the agent certifier. A copy of the agent is stored in the database of the agent creator.

4 Prototype of the System

The architecture consists of the following Components: Interfaces for the administrators; Vulnerabilities database; patches database; a database for agents’ actions log files; Monitored systems as shown in Figure 44. Every interface has sub-systems: Certification system, Smart card system, directory system and authorization system. In the smart cards system, one can create file systems in the smart; one can initialize the smart card, issue a smart and personalize a smart card. The authorization sub-system one can register different roles that exist in the system like administrator, normal user, security manager and so on. Another function is this system is to list roles that exist. It is also possible to remove roles whenever necessary. Another function is to register applications like databases and different programs. One can then list applications; one can assign roles to applications. If an application does not have a role to open, a certain file access will be denied to this application. For viruses, that come unnoticed to a system will not be able to run or open other files because they will not have been registered and will have no roles. Other functions in the authorization system include: assigning roles to users; removing roles from users; remove roles from applications. It is also possible to create access rules and list them. Other functions include creating a policy, removing a policy, creating and removing a policy set, exporting a policy or a policy set.

4.1 Interface

Every interface has sub-systems: Certification system, Smart card system, directory system and authorization systems. The functions in the interface include registration of users, servers, management of certificates and system administration [Muftic et al, 2001] as shown in Figures 45, 46, 47 and 48.
4.2 Vulnerability Database, Patches and Agent Logs

Most attacks are possible because of vulnerabilities in systems so if we can solve the vulnerability problem many attacks will not succeed. The vulnerability database contains vulnerabilities from the National Vulnerabilities database (NVDB) of the National Institute of Standards and Technologies (NIST). The database of vulnerabilities is downloaded from the NVDB and then it filtered from the XML format and converted to a relational database and stored and ready for querying. There is a set of mobile agents, which can access, query, read and dispatch data from the NVDB database. The patches database stores all the latest patches. All the actions of agents are logged in the agents’ logs database. [Muftic et al, 2001].

The Monitored System

The monitored system consists of the following components: security, where different security services are performed; response agents; Sensors (deterrence, detection and protection); Secure Mobile agents Run-Time System (SMART) [Muftic et al, 2001]. The interfaces are shown in Figures 45, 46, 47 and 48. When there is an alert or alarm from the sensors the response agents picks up the alerts. A secret key is used to protect the alert message using AES. This key is then protected by the system administrator’s public key. A response agent is assigned the task to take the message to the interface. The message is signed by the SMART system send alert messages to the administration interface, which sends agents to take of the system via the SMART system, where an alert came from as shown in figure 45.

![Diagram of the monitored system](image)

**Figure 45: Architecture of the Mobile Agents Structure**
**FIGURE 46: LOGIN TO THE SYSTEM**

**FIGURE 47: INTERFACE OF THE SYSTEM**
5 CONCLUSION

In this work, we have created a framework for securing software mobile agents that perform different tasks in deterrence, protection, detection, recovery and response sub systems. The framework provides protection of sub systems, agents and their baggage, and communication security. The agents provide authentication, confidentiality, integrity, non-repudiation and authorization security services. The training of agents during their creation bases on the immune negative selection and clonally selection algorithms and genetic algorithms. A prototype has been created but it reflects only part of the framework that deals with maintenance. A conclusion of the general behavior cannot be given from the prototype.

REFERENCES


PERMISSIONS
Jeffy Mwakalinga and Louise Yngström are the authors of this paper. This work is original and does not violate any copyrights, rights and privacy of others. We retain the right all or part of this paper in our future work. We grant the ISSA 2006 organizers the right to publish this paper in the ISSA 2006 proceedings
METHODOLOGY FOR CONSIDERING ENVIRONMENTS AND CULTURE IN DEVELOPING INFORMATION SECURITY SYSTEMS

Jeffy Mwakalinga, Stewart Kowalski, and Louise Yngström

Department of Computer and System Sciences,
Stockholm University/Royal Institute of Technology,
164 40, Kista, Sweden

Tel: +468 161 721 Fax: +468 703 9025

jeffy@dsv.su.se, stewart@dsv.su.se, louise@dsv.su.se

ABSTRACT
In this paper, we describe a methodology for considering culture of users and environments when developing information security systems. We discuss the problem of how researchers and developers of security for information systems have had difficulties in considering culture of users and environments when they develop information security systems. This has created environments where people serve technology instead of technology serving people. Users have been considered just as any other component in an information system, which has resulted in having efficient technical controls but inadequate social controls for security. In this paper, we propose a holistic and immune security framework that considers culture of users and system environments in developing information security systems.

KEY WORDS
Deterrence, response, recovery, value-based chain, adaptability, environments, and detection
METHODOLOGY FOR CONSIDERING ENVIRONMENTS AND CULTURE IN DEVELOPING INFORMATION SECURITY SYSTEMS

1 INTRODUCTION

1.1 INFORMATION SYSTEMS AND ENVIRONMENTS

Information systems have to learn to adapt to different system environments and to cultural environments. “A system is here defined as a set of objects together with relationships between the objects and between their attributes related to each other and their environment so to form whole” [22]. An information system can be modeled to consist of abstract systems, (information), living systems (people), and concrete systems (technology) [12]. “Churchman defines environment as those factors which not only are outside the system’s control but which determine in part how the system performs” [22]. An environment of an information system is outside of the control of an information system. There are hostile and friendly environments and an information system must be able to learn and adapt in both the hostile and friendly environments. Who defines the boundary between a system and its environment? What are the factors that set this boundary? Every information system has internal and external environments [22].

![Diagram of Organization: Resources of IT and Its Environment]

FIGURE 49: ORGANIZATION: RESOURCES OF IT AND ITS ENVIRONMENT

We suggest that values of people (culture, traditions, laws, policies, and other social issues) and geographical boundaries need also to be considered when an information systems security designer set the boundary between a system and its environment. Currently with information system, designers and developers of IT set the boundary between a system and an environment for users without asking their values. Users of information systems cannot really be regarded as system owners as long as their systems cannot be controlled or defended. The organization has the following environments: labor,
customers, ecology, public, material and equipment, land, capital, government, competitors, and technology but an organization controls only part of the environments, as shown in Figure 49 [22].

1.2 CULTURE AND INFORMATION SYSTEMS

There have been concerns about the role of culture in information systems [20]. Culture has been defined differently by different scholars [10]. Van Dam, Evers, and Arts define culture as a set of values, attitudes, and behaviors that people learn or are passed over to them over a period of time [26]. There is a general agreement among information system researchers that culture affects the way individuals’ interact with complex information systems [20]. However, a model has not been developed to measure the effect of culture to individuals. They [20] write, “Science educators, from Japan, India and Africa, appear to share a common understanding that science needs to be perceived in a cultural context and to link the development of scientific literacy with an understanding of worldview. Between them, they have examined the faiths, philosophies, and logic of students from various cultures to examine, within a culture, the conflict between ‘scientific’ and traditional concepts of science. Some have been able to link traditional belief and the understanding of scientific concepts or performance of experimental tasks. Others have also shown that science teachers’ worldviews and their traditional beliefs affect their teaching and thus their students’ learning.”

Another question is how much culture affects the decisions that an individual makes when using computer systems [20]. Further concern is whether a function that is provided by an Internet system is consistent across cultures [20]. Van Dam, Evers, Arts did a survey in three different cultures, Moroccan, Surinamese, and Dutch, on user experiences on e-government sites [26]. The results show that Dutch and Surinamese could notice titles on the left side faster while the Moroccan could notice things on the right sides of pages faster. The Moroccans are sensitive to green and red colors. This is because the Moroccans started to read from right to left. Dutch showed a less degree of uncertainty avoidance and they did not read in details but just browsed. The Moroccan needed confirmation that they are performing all right while Dutch and Surinamese did not need this confirmation. The Moroccan culture is a masculine culture in which recognition of achievement is important to participants. Dutch and Surinamese are feminine and they did not need recognition of achievement. In addition, the Surinamese and Dutch are neutral in culture, which means that showing emotion is regarded as unprofessional. The Moroccan culture is affective which implies that showing of emotion is regarded as normal. The Moroccan is a collectivist culture and it believes that the government website cannot have mistakes and so the Moroccans blamed themselves for the mistakes. The Dutch and Surinamese are individualists and they blamed the system for the mistakes. The conclusion was that people with different culture backgrounds experience different problems in using e-government applications.

We have created a holistic and immune security framework [17] [30] that is based on the Systemic-Holistic Approach and the Immune system. The holistic and immune security framework is a function of the deterrence, protection, detection, response, recovery value-based chain functions. The holistic and immune security framework applies the system theory and holistic approach to provide security for information. The holistic and immune security framework applies the principles of the immune system to make systems learn to adapt to environments. We apply the software agents to provide security services in analogy to B-cells and T-cells in immune systems.
2 The Steps to Take When Considering Culture of Users and System Environments in the Holistic and Immune Security Framework

2.1 Analyse the Threat Agent
In the first step, we start by analyzing the threat agent based on the socio-technical economical system [15]. We document the states that an enemy of an information system could control and the states that an information system owner could control. We created the model of the enemy in which we analyze the methods, tools and processes that an enemy to the systems can apply to attack information systems.

2.2 Classify Assets and Perform Risk Management
The second step is to classify the assets and perform risk management in an information system. We have automated the classification of assets and risk management using software agents. The recovery sub system of the holistic and immune security framework identifies, assesses, and manages risks. Risk management is based on the Enterprise Risk Management (ERM) – Integrated Framework of the Committee of Sponsoring Organizations of the Tread Way Commission (COSO) [21].

2.3 Analyze Environments Where the Systems in Focus Operate
The third step is to analyze the information system environments in the information system. This involves identifying the local environment, embedded environment, total environment, and predicting future environments [1] [27]. It also involves classifying the environments, analyzing the levels of security of these environments. We identify the environments where a system will be operating. An observation is made over a period of time to study the inputs that are coming and affecting an information system. Then the sources of the inputs have to be studied and traced. Some inputs could be more complicated as they are a result of several environments integrated together. After identifying the inputs, we have to find ways of modifying the inputs so that they do not affect the general state of information system as shown in Figure 50. Modification of inputs and outputs is done using the Cybernetics feedback mechanisms [22]. There are a number of ways in which we could classify environments [22]. In this work, we choose to classify the environments based on their complexities, dynamism and security levels of environments.

![Figure 50: Inputs from Environments](image-url)
An environment could be simple and static, simple and dynamic, static and complex, or dynamic and complex [22]. A static and simple environment has: few factors and components; homogenous factors and components; factors and components that do not change; a stable environment [22]. A complex and static environment has: large number of factors and components; heterogeneous factors and components; factors and components that do not change; unstable environment. The simple and dynamic environment has: few factors and components; similar factors and components; unstable environment; the state of factors and components that change; rate of change of change could be stable or unstable. A complex and dynamic environment has: large number of factors and components; heterogeneous factors and components; high level of uncertainty; unstable environment; the state of factors and components change and the rate of change could be stable or unstable [22]. Examples of environments affecting information systems include an operating system, computer hardware, intranet, Internet Service Provider (ISP), education, hardware, operating systems, electric power, heating, cooling, floods, earthquakes, fire, and cultural environments. What sets the boundary among different environments? Is it policies, ethics, culture, or laws?

The next step is to analyze, using the Systemic-Holistic Approach, the correctness of an environmental systems (like the operating system where an information system is running) at the theoretical/model, design/architecture, and implementation levels [27]. We apply different standards and criteria to analyze the correctness of environmental systems. We analyze the correctness at the different levels because a standard of a system can be correct but its implementation can be wrong. An example of this is the Wired Equivalent Privacy (WEP) encryption system for wireless systems. This encryption system bases on the stream cipher RC4. The algorithm of RC4 does not have flaws but the implementation, the key scheduling and management facilities, is flawed [2]. Many algorithms are basing on wrong mathematical assumptions, which can lead to vulnerabilities in security systems at the higher levels. Then we need to have proofs of correctness at the design and implementation levels.

2.4 ASSESS THE EFFECTS OF CULTURE AND TRADITIONS OF USERS TO INFORMATION SECURITY

The fifth step is to assess the effects of culture and traditions of users to information security in this information system. We apply the informal cultural model, Figure 51, to predict the behaviors of users. Chaula and Yngström made a study in [4], where they examined how human behavior affects systems security. They found that people with low uncertainty avoidance tend to lack holistic approaches to security which implies that they: lack security in depth measures; “lack attention to details”; tend have “poor risk assessment”; have “poor assumption about motivation, opportunity and methods”; “lack of information classification”, use metrics poorly [4]. Cultures where people have low future orientation have ineffective contingency planning. This affects prediction of disasters and preparation if an attack or a disaster was to occur. Cultures where power distance was high result in poor communication on security issues between upper level management and employees and technicians [3] [4]. In low power distance cultures communication and discussion on security issue was better but readiness to report unethical conduct in security was not high [4].

2.4.1 INFORMAL CULTURAL MODEL

We have established an informal cultural model for predicting the behavior of users to information security system of different cultures. This cultural model will help developers of security for information systems to predict the behavior and preferences of users of different cultures. This model consists of the following components: General Living System ID; Hofstede; Worldview; Social Identity theory (SIT); Computer Literacy; and General Education as shown in Figure 51.
The General living System Identity of an individual contains the cell, organ, organism, group, organization, nation, supranational [16] [27]. The general Living identity will provide among others information about cultural background. For instance if the culture reads from right to left then it means the important instructions or pictures in information security have to be placed on the right side of the pages to be noticed faster. The Hofstede [10] component consists of the values: power distance index; individual vs. collectivism index; uncertainty avoidance index; femininity vs. masculinity index; and long-term vs. short-term orientation index. The next component is the Cobern’s worldview theory [5] [20]. This theory consists of how an individual understands the world and other people, classification, causality, relationship, self, time and space. This includes a model of the world, what we should do, how we should reach our goals, where are we heading, what is true and false, etc. The next component is the social identity theory with categorization and identification as sub components [23] [20]. These identities can be at personal, group, national, ideological, and religion levels. Then we have computer literacy, which indicates the practical and theoretical computer knowledge that an individual has. The last component is the general education of the individual.

In cultures where power distance is high, there is a tendency of over respecting the older people and people who have higher positions in companies. Therefore, there is higher possibility of breaching security if there is external pressure from older people or people with higher positions in a company. This implies that if a boss wanted to borrow a password or a smart card from an employee, the employee is likely to accept the request, thereby breaching security. Therefore, as developers we need to create an authentication system that will not work in cases when there is a possibility of such external pressure to breach security. In countries with low power distance, this possibility is low. There could be a tendency of making security policies and procedures that are not widely accepted by all employees since high-level discussions do not always involve low-income groups in high power distance cultures. Björck and Jiang made a study to compare the implication of culture on IT security between Sweden and Singapore [3]. The power distance in Sweden is low, 31%, while in Singapore it is high, 74% [3] [10]. The manager of a company is Singapore commented that he makes the policies and other issues of IT security and then gives them to the IT department to implement. The Manager of a Swedish company commented on the same issue that he identifies the policies and other IT security issues and then calls a meeting with all the employees involved to discuss and solve the issues.

In cultures that value individualism, people tend to make decisions that are more in an individual’s interests than group’s interests are. This means that a security manager will tend to choose the security decisions of self-interest in the first hand, while security managers from cultures that value collectivism will tend to make security decisions favoring group interests. Another example from the same study [3] is that Sweden scores 71% in the individualism collectivism index, while Singapore scores 20% [10]. It was observed that in Singapore employees consider themselves as an extended
family and so they share passwords with each other and they do not consider this as a security breach, while in Sweden people do not share passwords. It was also noted that employees in the Singapore could access even resources that they do not need while in Sweden employees could access only the resources they needed. Hofstede [10] comments that in societies that value collectivism people consider themselves as an extended family, which implies that they trust each other and share responsibilities. This implies in the IT Security world that if for some reasons an employee is not at the workplace now, the employee can ask a colleague to access resources on her behalf by providing all the necessary authentication and authorization credentials. It was also noted that when employees leave companies in Singapore their accounts could remain for a long time without being terminated, while in Sweden when an employee leaves a company for another company the accounts are terminated immediately [3].

In societies where there is the index of uncertainty avoidance is high people tend to be protected against unknown situations and do not always allow their children to experience unknown situations. Students usually expect teachers to have all the answers to their questions [19]. People prefer to have rules, laws and regulations in most areas where environments are structured [19]. In societies where this index is, low people are not protected against unknown situations and they allow children to experience unknown situations. In information systems security, people would tend to take more risks and so leave parts of the information systems unsecure.

2.5 APPLY SOCIO-TECHNICAL MEASURES WHERE CULTURE AND TRADITIONS CREATE WEAK LINKS IN INFORMATION SECURITY

The sixth step is to apply social-technical measures [12] where culture and traditions create weak links in information security. Knowledge is applied to understand, to explain, to predict, and to control. The informal model will be applied in form of procedures to control. Control can be used to control negatively or positively. The different actions will be assigned values. If the consequence of a certain action or value is negative then this action will be forbidden. If the consequence of a certain value or action is positive then the action will be allowed.

2.6 PROVIDE FEATURES TO MAKE AN INFORMATION SYSTEM LEARN TO ADAPT TO ENVIRONMENTS

In this step, we provide measures for making an information system and information security system learn to adapt to environments. Ashby proposed two types of adaptations [25]. The first is to make the system adapt to an environment. The second adaptation is to make the system learn to adapt when the environment changes. We apply the Cybernetics feedback mechanisms [22] and digital immune system [9], variety and regulation [9] and Cybernetic structural models [11] [9] for the first type of adaptation. We apply the Viable System Model, VSM, [9] [1] for the second type of adaptation. Different nations and enterprises apply the VSM [9]. The major application of this model [9] was in Chile during the times of president Salvador Allende. The intelligent forces were trying to destabilize the economy because Allende was a dictator but Chile applied the Viable System Model [30] to stabilize the economy of the country. The environmental disturbances came from the intelligence agencies and the VSM was regulating the disturbances to stabilize the economy [25]. We apply this model to make the security framework learn to adapt to environments. The Viable system model [1] [27] [9], Figure 52, consists of five sub systems: Subsystem 1, Subsystem 2, Subsystem 3, Subsystem 4 and Subsystem 5.

Subsystem no 1 is the lowest level and subsystem 2 is coordinating the operations of subsystem 1 and it receives orders from subsystem 3 [1] [27]. Subsystem 3 is a commanding and controlling
subsystem. It controls the internal stability of subsystem 1 and audits it through command and audit channels [27]. Subsystem 4 is concerned with future, adaptation, planning, and simulation measures. Subsystem 4 is responsible for making sure that the whole system learns to adapt to dynamic environments. Subsystem 4 collects data on environmental disturbances and stores them in a database. We apply these data to create probabilistic models to forecast the future environmental disturbances [9] and thereby foresee how the system will react to those future disturbances. Subsystem 5 creates rules, identities, goals, and policies of operations. Subsystem 5 monitors the behavior of subsystems 3 and 4 to make sure that they follow the rules, policies and goals.

Every subsystem 1 has a local environment embedded in another environment. This embedded environment is part of a total environment, which contains a future environment. Subsystem 2 is responsible for stabilizing subsystem one. Subsystem 3 monitors the behavior of subsystems 1 and 2 and is concerned with internal operational controls of subsystem 1 [9]. It also audits the subsystem 1 to make sure that it performs in accordance to the plans given to it through subsystem 2. Subsystem 4 is concerned with the outside and future of a system. The controller of the desired essential variables mixes them with variables from the monitors to produce the harmless inputs to the information systems. There are two types of feeding: feed forward in which the regulator receives the disturbances and acts before the information security system; in the negative feedback, the information security system receives the environmental disturbances and then the regulator regulates the disturbances via the transformer. For every environmental disturbance, there is a corresponding response as shown in the outcome matrix in Figure 53. The framework for adaptive information security systems receives environmental disturbances through the deterrence, detection, prevention, response, recovery sub systems. The adaptability system of the security framework monitors and records the environmental disturbances, essential variables, and regulators over time as shown in Figure 53. The adaptability system applies these recorded data to create probabilistic models to forecast the future environmental disturbances [9] and thereby foresee how the whole security framework and the information system will react to those future disturbances.
There is a table of transformations in memory of environmental disturbances, essential variables and regulatory disturbances. The controller of the desired essential variables for the security framework and the information system mixes them with variables from the monitors to produce the harmless
inputs to the information systems. The implication to information security systems is that the regulator (R) must be able to produce as many responses as the number of disturbances (D) from an environment [9], as shown in Figure 54.

FIGURE 53: VARIETY AND REGULATION

2.7 COMPARE ALLOCATIONS OF ECONOMICAL RESOURCES ON THE DIFFERENT SECURITY VALUE-BASED CHAIN FUNCTIONS

In this step, we do an analysis of how to allocate economical resources to the different security value-based chain functions deterrence, prevention, detection, response, and recovery [13]. In the same way, we analyze to determine how to allocate economical resources to each sub system the framework for adaptive information security systems. We have used the Delphi method [28] to construct an ideal security value chain for an information security system in an abstract situation [29] as shown in Table 11.

TABLE 11: ALLOCATION OF ECONOMICAL RESOURCES ON SUB SYSTEMS

<table>
<thead>
<tr>
<th>Sub system</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average distribution</td>
<td>18.75%</td>
<td>24.38%</td>
<td>23.13%</td>
<td>14%</td>
<td>19.38%</td>
</tr>
</tbody>
</table>

2.8 EDUCATE USERS OF INFORMATION SYSTEMS IN SOCIAL ENGINEERING AND ABOUT THE SECURITY FRAMEWORK

The ninth step is to educate users of information systems in the information system in social engineering and about the security framework. This could be done physically, electronically using mobile agents or knowledge bots [24] [14].
2.9 Evaluate the outcomes of the implementation of the framework for adaptive information security systems

The last step will be to evaluate continuously the outcomes of the implementation of the framework for adaptive information security systems and follow the plan, do, check, act process for continuous security improvement outlined in ISO27001 [6].

3 Conclusion and limitation

We have proposed a holistic and immune security framework in which we describe a methodology for considering culture of users and environments where information systems operate in developing information security systems. The methodology is also aimed at creating environments where technology serves people instead of people serving technology. We show the importance of applying both socio and technical controls in strengthening weak links that have been created by culture of users. The holistic and immune security framework provides adaptability features that make information systems learn to adapt to environments. The limitation is that the framework has never been applied in its totality and consequence there is no data to either validate the framework or compare this framework with other information security frameworks.

4 References


PERMISSIONS

Jeffy Mwakalinga, Stewart Kowalski and Louise Yngström are the authors of this paper. This work is original and does not violate any copyrights, rights and privacy of others. We retain the right all or part of this paper in our future work. We grant the ISSA 2009 organizers the right to publish this paper in the ISSA 2009 proceedings.
PAPER VIII
A Holistic and Immune System Inspired Security Framework

Jeffy MWAKALINGA
Department of Computer and Systems Sciences,
Stockholm University/Royal Institute of Technology,
16440 Kista, Sweden,
jeffy@dsv.su.se
and
Louise YNGSTRÖM
Department of Computer and Systems Sciences,
Stockholm University/Royal Institute of Technology,
16440 Kista, Sweden,
louise@dsv.su.se
and
Stewart KOWALSKI
Department of Computer and Systems Sciences,
Stockholm University/Royal Institute of Technology,
16440 Kista, Sweden,
stewart@dsv.su.se

Abstract
This paper presents a Framework for adaptive information security systems for securing information systems. Information systems today are vulnerable and not adaptive to the dynamic environments because initial development of these systems focused on computer technology and communications protocol only. Most research in information security does not consider culture of users, system environments and does not pay enough attention to the enemies of information systems. As a result, users serve technology instead of technology serving users. We apply the Systemic-Holistic Approach, the living systems theory, the Immune system, Systems theory, Cybernetics, and Socio-Technical systems to provide adaptability features, to consider culture of users and system environments in developing and designing information security systems. We apply socio-technical measures to secure the weak links in information security systems that have been created by culture of users. This security framework will help researchers and designers consider not only communication protocols and technology but also values of people like culture, legal, and traditions; environments where information systems run; and adaptive features in information security systems.

1. INTRODUCTION
Information security systems today are vulnerable and not adaptive to dynamic environments because researchers and designers of security for these systems have concentrated on technology and communication protocols [20]. Researchers and designers of security for these systems also have not focused on values like politics, culture, religions, laws and other social issues of the people using the systems [20] and the environments where these systems run [20] [13]. When a designer of a car wants to create a new car, the designer
has to apply the technology and standards that the market has to offer at that moment. If the current technology and standards for developing cars do not consider values of people using the cars and the environments where the cars are running, the resulting cars will fail to meet the demands of people and environments. The resulting cars will certainly not learn to adapt to the environments where they run. Likewise, developers of security for information systems created current systems by applying the existing security models, paradigms, frameworks and standards [20], which fail to consider values of people using the systems and environments where these systems operate. As a result, developers have been able to enforce technological controls but have failed to enforce socio-technical and social controls [13].

The problems addressed in this article include how to involve values of people using information security systems in the design, development, and operation of these systems; how to consider environments where information security systems run while developing these systems; and how to make them adaptive to environments. To address these issues the Systemic-Holistic Approach and the immune system were chosen as the fundamental concepts. The Systemic-Holistic Approach was selected because it is used for studying, investigating, designing, and analyzing security systems in different dimensions including values of a system as one whole system. This approach has been used as a base to understand security in relation to IT since the mid-1980’s [20]. In addressing the problems, the value-based chain as applied for security by [3] is also applied. Porter [16] developed the value-based chain model in 1985 to describe the concept of value adding activities in a company. Kowalski developed the value-based chain to address information security problems [8] as shown in Figure 55.

![Value-Based Chain](image)

**FIGURE 55: SECURITY VALUE-BASED CHAIN**

The value-based chain model for information security consists of deterrence, protection/prevention, detection, response, and recovery measures [8]. In any system there have to be measures to deter, that is to scare away attackers [13]. If one fails to deter attacks then one has to have measures to prevent attacks. If one fails to prevent attacks, the next step is to detect attacks. If one fails to detect attacks, the next step is to respond to the attacks. If one fails to respond properly to attacks the next step is to recover from attacks. This value-based chain could apply at different levels as example: family, national, and supranational. Every country has measures for deterring potential enemies. Countries announce in different media advanced nuclear weapons aimed at deterring potential enemies from attacking the country. The same apply to securing information systems. Every country has measures for preventing attacks and protecting her borders and territories. Every country has ways of detecting intrusions and spies from other countries. When a country is under attack, it must have measures of responding to the attacks. A country also has measures of recovering from attacks, which include restoring infrastructures and services.
2. THE HOLISTIC AND IMMUNE SYSTEM INSPIRED SECURITY FRAMEWORK

2.1. COMPONENTS OF THE FRAMEWORK

The security framework consists of the following sub systems: deterrence, protection, detection, response, recovery, management, and adaptability as shown in Figure 56. The management section consists of the agent creator, agent creator, integrated security system, system manager, special analysis, system fault-tolerance manager, two databases, and security management. The agent creator generates software mobile agents. The integrated security system manages certificates, authorization attributes and tokens, and providing security services for security framework and the information system, which implements the security framework. The special analysis performs special analysis of unknown and abnormal inputs as requested by the sub-systems. The system manager is responsible for managing and coordinating the operations of the whole system. The system fault-tolerance manager takes care of all the fault-tolerance measures in the whole framework. The two databases keep records of the whole framework. Security management is responsible for risk management, policy management, compliance management, and business continuity management.

2.2 THE ADAPTABILITY SYSTEM

The adaptability system provides measures to make the system and its subsystems learn to adapt to environments through the environmental analyzer, people’s value analyzer and threat analyzer. The adaptability system provides adaptability measures to the security framework and an information system.

2.2.1 THE ENVIRONMENT ANALYZER

The environment analyzer provides measures for considering environments where an information system is running basing on the Systemic-Holistic Approach [20], the Cybernetic structural model [9] and the Viable System model [2].

![Figure 56: Components of the Holistic and Immune System Inspired Security Framework](image-url)
thereby foresee how the whole security framework and the information system will react to those future disturbances. There is a table of transformations in memory of environmental disturbances, essential variables and regulatory disturbances. The controller of the desired essential variables for the security framework and the information system mixes them with variables from the monitors to produce the harmless inputs to the information systems. The adaptability system of the security framework is responsible for making sure that the whole system learns to adapt to dynamic environments. The adaptation system though the environmental analyzer collects data on environmental disturbances and stores them in a database system. The adaptability system creates a table of transformations to represents the possible outcomes of the actions of environmental disturbances and regulators on the Framework for adaptive information security systems as shown in Figure 57. This table of transformations represents every possible action that the regulator, Ri, can apply in response to every environmental disturbance, Dj, resulting into a state Eij, which are essential variables of the security framework and the information system that must be maintained to keep the framework and the information system in a stable state.

2.2.2 THE PEOPLE’S VALUE ANALYZER
The people’s value analyzer provides measures for analyzing how people’s culture, traditions, laws, and ethics affect information security system. The socio-technical system [13], Security by Consensus [13], and the Systemic-Holistic Approach [20] are applied to provide socio and technical controls where culture, traditions, laws, and ethics create a weak link in information security systems. We have established an informal cultural model for predicting the behavior of users to information security system of different cultures. This cultural model will help developers of security for information systems to predict the behavior and preferences of users of different cultures. The informal cultural model consists of the General Living System [14] ID component, Hofstede [10] component; Worldview [5] [17] component; Social Identity theory (SIT) [18] [17] component; Computer Literacy component; and General Education component as shown in Figure 58. The General living System Identity of an individual contains the cell, organ, organism, group, organization, nation, supranational [14] [20]. The cell represents a number. The organ is for location. An organism is a label for a common name. The last parts in the ID are organization, nation, supranational of a person. The Hofstede [10] component consists of the values: power distance index; individual vs. collectivism index; uncertainty avoidance index; femininity vs. masculinity index, and long-term vs. short-term orientation index.
levels. The computer literacy component shows practical and theoretical computer knowledge that an individual has. The general education component indicates education of a person.

This security framework is a function of the security value-based chain functions deterrence, detection, prevention, response, and recovery. These security value-based chain functions are in turn functions of the immune system features, living system features, and system properties, and people’s values. Kowalski [13] developed the security value-based chain functions deterrence, prevention, detection, response, and recovery. The security value-based chain functions apply the Cybernetic third order feedback mechanism to maintain the security framework into a stable state. The inputs to any subsystem are processed and the outputs are feedback to self-regulate the system.

2.2.3 The Threat Analyzer
We have created a model of the adversary of IT to analyze threats and understand tools, methods, and processes that an adversary applies to attack information systems. The adversary of IT investigates the tools, methods, and processes that an information system is applying to defend in the different subsystems like deterrence, prevention, detection, response, and recovery. The adversary also finds out how much financial resources were spend in tools, methods and processes for the deterrence, prevention, detection, response, and recovery sub systems. This information will help the adversary of IT to determine weaknesses in the different sub systems. The information gathered so far will assist the adversary of IT to decide whether it was possible to attack and get out fast without leaving any evidence.
3. COMMUNICATION IN THE FRAMEWORK

3.1. OVERVIEW

The system manager acts as subsystem 5 in the Viable System model [2], creates rules, identities, goals, and security policies of operations, and monitors the behavior of all the components in the security framework. The system manager activates the security framework and initializes all the components of the framework. The integrated security system performs identity management for the whole security framework and the information system where the security framework is operating. The integrated security system is the commanding and coordinating system and performs the functions of the subsystems 2 and 3 in the Viable System model [2]. All the components receive orders from the integrated security system. The immune system marks ‘self’ all the cells of the body. Those that are not marked ‘self’ are detected by the B-cells and T-cells and removed from the body. The integrated security system gives identities in the form of mini certificates [15] to all the components. The integrated security system gives identities in the form of mini certificates [15] to all the components and registers them into the database system. The agents that monitor the security framework and the information system detect objects that do not have identities and remove them from the information system. The security management component use the recovery sub system to perform the risk management, security policy management, compliance management, and continuity planning management services for the security framework and the information system.

3.2. CREATION OF MOBILE AGENTS

All components of the security framework request specialized mobile agents for providing security services in the security framework and the information system where the security framework is operating. The agent creator generates software agents as shown in Figure 59. In the immune system, there are two main types of protection cells, B-cells and T-cells. The bone marrow generates the B-cells while thymus generates the T-cells [12]. The generated agents have the immune system features multi-layered structure, local detection, diversity, autonomy, adaptability, dynamically changing coverage, identification are applied in the deterrence, prevention/protection, detection, response, and recovery [8] as shown in Figure 59. The agent creator provides the features of the immune system in the following way. Distributed – B-cells and T-cells detect the presence of infections locally without any coordination. The mobile agents act as cells in different deterrence, protection, detection, response and recovery sub-systems and every agent can detect intrusions and abnormalities locally. Multi-layered – The immune system apply multiple layers to provide overall immunity in body. The security framework has multiple protections in the deterrence, detection, prevention, response, and recovery sub systems. Autonomy – the immune system does not require outside maintenance or management. It autonomously classifies and eliminates foreign cells and it repairs itself by replacing damaged cells. This behavior is suitable but its implementation is challenging, as technology is still not ready, though it could be partly modeled by having an odd number of agents vote for a
decision. The agent creator train mobile agents of to make intelligent decisions. We apply the fuzzy logic controllers to train the agents to make decisions [7] [6]. Fuzzy logic is a concept in which objects or entities can partially belong to a set. The objects can for instance belong to a set $A$ by 50%. The range of belonging is 0-100%. In classical sets, either an object or an entity is inside or outside a particular set [7]. We apply the fuzzy logic in detection system decisions because the differences between normal and abnormal behaviors in networks are not distinct but fuzzy [7]. Adaptability – the immune system is able to detect and to learn to detect new foreign cells and retains the ability to recognize previously seen foreign cells through immune memory.

FIGURE 59: AGENTS’ GENERATION PROCESS

This feature is not new it in computer systems, though determining that a certain program is malicious with 100% is a hard problem. We apply the artificial neural networks and genetic algorithms [12] to train the mobiles agents to detect new abnormalities. Dynamically changing coverage - The immune system cannot produce a large enough set of detectors at any moment, so it maintains a random sample of its detectors that circulates throughout the body. This is because there are approximately $10^{16}$ foreign cells and these have to be distinguished from approx. $10^5$ "self"-cells. The security framework models this feature by having every agent to detect, prevent, or deter multiple intrusions, attacks, abnormalities and
viruses. Identification – In the Immune systems all the cells belonging to the body are marked as ‘self’. The immune system marks all the cells belonging to the human body as ‘self’, considers all other foreign cells as ‘non self’. The mobile agents recognize normal patterns and regard any other unknown patterns as malicious. The security framework models this feature by providing identities to the all the objects in the form of mini-certificates [15].

There is general prior knowledge with adapting features is stored in the database of gene libraries as shown in figure 59. This gene library contains genes that have been predetermined based on the priori knowledge [11]. These genes combine to form different solutions like the way you combine Lego blocks to form some solution [11]. The gene libraries provide information for the agent creator as shown in Figure 59. The agent creator acts like a bone marrow in the human body [12] [11]. The agent creator combines genetic expressions from the database of genetic expressions and artificial immune algorithms from the database of artificial immune system algorithms to create agents. The agent creator gives security agents specialized features for deterrence, prevention, detection, response, and recovery sub systems. The agent creator applies the priori knowledge to create different normal and abnormal profiles for the deterrence, detection, prevention, response, and recovery sub systems. The agents that pass this test go the body and start monitoring in the human body. The agent creator applies the Negative selection algorithm to test the agents for deterrence, detection, prevention, response, and recovery sub systems. This algorithm is based on [12] [11]. The sub systems of the security framework request mobile software agents from the agent creator. The agent creator trains all the agents before releasing them into the real environment. In the first phase of the training, the agents pass a negative selection test [12]. The negative selection algorithm:

(a) Generate normal traffic profiles for the sub system Deterrence (likewise for the other subsystems detection, prevention, response, and recovery) from a library of the latest available normal traffic for this system.

(b) Let the deterrence (likewise for the detection, prevention, response, and recovery) agents match the generated profiles of normal traffic.

(c) If the deterrence agents match these normal traffic profiles then we reject the agents.

(d) If the deterrence agents do not match the normal traffic, profiles for this system then keep these agents.

(e) Generate abnormal traffic profiles for the sub system Deterrence (likewise for the other subsystems detection,
prevention, response, recovery) from a library of the latest available abnormal profiles and intrusions for this system.

(f) Let the deterrence (likewise for the detection, prevention, response, and recovery) agents match the generated abnormal traffic profiles.

(g) If the deterrence agents do not match, the abnormal traffic profiles then reject the agents.

(h) If the deterrence agents match, the abnormal traffic profiles then keep the agents.

In the immune system, the negative selection algorithm produces immature B-cells. These B-cells monitor in the human body. The immune system clone the B-cells that perform best and store their detecting features are stored in memory cells [12]. The agent creator applies the clonally selection algorithm [12] [11] to clone the best performing mature agents for the deterrence, detection, prevention, response, and recovery sub systems. The clonally selection algorithm for the agents:

(I) initialize the population of mature agents for each sub systems deterrence, detection, prevention, response, and recovery.

(II) Apply the fitness function to determine the fitness of each mature agent of the subsystems.

(III) Select the highest scoring mature agents based on fitness function, genetic algorithm, for each sub system.

(IV) Clone new mature agents for the sub systems through hyper mutation.

(V) Determine the fitness of the newly generated children and store the features of these agents in the gene libraries.

(VI) Replace the less successful old mature agents of the subs systems with the new children that have high scores.

The agent creator records the features of the most successful agents, according to policy specified criteria. The agent creator applies these features to improve the features of next generation of agents.

The mobile agents have life times according to the security policy even as cells in the human body have life cycles. When the lifetime of the agents is over, the agent creator replaces them with better agents.

The fault tolerance manger performs fault tolerance services in every component of the security framework. The fault tolerance manager is responsible for error detection measures, damage assessment measures, damage confinement measures, error recovery measures, fault treatment, locator, and continued service measures in the Framework for adaptive information security systems. The adaptation system acts as sub system 4 in the Viable System Model [2]. The adaptation system is concerned with future, adaptation, planning of the security framework. The adaptability system has specialized mobile agents for environment analyzers, people values analyzers, and threat analyzers that perform adaptability services in every component. The adaptability system acts as system no. 4 in the Viable System model [2]. The adaptation system collects data on environmental disturbances from all the components and stores them in a database. The environmental disturbances can come from the local, embedded, and total environments. For an information system, the environments could include the operating systems, hardware systems, electric and electronic systems, intranets and extranets, internet, internet service providers. The adaptability system applies these data to create probabilistic models and to forecast the future environmental disturbances [9]
and thereby foresee how the framework will react to those future disturbances.

3.3. SECURITY OF MOBILE AGENTS

We secure and train the mobile agents before allowing them to perform different tasks in the security framework and an information system where the security framework operates. The Agent creator generates mobile agents with features from the immune system. The special analyzer certifies the agents locally but in future, there could be an independent body for certification of agents. The agent creator and the requesting sub-system mutually authenticate each other before communicating further. Every sub-system has many different agents for doing diverse kinds of tasks in this sub-system. To provide authenticity and integrity of agents the agent creator signs the agent. To provide confidentiality security service, the agent creator seals the agent by using the public key of the special analyzer, which is acting as the agent certifier. The agent creator sends the agent to the special analyzer. The special analyzer opens the message by the private key and verifies the signatures of the agent. The special analyzer checks whether the agent is behaving in accordance to the specifications of the agent requestor. The special analyzer puts a trust level and its digital certificate [4]. The analyzer signs the agent, protects it, and sends it to the sub-system. The security framework protects mobile agents and the baggage they carry. During the handshake, the sending and receiving sub systems exchange session secret keys to secure communication. The security framework secure communication of agents in the deterrence, detection, protection, response, and recovery sub systems and other components of the security framework in the following way. The security framework uses the session keys to protect the agents and the messages. The sending system signs the agents and the baggage. The receiving sub system verifies the integrity and authenticity of the agent and messages by verifying the signature. Protecting agents when they are visiting a sub system is different from protecting agent servers because agents do not have their own processors and they cannot extend the home sub system, but have to rely on the environments provided for them there.

3.4. PROTECTING THE SUBSYSTEMS

There are a number of technologies for protecting agent systems. The home agent servers verify the correct state of an agent before accepting the agent and before authorizing the agent to access objects. The security framework policy is to sign agents using the private keys of the agent creators and dispatchers. The sub-system opens the message using its private key. It verifies the signatures of the agent creator and of the special analyzer. The sub-system also verifies the authenticity of all the agent servers that where the agents visited before the current sub-system. The sub-system then notifies the agent creator and the certifier that it has received the agent. All the agent systems must sign the information collected by the agent.

3.5. SENDING AN AGENT FOR CLONING

If the agent is very successful in deterrence, protection, detection, response and recovery functions, other tasks in accordance to the specified criteria the agent will be sent to the agent creator for cloning. Before sending the agent, the sending sub system and agent
creator will authenticate each other. The sending system creates a secret key and protects it with the public key of the agent creator, the sending sub system then signs it. When the agent creator receives the agent, it verifies the signature of the sending sub system. The agent creator will then clone the agent and will send the agent back though the agent certifier, the special analyzer. A copy of the agent is stored in the database of the agent creator.

4. VALIDATION
This section briefly discusses validation of the Framework for adaptive information security systems. In validating, the whole framework it was necessary to understand whom the adversary of information systems was and how to model the adversary of IT. We validated the framework by criteria recommended by the functional requirements of Common Criteria [3], the National Institute of Standards and Technologies (NIST) [19], Systemic-Holistic Approach (SHA) [20] Socio-Technical System [13]. We also validated the Framework for adaptive information security systems by using structured interview of security experts and master students in information security. The results of interviews show that the Holistic and immune inspired security framework had sound adaptability features to make information systems survive in dynamic environments. The results show also that the security framework is suitable to involve values of people in developing, designing and in operations. Table 12 shows the results of question: This Framework for adaptive information security systems its subsystems will be useful in your organization. The results further show that the security framework could integrate the different technical solutions since there is no holistic security framework, currently, that can make the technical solutions fit together. One expert commented that the security framework could holistically structure the information security work in organizations. It could also be used to consider environments where information systems run in the development, design, and operations stages. However, there were some concerns as to how effective this security framework would be when implemented in organizations.

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
<th>Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>7</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Agree</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Do not agree</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Need more info.</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

5. CONCLUSION
This security framework applies the features of an immune system and general living systems to make information security system learn to adapt in dynamic environments. The holistic and immune inspired security framework involves culture, traditions, and other social issues in designing and developing information security systems. We apply socio-technical measures to strengthen the weak link that have been created by culture of users. The security
framework also considers environments where an information system is operating. This security framework is a function of the security value-based chain functions deterrence, detection, prevention, response, and recovery. We apply software mobile agents to provide security services.

6. REFERENCES


PAPER IX
Secure E-learning using the Holistic and Immune Security Framework

Jeffy Mwakalinga, Stewart Kowalski and Louise Yngström
Department of Computer and Systems Sciences,
Stockholm University / Royal Institute of Technology, Sweden
jeffy@dsv.su.se, stewart@dsv.su.se, louise@dsv.su.se

Abstract

This paper describes how to secure e-learning systems by applying the Holistic and Immune Security Framework. E-learning has great potential for developing communities but security of e-learning systems has not been fully addressed. We have developed a security framework that considers culture of users and environments where information systems operate. We apply the holistic approach to secure e-learning systems. The holistic and immune security framework is a function of the deterrence, prevention, detection, response, and recovery system. The security framework makes an E-learning system learn to adapt to environments and to culture of users. We apply the principles of immune system to secure E-learning systems. We describe how to secure the weak links that are created by culture of users in E-learning systems.

1. INTRODUCTION

E-learning is a special form of learning in which material is delivered electronically to learners in different cultures and environments [6]. We have assumed that users in E-learning systems is just another component which must follow instructions as other technological components, which has resulted in people serving technology and not technology serving people. Culture affects the way users interact with different information systems [14]. E-learning systems should learn to adapt to environments where they operate and to cultures of users. An e-learning environment consists of five layers as shown in Figure 60. The first layer is users’ gate. In this gate, different users like owners, designers, developers, teachers, authors, reviewers, learners, and administrators are identified and given access the e-learning system. The second layer contains the common management services like user management, collaboration management, and courses’ catalog management. The third layer has e-learning services and consists of learning content management system (LCMS) [20], learning management system (LMS), assessment, evaluation, business operations, and administration. The learning content management system is concerned with content development in which authors, reviewers, content experts, administrators submit, review edit contents. Learning management services are concerned with content delivery services and interaction services with learners. The fourth layer consists of databases for all the information of the e-learning environment. The fifth layer consists of network infrastructure. This layer has delivery networks for audio, voice of IP, video, IP data, servers, and protocols like FTP, HTTP, SOAP, XML, and TCP/IP as shown in Figure 60.

2. HOLISTIC AND IMMUNE SECURITY FRAMEWORK

We have created a holistic and immune security framework as shown in Figure 61. The security framework bases on the Systemic-Holistic Approach [11] and the principles of the immune system [8]. In the security framework, we apply the holistic approach to
secure information systems. We believe that there is much more to information security than technology and communication protocols. Therefore, we also consider different factors that affect information security like environments, culture, laws, and ethics of users, economy, and other issues. The security framework is a function of value-based chain functions [2]. The value-based chain for information security was developed by [3]. The security value-based chain contains deterrence, prevention, detection, response, and recovery functions. The security framework consists of the following components: the management system, the adaptability system, the deterrence sub system, the prevention sub system, the detection sub system, the response sub system, and the recovery sub system. The management system contains the agent generator, databases, integrated security system, special analyzer, system manager, security management, and fault tolerance management. The agent generator creates agents that provide security services to the different components of the security framework and the e-learning system. The integrated security system manages certificates, smart systems, authorization systems, and database systems.

We apply the special analyzer to study all the inputs that are new to the different components of the security framework and the e-learning system. The system manager takes care of administration of the security framework. Security management takes care of risk management, policy management, compliance management, and business continuity management in the E-learning system. The fault tolerance manager is responsible for detecting errors, assessing damages, confining damages, treating faults, locating faults in the security framework and the in the e-learning system [6]. The adaptability system provides measures for making an e-learning security system learn to adapt to environments. A deterrence sub system scares away attackers of an e-learning system. Prevention sub system guides the territory of an e-learning system and its entities. Detection sub system detects attacks and abnormalities in an e-learning system. Response sub system responds to attacks and intrusions in an e-learning system. Recovery sub system restores an attacked e-learning system back to normal. In every sub system, we analyze, control and process all the inputs and then take out poison in the inputs by applying the feedback systems from cybernetics [11] as shown in Figure 61.

2.1. PROVISION OF SECURITY IN AN E-LEARNING SYSTEM

The holistic an immune security framework methodology that we apply for securing an e-learning system is as follows [21]. We start by analyzing the threat agent to the e-learning systems based on the socio-technical economical model. Then we classify the assets of the e-learning system and perform risk management. The next step is to analyze environments where the e-learning system is operating. Thereafter we assess the effects of culture, laws, ethics, and other social issues of e-learning system’s users to the information security of the system. In the next step, we apply socio-technical measures [19] to secure the weak links that have been created by culture of e-learning system’s users. Then we provide measures for making an e-learning security system learn to adapt to environments and culture of users.

The next step is to analyze how to distribute economical resources to the deterrence, prevention, detection, response, and recovery security functions of an e-learning system. Then we educate users electronically on social engineering and other security issues. In the last step we evaluate the outcomes of the implementation of the holistic and immune security framework based on the plan, do, check, and act process for continuous security improvement outlined in ISO27001 [22].
First layer: Users’ gate (owners, designers, developers, teachers, authors, content experts, learners, and administrators)

Second layer: common management services (user management, collaboration, courses’ catalog management)

Third layer: e-learning services (learning content management services, learning management services, assessment, evaluation, business operations, administration)

Fourth layer: databases

Fifth layer: network infrastructure (delivery networks, audio, voice of IP, video, FTP, HTTP, SMTP, SOAP, XML, TCP/IP, servers, etc)

FIGURE 60: LAYERS OF AN E-LEARNING SYSTEM AND THE HOLISTIC IMMUNE SECURITY FRAMEWORK

FIGURE 61: THE MODEL OF THE HOLISTIC AND IMMUNE SECURITY FRAMEWORK
All the components of an e-learning system users’ gate, common management services, e-learning services, databases, and network infrastructures are given identities and means to authenticate them. These components are then registered in the database of the security framework. We secure e-learning system’s information when it is being processed, stored in databases, in transmission, when collecting information, and when displaying, in all components of the e-learning system.

The most common scenarios in e-learning include teacher centered, evaluation centered, and collaboration centered [4].

In teacher centered scenarios a teacher has to provide material, monitor students, assess students, learn about students, and interact with learning environments, collaborate with other teachers in cases where different modules are integrated. Risks in this scenario include bogus material could be loaded to course websites. Students could gain access to teachers’ login credentials. Course material could be changed by unauthorized people; course web sites could be attacked [5]. The software agents provide authentication, authorization, non-repudiation, availability, integrity, privacy, anonymity, and confidentiality security services. Teachers should be identified, authenticated, and authorized before interacting with e-learning environments. The software agents provide privacy and anonymity for teachers. There are some cases where identities of teachers and e-learners are necessary to remain classified. This is especially applied when teachers and e-learners are working in intelligence, military and other government ministries where it is necessary to remain classified. In the evaluation cantered scenario, the risks include: people masquerading as students; and students getting outside help in writing tests; submitted answers could be copied or altered by non authorized parties; tests could be accessed beforehand; marks could be changed [5]; and so on. In this scenario, software agents provide authentication, authorization, privacy, integrity, availability, confidentiality, anonymity, and non-repudiation. The e-learning security system identifies, authenticates, and authorizes e-learners before performing any tasks. Evaluators should also be identified, authenticated and authorized before performing any assessments. Privacy should be provided so that marks, grades and other classified information could remain secret. Integrity is provided at all levels so that assessed and non-assessed information should not be modified. The servers and all systems providing e-learning services should be available all the time. Some e-learners and teachers prefer anonymity so software agents provide anonymity security service. Both students and evaluators sign information. In collaboration-centered scenarios, e-learners work in groups from different locations. The software agents register, monitor, protect, and assess communications among students [4]. In this scenario, the e-learning security system identifies, authenticates, and authorizes e-learners before participating in collaboration groups. The software agents provide integrity, confidentiality, non-repudiation, privacy security services in this scenario. Different cultures prefer different mechanisms for implementing security services due to different levels of computer literacy and different cultural values. The Software agents provide multiple authentication schemes, multiple identification schemes, multiple authorization schemes, multiple non-repudiation schemes, multiple confidentiality schemes, and multiple integrity schemes, multiple anonymity schemes, and multiple privacy schemes. We provide security services using software agents.

2.1.1. SOFTWARE AGENTS PROVIDE SECURITY SERVICES.

We apply software agents to provide security services in the different components of an e-learning system and the security framework. All components of the security framework request specialized software agents for providing security services in the e-learning system. We apply the principles of the immune system to create software agents. The immune system has B-cells and T-cells. The bone marrow creates B-cells while the thymus generates T-cells [8]. We apply the immune system features, which include multi-layered structure, local detection, diversity,
autonomy, adaptability, dynamically changing coverage, and identification. The agent creator provides the features of the immune system in the following way [8]. The principle of distribution – B-cells and T-cells detect the presence of infections locally without coordinating with each other. The mobile agents perform tasks in analogy to immune system cells in different subsystems. Every software agent can detect intrusions and abnormalities locally. The multi-layered principle - The immune system applies multiple layers to provide overall immunity in body. The security framework provides multiple protections in e-learning components. The principle of autonomy – The immune system autonomously classifies and eliminates foreign cells and the immune system repairs itself by replacing damaged cells. This behavior is suitable but its implementation is challenging as technology still is not ready, but we model this partly by having an odd number of agents vote for every decision. The agent creator trains software agents of to make intelligent decisions. We apply the fuzzy logic controllers to train the software agents to make intelligent decisions [7]. Fuzzy logic is a concept in which objects or entities can partially belong to a set. The objects can for instance belong to a certain set by 50%. The range of belonging is 0-100%. In classical sets, either an object or an entity is inside or outside a particular set [7]. We apply the fuzzy logic in detection system decisions because the differences between normal and abnormal behaviors in networks are not distinct but fuzzy [7]. The principle of adaptability – the immune system is able to detect and learn to detect new foreign cells and retains the ability to recognize previously seen foreign cells through immune memory. This feature is not new in computer systems, though determining that a certain program is malicious with 100% is a hard problem. We model this by artificial neural networks [8] and genetic programming. The principle of dynamically changing coverage - The immune system cannot produce a large enough set of detectors at any moment, so it maintains a random sample of its detectors that circulates throughout the body. This is because there are approximately $10^{16}$ foreign cells and these have to be distinguished from approx. $10^5$ ‘self’- cells. We model this principle by having one agent detect, prevent or deter multiple intrusions, attacks, abnormalities and viruses. The principle of identification –The immune system marks all the cells belonging to the human body as ‘self’, considers all other foreign cells are as ‘non self’. The mobile software agents recognize normal patterns and regard any other unknown patterns as malicious. We model this principle by providing identities to the all the objects of a system in the form of mini-certificates [9]. We have designed a system of mobile software agents for providing different security services in the sub systems. These include helper and killer agents, authentication agents, confidentiality agents, authorization agents, Non-repudiation and integrity agents, and third-order feedback agents system. We secure the mobile software agents before performing different tasks in the security framework and in the e-learning system as described in [10].

3. ADAPTABILITY OF THE E-LEARNING SECURITY SYSTEM

Users of different cultures and in different environments use e-learning systems. An e-learning security system has to learn to adapt to the values of users of different cultures and environment where it is operating. In order to provide measures for adaptability we apply different analyzers to study environments, culture of users of e-learning systems. We also study models that adversaries apply to attack e-learning systems.

3.1. ENVIRONMENTAL ANALYZER

The environment analyzer provides measures for analyzing environments where an e-learning system is running. The analysis bases on the Systemic-Holistic Approach [11], the Cybernetic structural model [1] and the Viable System model [12]. Examples of environments affecting information systems include an operating system, computer hardware, intranet, Internet Service Provider
The adaptability system of the security framework monitors and records the environmental disturbances, the essential variables, and regulatory variables to the e-learning system over a period of time [1] as shown in Figure 62. The adaptability system receives environmental disturbances as inputs through the different components of the e-learning system and the security framework. The system creates a table of transformations of environmental disturbances, essential variables and regulatory variables. There is a controller of the desired essential variables for the e-learning system and the security framework. This controller mixes the data in the transformations table with the monitored environmental disturbances, essential variables, and regulatory variables to produce the harmless inputs to the e-learning system. The table of transformations represents every possible action that the regulator could apply in response to every environmental disturbance, resulting into a state with the essential variables that must be maintained to keep the e-learning system and the security framework in a stable state. The adaptability system applies the recorded data to create probabilistic models to forecast the future environmental disturbances [9] and thereby foresee how the security framework and the e-learning system would react to those future disturbances. The adaptability system of the security framework is responsible for making sure that the e-learning security system learns to adapt in dynamic environments.

FIGURE 62: THE MODIFIED CYBERNETIC STRUCTURAL MODEL

3.2. E-LEARNING SYSTEM USERS’ CULTURAL VALUES ANALYZER

There have been concerns about the role of culture in information systems [13]. Culture has been defined as a set of values, attitudes, and behaviors that people learn or are passed over to them over a period of time [14]. There is a general agreement among information system researchers that culture affects the way individuals interact with complex information systems [13]. This applies to e-learning systems as well. There is a need to develop models to measure the effect of culture on individuals when interacting with information systems. Researchers made a survey in three different cultures, Moroccan, Surinamese, and Dutch on user experiences on e-government sites [14]. The conclusion was that people with different culture backgrounds experience different problems in using e-government applications. We could deduct from this conclusion that users with different cultural backgrounds experience different problems in using e-learning systems. The e-learning users’ value analyzer provides measures for analyzing how users’ culture, traditions, laws and ethic affect e-learning security system. We have established an informal cultural model for predicting the
behavior of e-learning system users of different cultures. The informal cultural model bases on the General Living System [15], Hofstede’s Culture Consequences [16] Worldview theory [17], Social Identity theory [18], and computer literacy. This cultural model predicts the behavior and preferences of e-learning system users of different cultures. In some cases, cultural values create vulnerabilities and weak security links in e-learning systems. We apply the socio-technical system [19], Security by Consensus [19], and the Systemic-Holistic Approach [11] to provide socio and technical security controls where culture, traditions, laws, and ethics create a weak link in e-learning security systems. We apply knowledge that we again from the e-learning users’ values analyzer to understand, explain, predict and to control. We create policies and procedures to forbid actions that create weak security links in e-learning security system. The results from the e-learning users’ values analyzer will show us actions that create vulnerabilities in an e-learning security system. We will assign values to different actions. We forbid actions whose consequences bring negative values.

3.3. E-LEARNING SYSTEM THREAT ANALYZER

The threat analyzer deals with understanding the methods, tools and capacity of adversaries, which they apply when attacking e-learning systems. The adversary of e-learning systems investigates the tools, methods and processes that an information system is applying to defend in the different subsystems: deterrence, prevention, detection, response and recover. The adversary of e-learning systems also finds out how much financial resource e-learning systems allocate in tools, methods and processes for the deterrence, prevention, detection, response, and recovery sub systems. This information helps the adversary of e-learning systems to determine weaknesses in the different sub systems. The information gathered so far will assist the adversary of IT to decide whether it was possible to attack and get out fast without leaving any evidence.

4. CONCLUSION

We have described how to protect an e-learning system by applying the holistic and immune security framework. We apply the holistic approach to provide secure e-learning system using the principles of the human’s immune system. Information security is not just technology and communication protocols and so we consider other factors like environments and values of users of e-learning systems. The security framework provides measures that help an e-learning system learn to adapt to environments and to culture of e-learning users. We provide multiple security service schemes to accommodate users with different computer literacy levels and cultural backgrounds. The mobile agents provide security services in an e-learning system. Limitation is that the security framework has not yet been fully implemented. Future work will include fully implementing the security framework and to measure performance of the framework.

5. REFERENCES


[14] N. Van Dam, V. Evers, and F. Arts, Cultural user experience, issues in e-government: Designing for a Multicultural society. Digital Cities 3, University van Amsterdam, Netherlands. 2003


PAPER X
Modeling the Enemies of an IT Security System - A Socio-Technical System Security Model

Stewart KOWALSKI and Jeffy MWAKALINGA
Department of Computer and Systems Sciences,
Stockholm University, 16440 Kista, Sweden,
stewart@dsv.su.se, jeffy@dsv.su.se
ABSTRACT
This paper presents a socio-technical security model for security systems that include both the system being defended and the attacking system. We first model security as a ratio or function of the states that an attacker can produce over the states that defend can control. We then subdivide the control states of a defending systems using the security value chain and socio technical system security model. The paper then presents two attempts to validate the acceptance of the defense model using cross culture surveys of individuals from over 20 different countries indicate culture variation in security modeling. An example of how an attacker can model an attack strategy is given at the end of the paper. The paper concludes with a discussion of how the modeling can be new research in modeling criminal organization using effective based operations methodology.

KEY WORDS
Enemy of IT, deterrence, prevention, detection, response, and socio-technical model, center of gravity

1. BACKGROUND AND INTRODUCTION
One of the systemic security problems with information and communication technology (ICT) is that it is a double-edged sword. That is to say, it can be used for constructive and destructive purposes [10]. For example, remote computing technologies permit individuals to work from home but they also permit hacks to attack them from their homes. Over the years, we have seen continuous waves of new technologies to construct better and better security solutions for ICT systems. First, simple reference monitors were developed to monitor and separate different users. Then, multipurpose operating systems, firewalls, intrusion detection systems, and prevention systems were developed. These point security products provide solutions to a single problem rather than systems solutions. However, many of these technologies do not meet stakeholders’ expectations and it could take between two and ten years for a security product to mature [1]. However, how long shall we continue to be reactive [18] to yesterday’s hacker technologies? We have to be proactive by studying hackers’ technologies and by predicting their next moves and making our systems adaptive [18].

In the beginning of ICT era, hacking was for fun and to get attention, but hackers developed it into a business and the cyber criminals created their own business models [18]. The goal of cyber criminal or hackers like all criminals is to increase revenue flows at minimum costs [18]. One of the cheapest ways of obtaining information is by social engineering. Results presented by [11] show that social engineering is a technology that has a good probability to succeed at minimal cost. Social engineering is a type of attack against the human factors in which a victim is persuaded to hand over sensitive information. Hackers succeed in social engineering because people are not trained to be suspicious of each other [2]. Technical and non-technical means were used by Mitnick [2] to obtain the source codes of operating systems and telecommunications devices to study their vulnerabilities. The security systems today protect information against amateur computer intruders like the script kiddies but not against professional criminals [2].
For hackers information is the currency and consequently more information implies more money [18]. To get more information one should perform more attacks. Since one of the primary goal of computer science is to automate and therefore in order to gain more information the hackers automate attacks. In order to cut costs the hackers use downloadable toolkits to perform almost any kind of IT systems attack. However, there is some exception in the community to focus on cutting costs. There are other groups like the Advanced Persistent and Threat (ATP) hacker groups, which tend to perform attacks independent of the cost [13]. Their goal is to gain access to the defense, financial or governmental information at any price. Bar-Josef has suggested that some possible example of ATP activities can include the Stuxnet worm and the attacks on Estonian and Georgian governments in 2007 [23].

This paper is divided into 5 sections. Following this introduction in section 2 we briefly describe the history and organization of IT hacking. In section 3 we introduce a socio-technical systems security model. In section 4 we combine the IT security model and the IT hacking organization model and give an example of a high level insecurity attack strategy matrix. The paper concludes in section 5 with a discussion on methods that can be used to collect more information on the enemy’s socio-technical systems models to better understand predict and control them.

2. GENERATIONS AND ORGANIZATION OF THE ENEMY OF IT SECURITY

2.1 GENERATIONS OF THE ENEMY OF IT

According to Rogers, there are four generations of hackers or as the author refer to enemies of IT systems security [8] [9]. The first generation was a group of creative programmers and scientists in the 1960s mostly from MIT and Stanford institutes. This group was much respected. The members of this group were called “gurus.” The second generation was a group of computer hackers of both hardware and software for mainframes and personal computers in the 1970s. Some of them founded major computer companies. The third generation concentrated on breaking computer games and copyrights in the 1980s. The fourth generation is a group of hackers from the 1990s up to today. This is a group of script kiddies, cyber punks, insiders, coders, professionals, and cyber terrorists. Script kiddies have very limited computer skills and depend on programs and tools that are freely available on the Internet. Script kiddies are motivated by media attention. They can cause a great deal of damage by launching attacks like distributed denial of service attacks (DDoS), but they do not necessary understand how a computer attack works. Cyber punks have better computer skills than script kiddies and have some understanding of how a computer attack works. Insiders are usually computer knowledgeable and are employees, ex-employees, or contractors. They are able to carry attacks because they have access privileges to computer and information systems. Most of them appear to be are
motivated by revenge. Coders are those hackers with technical skills to write scripts and automated tools for attacking computer and information systems. They act as mentors to the script kiddies and other related groups. This is a dangerous group and is motivated by power and prestige. Professionals are a group of thieves, criminals, corporate espionage who are highly trained and motivated; they are like guns for hire. There is not much information about this group. Cyber terrorists appear to be having its back ground after the fall of the intelligence agencies in the Eastern bloc. They are well funded and well trained and could carry out information warfare. They are motivated by political and criminal activities [8] [9]. Next, we discuss the organization of hackers.

2.2 THE ORGANIZATION OF HACKERS

The hacking community appears to be organized in the following way as Figure 63 outlines. There are six groups in the organization. The first group is of researchers. They investigate systems to find vulnerabilities in applications, operative systems, frameworks, and in different products [19]. Notice here that there are two dimensions of vulnerabilities [9] the objective and subjective vulnerabilities. The objective vulnerabilities depend on the social, political, economical, and demographical entity that determine the vulnerability to cyber attacks. Subjective vulnerabilities depend on the person’s or entities self-perception on the risk of becoming a victim of an attack.

The next group is software coders, who write intelligent malicious toolkits and programs like Trojans for monitoring, capturing, retrieving information, and covering their activities.

FIGURE 63: OVERVIEW OF HACKERS TYPES

The marketing for their programs is done in the underground forums. As an example, one master hacker wrote a phishing toolkit for gathering information from victims and put it on the Internet [21]. The other hackers downloaded the toolkit and started using it on the websites of their choices. The master hacker had provided cloud storage for the gathered information. Once retrieved the information would securely stay in the cloud where only the proxy hacker who was applying the toolkit would access the information. It was supposed to work exactly as in the cloud computing. However, what the proxy hackers did not know was that the master hacker was able to access all the information that was gathered by all the proxy hackers [19]. The next group is botnets army keepers, which maintain and increase the army of botnets [21]. They control the botnets using modern technologies by issuing commands and controls [21]. Now hackers are using the social networks to control the botnet armies [18]. Social networks have brought trust among friends of sharing different kind of information and since social networks are very tender there appear to have much vulnerability with very few strong security controls. The next group consists of attackers, which include all kinds of hackers that perform the attacks. Some attackers use botnets, which they hire at prices that are set by botnet army keepers to gain information.
Some attackers use free tools that are available on The Internet. One example of the botnet is called ‘Mumba’ [20]. The botnet was created by a criminal group called Avalanche group, which had installed information stealing software in 55000 computers. As a result, hackers retrieved 60 GB data. The data include bank accounts credit card numbers and social networking web sites that were stored in one server [20]. The acquired information is sold to the consumers [21]. The next group consists of consumers who use the stolen information and translate it into money [21]. Consumers use the stolen information by creating fake credit cards, transferring money from victims’ online banking accounts and to create fake identities. The helpers group includes mules and entities who offer free hosting servers for storage of stolen information. Mules are a network of people who transfer stolen money from banks in one country to other countries at commissions. The next section presents the social-technical economic model.

3. THE SOCIO-TECHNICAL SECURITY MODEL

The Social-technical model is aimed at addressing security problems at different levels and perspectives. This model has two main components: the value chain and three general abstraction levels. The value chain model was established in industry to describe the concept of value creating security activities in a large telecommunication supplier [15]. The abstraction levels of the model are taken from security modeling work in the early 1990 [3]. In system science the general premise is that are three types of systems: living; abstract; and concrete. These systems share some properties, which can be used to explain, predict, control, create, and destroy any systems with a given degree of certainty [3]. The Socio-technical model is outlined in figure 64.

![Value-based chain model](image)

FIGURE 64: THE SOCIO-TECHNICAL SECURITY MODEL

The security value based chain model was developed for commercial security targets in the telecom industry [7]. Applying this to value based chains we have an abstract information security value chains, which contains deterrence, protection, detection, response, and recovery sub systems [5]. A security system should have measures to deter attackers from attacking an information system. If the security system can not deter attackers then it has to have measures to control or prevent attacks to an information system. If the security system can not deter or prevent attacks,
the next step is to detect attacks. If the information security system can not deter, prevent or detect, it has to have measures to respond to attacks. If an information system can not deter, prevent, detect, or respond then it should have measures to recover after attacks

3.1 Value Chain Model
The value chain model is a general security model that could be applied at different personal, family, organizational, national, and supranational levels. For example, at the national level there are sub systems that control measures: for deterring intruders; for protecting the inside of the nation and natural boundaries; for detecting pries; for responding to an attack; and for recovering from an attack. When the government makes a budget for the defense ministry, they have to allocate the budget to the different departments of the ministry. The question is, how much of the total military budget to allocate for deterrence department? How much of the total military budget should be allocated for protection, detection, response, and recovery departments? In the same way an analysis is needed to determine how much of the total security resources should be allocated to the different sub–systems of the of an information security system in a company. If a security manager of a company was to be given a budget of two million dollars to spend on information security in the company how will it be spent. [3] That is to say, how much would the manager use on the deterrence sub-system, on protection sub-system, on detection sub-system, on response sub-system, and on recovery sub-system. Some sub systems may require more resources depending on the nature of the information system.

A survey was made of master students in information security to help understand which value-based chain functions are perceived to be the more important. We asked respondent to imagine they were security managers of companies. We made a survey of 60 students from France, Sweden, Sri Lanka, Libya, USA, Libya, Taiwan, Thailand, Uzbekistan, Spain, Peru, Pakistan, Nepal, Iran, India, Iceland, China, Brazil, Bangladesh, and Serbia Montenegro. We made this survey to understand whether culture affect the decisions, which users make when deciding, which of the five security value-based chain were more important. The average of the allocations is shown on figure 66.
We also compared results of bachelor and master students. A second survey was made on 37 international master students in information security from Austria, Bangladesh, China, Greece, Hong Kong, India, Iran, Nigeria, Pakistan, Sweden, Tanzania, and Turkey. Every student was to assume to be working for a Global Socio-Technical Security Group. The student was to setup a social technical security system to decrease plagiarism at the Stockholm University. The students were to outline a budget of how 10 million monetary units would be spent using the security value chain of deter, protect, detect, respond, and recover functions.

The results from the second survey are outlined in figure 65. It is interesting to note that all the students from China allocated less than 10% on the prevention, response, and recovery sub systems but allocated around 47% of the total budget on detection sub system. Note also that Nigeria allocated nothing on the prevention and detection sub systems. Turkey on other hand spent 62% of the whole budget on detection sub system. In this scenario, the detection function was perceived to be more important than other functions with the average of 37% of the whole budget. The recovery sub system got the lowest allocation with average 10.4% of the whole budget.

Another example of the security value-based chain concept can be applied in a more concrete manor [6]. This concrete information security value-based chain consists of the hardware, software, systems, and services in a computer. The manufactures of hardware add some value when they create hardware and put into computers. The software producers add another value when the put software into the computer. The other vendors add value by putting systems into the computer. Then other vendors add value to the computer by putting services. Let us assume that computer hardware producers spend 100 dollars to create the hardware and expect to sell for 150 dollars as shown in figure 67. In the same way, software producers spend 50 dollars to create computer software and sell it for 70 dollars. Let us assume those who create systems spend 60 dollars and sell them for 80 dollars. Assume that vendors who create services spend 40 dollars and sell for 60 dollars. Let us assume that distributors, whole sellers, and retailers charge 100 dollars and so the end customer buys a computer for 460 dollars.
The computer in this case has no security services. Let us assume that producers and vendors decide to add the basic security services into the computers. Because of this the computer hardware producers spend 120 dollars to add security measures and expect to sell it for 180. The software vendors spend now 70 dollars to produce software with security and expect to sell them for 100 dollars. The vendors of systems now spend 80 dollars and expect to sell for 110 dollars. The vendors of services spend now 60 dollars, and are expected to sell them for 80 dollars. Let us assume that the distributors, whole sellers, and retailers charge now 150 dollars per computer. Now the end customer has to pay 590 dollars for the computer. A customer has to choose between a computer without security that costs 460 dollars and the one with security that costs 590 dollars. The decision will depend on the security knowledge that a customer has and the size of customer’s wallet. With the current situation where there is an asymmetric knowledge about security in computers between vendors and customers, it would be interesting to see how end customers react to the prices. In this scenario the middle men are gaining more profits than the producers of computer hardware, software, systems and services. Therefore, this could imply that in future they could be reluctant to add any other security measures because they are not the ones that gain from additional security measures.

As figure 68 suggests, an information system could be broken down into a socio and technical sub-system. The social subsystem can be sub divided into culture and structural sub systems. People using an information system have culture like ethics, traditions, laws and other social values. The technical part consists of methods and machines. Every system strives to be in balance so when any of the components or subsystems of the socio-technical system change then other components change too, to keep the balance. In an IT system the social sub system can include ethical/cultural, legal/contractual, administrational managerial and operational procedural layers. The Technical sub system can include the following layers: mechanical/electronic; hardware; operating system; application; data, store, process, and collect information [3]. When a new machine is introduced into a company it can require that changes be made in procedures, ethical, legal, and administrational issues. Insecurity is the result of instability that is created when social and technical systems adapting at different levels at the same rate to each other and the environment [3]. The Socio-technical
system consists of the living, abstract, and concrete systems.

3.2.1 Living Systems: At the living system, the enemy could apply human resources in social engineering to gather information and architecture of an information system. In the next generation information systems one could use botnets, which act on behalf of human being to perform different activities. In the living system, an information security system one could use human resources to deter attackers, prevent attacks, to detect attacks, to respond to attacks, and to recover from attacks. It is also possible to train users or immunize them from attacks by injecting small doses of spams and phishing in the same way that medical systems vaccinate people with small doses of the diseases [11]. Even training users against undue influence from others, such as used for instance in social engineering, could be done by the same inoculation method, as argued by Levine [12]. Here users are exposed to small, controlled, doses of influence, and then taught about influence in order to strengthen their defense.

3.2.2 Abstract Systems: With these systems, the enemy of IT could automate an attack on information system by applying mobile software agents. To defend an information system at this level one could apply different agents to deter attackers, to prevent attacks, to detect attacks, to respond to attacks, and to recover from attacks. It will be not feasible to use human recourses to deter, protect, detect, and respond to different attacks.

3.2.3 Concrete Systems: With these systems level the attackers use different technologies like inside channel attacks to attack physical components. These include probing, fault-based analysis, timing analysis, and power analysis [4]. We could apply tamper resistant technology to deter attacks, prevent attacks, to detect attacks, to respond to attacks, and to recover from attacks. At this level one can apply cryptographic modules in deterrence, prevention, detection, response, and recovery sub systems [5]. In timing attacks one could apply randomizing timings’ technology [4]. Cryptographic modules can also apply data masking [4].

4. ATTACKING A SYSTEM USING THE SOCIO-TECHNICAL MODEL

As figure 69 outlines, all the groups in the organization of the enemy of IT have socio-technical systems. A defender’s information system, with inputs and outputs, is also a system consisting of culture (people who have culture), structure, methods, and machines. The enemy of IT scans the defenders systems to understand the culture of users, the structure, the methods, and machines of an information system. The enemy of IT will try to find out the tools, methods, and processes that an information system is applying to defend in the different subsystems: deterrence, prevention, detection, response and recovery at the living, abstract and concrete systems. The aim is to understand the number of states that the hacker could control in an information system. Security can also be defined as the ratio of the states known and unknown that could be controlled by the enemy of IT to the states that can be controlled by the information systems [3]. There are states that are controlled by the enemy of IT but are unknown [3] to the defending information system.
The smaller the ratio of the states controlled by the hacker to the states that are controlled by an information system the harder it is to succeed when attacking. If this ratio is high it is easier for the attacker to succeed the information system and difficult to control the information system.

Vulnerabilities in an information system could be exploited by an enemy of IT. Assume that there are N vulnerabilities. Assume also that the enemy of IT has vulnerabilities 1, 2, 3 … N and has 1, 2, 3… k methods and tools for exploiting the vulnerabilities. Assume that an information system could defend H% of the K methods and tools that an enemy of IT could use for the first vulnerability. The H% methods and tools are the states that an information system could control for this vulnerability while (K-H) % methods and tools are the states that the enemy could control. By analyzing the number of states in this way for all the vulnerabilities, we will get the total number of states that could be controlled by the enemy versus the states that could be controlled by an information system.

The scanning of the defenders socio-technical systems could also be done at all three levels the living, abstract and concrete systems. For example at the living system, they apply so-called social engineering methods to scan. Social engineering methods can be automated or manual. In manual social engineering, the attacker makes phone calls or just listens to conversations of system administrators during lunches etc.

FIGURE 69: APPLYING THE SOCIO-TECHNICAL SECURITY MODEL TO ATTACK AND TO DEFEND SYSTEMS

In automated living engineering the enemy of IT could for instance use botnets to gather the information. At the abstract system level, one could use manual or automated mechanisms to utilize the information gathered during the social engineering to attack an information system. In automated mechanisms, the enemy of IT can use software agents [agents] for instance. The same is applied at the concrete and physical systems of the defender’s system. This information will help the enemy of IT to determine weaknesses in the different sub systems and in the whole information system. The enemy of IT could analyze the allocation of economical resources of different sub
systems on the defenders information system. For example, an authentication system can be implemented to provide strong authentication, which can be more expensive to attack than a system providing simple authentication. The enemy of IT could use these results to decide whether attacking the IT security system could bring a good economic outcome.

5. CONCLUSIONS AND DISCUSSION

We have described a model for understating and explaining possible attack strategies of the enemies of IT: The enemy tests the strength of information systems before attacking. By checking tools, methods and processes that a defender uses to deter attackers, to prevent attacks, to detect attacks, respond, and recover an information system after attacks at the . The enemy uses Socio-technical security model to attack an information system at the living, abstract and concrete layers. As figure 70 indicates in some information systems much more resources are spent on detecting and preventing attacks while very little is spent on deterrence, response and recovery subsystems. For instance in the abstract system, figure 70, 5% was spent on deterring attackers, 40% was spent on preventing attacks, 35% of the security budget was spent on detecting attacks, 10% was spent on responding to attacks, and 10% was spent on recovering from attacks.

![Value-based chain model](image)

**FIGURE 70: EXAMPLE OF SECURITY ATTACK BUDGET USING VALUE-BASED CHAIN**

The enemy of IT could find out that the deterrence subsystem is the weakest and attack the information system through the deterrence subsystem. As a defender, this model could help to analyze the subsystem or the point in the information system that has weakness and strengthen it. A security manager could use this model to determine the potential victims in a company by analyzing all the computers and information systems in a corporation. The results of the analysis should indicate in which systems to add security measures.

In future, we intend to extend the research work done by Z. Alach on applying Effects-based operations (EBO) to model methamphetamine criminal behavior and organize in New Zealand [14]. The aim of Alach’s research is to holistically identify key processes, behaviors, criminal groups, critical paths and the interactions in order to identify the center of gravity of the criminal organizations. Alach believes that by identifying the center of
gravity of a drug organization, police
could more effectively combat these
organizations. We intend to investigate
the center of gravity of the enemy of IT
by using the socio-technical system.
There are nine possible centers of
gravity in the socio-technical system as
outlined in figure 71. The center of
gravity of the enemy could be methods,
machines, culture, structure or some
kind of combinations. If for example the
center of gravity is the methods that an
enemy of IT is using to attack, then a
defending system could modify the
deterrence, prevention, detection,
responding sub systems to make it
harder for the enemy of IT to succeed.

FIGURE 71: CENTRE OF GRAVITY

6 REFERENCES

information security, Building
secure applications, Gartner, Inc.
56 Top Gallant Road, Stamford,
USA, 2006
of deception: Controlling the human
element of security, Wiley
Publishing, 2002
Information systems security.
Scientific methodology course,
Department of Computer systems
sciences. University of Stockholm

and Royal Institute of Technology
Stockholm Sweden, 2008
Fujisaki, N. Torii, S. Ishida, Y.
Tsunoo, M. Saeki, A. Yamagishi,
TSRC and Side Channel Security
Requirement. Physical Security
Testing Workshop. Tamper-
resistance Standardization Research
Committee (TSRC), 2005
[5] S. Kowalski, IT Insecurity: A Multi-
disciplinary Inquiry. Doctoral thesis,
Department of Computer Systems
Sciences. Stockholm University and
Royal Institute of Technology.
Stockholm, Sweden.
Kowalski, A holistic and immune
system inspired security framework.
Proceedings for the 2009
International Conference on
information Security and Privacy
(ISP-09), Orlando, FL, USA, 2009
Based Risk Analysis: The Key to
Successful Commercial Security
Target for the Telecom Industry, 2nd
Annual International Common
Criteria CC Conference Ottawa,
2002
[8] M. Rogers, A new hacker
Taxonomy, Department of
Psychology University of Manitoba,
Winnipeg RSA Security Conference,
2001
and moral disengagement analysis of
criminal computer behavior: An
exploratory study, Doctoral Thesis.
Dept of Psychology. University of
Manitoba. Winnipeg, 1999
[10] P. Dalal, Cyber Crime and
Cyber terrorism: Preventive
defense for cyberspace violations,
Cyber crime research center,
ICT CRIME CASES AUTOPSY: USING THE ADAPTIVE INFORMATION SECURITY SYSTEMS MODEL TO IMPROVE ICT SECURITY

Jeffy Mwakalinga and Stewart Kowalski
jeffy@dsv.su.se stewart@dsv.su.se
Department of Computer and Systems Sciences,
Stockholm University,
16440 Kista, Sweden

Summary
This paper presents an analysis of ICT crimes using the adaptive information security systems model. There is a desire of being able to identify potential ICT victims so that measures could be taken to protect them. We briefly describe the crime theories, the top ten crimes, and the desire to have crime proofing products. We then describe the adaptive model for information security systems, and the architecture and the socio-technical system for analyzing ICT crimes. The analysis of the ICT crimes is presented. Finally, we present recommendations on how to improve on how to improve ICT security.

Key words: Socio-technical, deterrence, prevention, detection, response.

1. INTRODUCTION
ICT crime resulted when some hackers understood that they could make money out of hacking. The early hackers were creative programmers and scientists in the 1960s that were mostly from MIT and Stanford University [20]. They were very respected and started computer companies. These people include people like Steve Jobs and Gordon Moore [19]. The hackers started getting ideas of using hacking for criminal activities in the 1980s because of the film ‘war games’ [19]. According to Paulsen [19], this film inspired the mini-boom in amateur hacking. A wave of law breaking teen hackers came up in the years after this film in contrast to the original MIT hackers who were not breaking laws [19].

ICT crime is part of the techno crime involving crimes against computers, or committed with computers, cybercrimes, and crimes involving credit cards, automated telling machines, and crimes against digital rights properties [11]. The results of these crimes have given birth to new techno laws, techno security, and techno police. There are a number of theories to explain the general crime [14]. The first one is a traditional explanation called environmental theory. The theory is based on the effect of biology and heredity on criminal behavior in humanity. The second traditional theory is called personal theory. This theory is based on the effect of upbringing on behavior of individuals.

FIGURE 72: THE MODEL FOR OPPORTUNITY THEORY [14]
The modern theory on crime explanation is called opportunity theory. According to this theory, for a crime to occur there must be a situation, an offender, and a victim as shown in Figure 72 [14].
Today we have a situation where ICT criminals have made hacking a business with models, supply chains, and pillars of business [17]. Paul Otellini, the Intel CEO, announced recently that security has become the third pillar of business together with networking and power consumption [17]. For the hacking industry the pillars of their business is supply chains, optimization, and automation [17]. The supply chain comprises different groups of hackers with different roles. Optimization is done by effectively using the compromised resources and tools for command and control. The hacker groups compete against each other by removing competitors’ tools in a compromised computer. For example, a tool kit called the Spy Eye first removes the Trojan called Zeus before making an installation is a compromised zombie computer [17]. Automation is achieved by using attack templates and kits, botnet army, search engines to find potential targets. In this way, a hacker could make a complete attack with just a few mouse clicks [17]. The next section presents the top ten Internet crimes in the USA in 2009.

1.1. The Top Ten Internet Crimes
The Internet Crime report for 2009 reported 336 655 Internet crimes reported in USA that year [10]. The top ten most common Internet crime complaints are briefly described [10]. The first crime is the category of FBI scams with 16.6% of the total crimes. In this fraud, a victim receives an e-mail supposed to be coming from the FBI director. In the e-mail, it appears that FBI is trying to get something, like money or identity information, from the victim. Another type of scams is when a sender uses threatening methods to make a victim part with money. A victim receives an e-mail and the sender claims that the message was sent by a gang to assassinate the victim because of some offense against the gang. The victim is asked to send a certain amount of money within 72 hours to the sender or die if the victim does not do that. The next crime in the top ten Internet crimes is the non-delivery of merchandize, 11.9%, in which the victim bought something but it never arrived. Next is the crime called advanced fee fraud, 10.4%. It is an incident where a victim is promised to receive a huge amount of money if the victim helps to transfer a huge sum of money from the sender. The victim is to pay some kind of expense fee before the transfer. The next crime is identity theft, 10.3%, an incident where someone steals an identity or identity information. Overpayment fraud, 7.9%, is a crime in which a seller of an item advertizes on the Internet. The purchaser gives to the seller a counterfeit cheque that has an excessive amount than that agreed. The seller is asked to deposit the cheque and wire back the excessive amount immediately to the buyer but the cheque bounces at the bank and the wired amount is never returned. Miscellaneous consumer frauds are different types of frauds where victims are asked to send money where nothing is bought or sold. Spam, 4.8%, is unwelcome mass distributed e-mails. Credit card fraud, 4.5%, is a crime where someone is charging goods or services to victims’ credit cards. Auction fraud, 4.3%, occurs during online auction transactions. Computer damage, 3.5%, is a crime that occurs because of intrusions or some kind of hacking to victims’ computers.

1.2 ICT Crime Prevention Efforts
The main concern is how to prevent or reduce crime? Experiments show that some crimes could be reduced by modifying the opportunity for committing a crime in the design or built environment [14]. In Canada and USA, street crime prevention is done through environmental design [14]. In Europe, street crime prevention is done by reducing crime and fear of crime by designing out crime, which implies reducing crime through urban planning and architectural design [14]. In efforts to prevent ICT crime, the European Telecommunications Standards Institute comments that “The European Commission services believe that European standardization in this area will contribute significantly to crime proofing products or services. One possible solution would be the development of a check list of factors to be taken into account at an appropriate stage in the product/service development process that will increase general crime prevention and contribute to the protection of citizens” [3].

The aim of product proofing, as suggested by European commission services, is to prevent an offence, lower the impact of an offence, increase the ability to detect an offence, and establish responses to an offence [3]. The European commission services suggest five main keys [3] in this regard. The first key is intelligence, which involves gathering necessary information on a crime. The second key is to be able to intervene by using generic principles. The third key is to encourage crime proofing at the implementation stages during manufacturing of products and systems. The fourth key is to involve organizations and individuals as crime proofers. The last key is to assess the impact of the crime proofing measures.

The International and European police have special sections for dealing with ICT crime. The international police (Interpol) have set a special section that gathers intelligence information including strategic reports and operational reports to help member states [11]. Interpol presents a checklist of IT crime prevention on what to consider in different areas of an organization [18]. For instance, in the management responsibilities one should consider whether an
information security policy exists and whether the all management staff knows the contents in it. Other areas include whether there is an information-training plan. In addition, whether there is an initiative to create security architecture, and whether there is an initiative to create a security plan. The European Union police (Europol) also support member states police departments in exchanging experiences and best practices in the fight against cross-border crimes [11].

The second chapter describes the adaptive information security systems model. Chapter 3 presents the analysis of the crimes. Chapter 4 describes the recommendations. Chapter 5 presents the conclusion.

2. THE ADAPTIVE INFORMATION SECURITY SYSTEMS MODEL

The adaptive information security systems model was developed to minimize the gap between what we can do with ICT and what we can control with ICT. This is because one of the systemic problems with ICT is that it is a double-edge sword and it could be used for constructive and destructive purposes [12]. The model is based on the Systemic-Holistic Approach [4], Immune system [13], the Security by Consensus model [1], and the Socio-Technical system [1] as outlined in Figure 73.

2.1 CRITICAL SUB SYSTEMS

The model consists five critical systems the deterrence, prevention, detection, response, and recovery [2]. This is analogous to Millers critical systems in every living system [7]. According to Miller, 19 critical systems must be present in every living system for it to survive in different environments [7]. We believe that there are critical systems that should be present in every model for adaptive information security systems in analog to living systems. We identified the critical systems that should be present in every framework for adaptive information security systems. The critical functions are based on the value-based chain. Kowalski developed the Value-based chain for security [2] from the Value chain model [8]. The Value chain model was first established by Porter to describe the concept of value adding activities in a company [8]. The Value chain model was aimed at maximizing value creation at minimum costs.

2.2 CRITICAL SYSTEMS IN THE IMMUNE SYSTEM

The value-based chain functions are also present in the immune system. The Immune system consists of three main layers. These include the surface barriers, the innate immune system, and the adaptive immune system [16]. The surface barriers are the first line of defense, like firewalls, against infection and include the mechanical (skin), the chemical (enzymes), and the biological (potential hydrogen (pH)) barriers. The surface layer of defense acts as a deterrence and prevention systems.

FIGURE 73: THE ADAPTIVE INFORMATION SECURITY SYSTEMS MODEL

The innate immune system is the second layer of defense. This layer consists of specialized white blood cells that detect and respond to foreign cells. All the cells belonging to a human body are labeled as ‘self’. The foreign cells are identified as ‘non-self’. The surface of a cell has antigens, which tell an immune system if the cell belongs to the body or not [16]. If the cell is a ‘non-self’, it will be destroyed by the immune system. The third layer of defense is the adaptive immune system. The adaptive immune system has the ability to detect and remember new foreign cells and creates immunity to prepare the body for future challenges. We apply these futures by
providing adaptability measures in our model as described in the next section.

2.3 The Architecture

The architecture for implementation consists of the components as outlined in figure 74. The first component is the system manager. This is the only component that has access to all the components. The system manager creates rules, identities, goals, and security policies of operations and monitors the behavior of all the components in the security framework.

The system manager activates the security framework and initializes all the components of the framework. The second component of the architecture is the integrated security system. This component performs identity management and provides security services. The immune system uses cells to protect the body. The adaptive model uses software agents to provide security services. All components request specialized software agents for providing security services from the software agents’ creator. The software agents are generated based on the existing knowledge of adapting principles of the immune system [13] and cybernetic feedback mechanisms [4].

FIGURE 74: THE ARCHITECTURE OF THE ADAPTIVE INFORMATION SECURITY SYSTE

This knowledge is stored in the gene libraries. The DNA combines the genes to form different solutions the way children combine Lego blocks to form different solutions. The gene libraries provide information for the agents’ creator. In the immune system, there is a bone marrow that has the gene library and this library is the DNA [16]. The DNA rearranges the genes to form future B-cells. After the rearrangement of B-cells, they are tested by the
negative selection algorithm [16]. If the B-cells pass the test, they will be allowed to monitor in the body. In our architecture, the software agents’ creator represents the immune system’s bone marrow. The software agents’ creator forms software agents by combining genetic expressions using the artificial immune algorithms as outlined in figure 74. The agent creator applies the existing knowledge to form different normal and abnormal profiles for the sub-systems deterrence, detection, prevention, response, and recovery. The agent creator applies the Negative selection algorithm to test the agents [16]. The agents’ creator equips software agents with specialized principles for the deterrence, prevention, detection, response, and recovery systems. The software agents that pass the test are trained before released into the real environment. The performance of agents is monitored and recorded. The software agents provide security services to all the components of the architecture. The software agents that perform successfully according to the specified policy are cloned using the clonally selection algorithm [16]. The agent creator applies these principles to improve the next generation of software agents.

3. ANALYSIS OF CASES

We made an autopsy of 41 ICT crime cases [5]. We applied the Socio-Technical system [1] as outlined in Figure 75.

3.1 The Socio-Technical System

![Figure 75: THE SOCIO-TECHNICAL SYSTEM](image)

The Socio-Technical system consists of social and technical parts [1]. The social part consists of culture and structure. Structure refers to the power structure in an organization. People using an information system have culture like ethics, traditions, laws, and other social values. The technical part consists of methods and machines. In an IT system, the social part can include ethical/cultural, legal/contractual, administrative managerial and operational procedural layers. The Technical part includes the following layers: mechanical/electronic; hardware; operating system; application data, store, process, and collect information. Every system is required to be in balanced state to be able to reach the goals set for the system. When the methods change in a socio-technical system the machines, culture and structure may have to change to sustain the balance [1]. When a new machine is introduced in a company, it can lead to changes in procedures, ethical, legal, and administrative issues. In the next section, we apply the adaptive information security systems model and the socio-technical systems [1] to analyze the ICT crime cases.

3.2 Analyzing Criminal Cases

We analyzed 41 computer crime cases to see how many systems had deterrence, prevention, detection, response, and recovery measures. In addition, we analyze using the socio-technical system the methods and tools that the hackers applied in attacking the information systems. We present the structure or organization of criminals at the end of the analysis. Out of 41 cases, no system that was attacked had strong deterrence measures to scare away attackers. Seven systems had weak deterrence measures, which could not scare away attackers. 34 systems had no deterrence measures. When it comes to prevention measures, 40 systems had weak prevention measures, which could not prevent attackers. One system had no prevention measures at all. 31 systems had no response measures at all, while 10 systems had weak response measures. As to the recovery systems, 34 systems had no recovery measures while 7 had weak recovery measures. 18 of the cases did weak confidentiality measures. In 31 of the cases authentication, security service was not strong. In ten cases availability security service was weak. In 32 cases, access control was not strong enough. 23 cases had breaches in integrity security service. 9 cases had breaches in privacy security service.

3.2.1 SOCIO-TECHNICAL MEASURES

The Socio-Technical system [1] contains the social and technical parts. Criminals appear to use both social, like social engineering, and technical measures to attack information systems as outlined in table 13. Criminals used social attacking measures in 26.8% of the crimes. In 31.7% of the crime cases criminals used both social and technical attacking measures. The criminals used technical attacking measures in 41.5% of the crime cases.
Figure 76: How Fraud Works [Adopted from 6]

Table 13: The Degree of Social and Technical Attacking Measures Used by Criminals

<table>
<thead>
<tr>
<th>Social attacking measures</th>
<th>Technical attacking measures</th>
<th>Social-technical attacking measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.8%</td>
<td>41.5%</td>
<td>31.7%</td>
</tr>
</tbody>
</table>

In Technical part of the Socio-Technical systems, there are methods and machines that the criminal could use to attack ICT systems. The methods that criminals used in the 41 crime cases include stealing credit cards and identities, installing Trojan horses, reconfiguring networks, redirecting traffic, deleting and modifying records. Other methods include impersonation, stealing program codes, diverting salaries, distributed denial of service, SQL injection [21], stealing secrets and formulas from companies and Web defacing. The method of stealing identities and credit card information and selling the information was applied in ten crime cases. The method of stealing secrets from companies like trade secrets, formulas, and new product designs was used in five crime cases. The method of distributed denial of service was applied in four crimes cases. The SQL injection method used in two of the crime cases. Web defacing method was used by criminals in two crime cases. Another method that used in one of the crime cases was selling the botnet army to other criminals using the state web sites.

As regards machines, it is not easy to understand the exact machines that they used to conduct their criminal activities. However, it appears that they were using powerful computers and fast ubiquitous internet access [19]. The same goes to culture of the criminals they tend to come from different cultural backgrounds. The organizational structure of criminals appears to be as outlined in figure 77.

Figure 77: Organization of Hackers
The first group is of coders who write malicious codes. The second group in the organization consists of keepers of botnet army, which is automated and used to extract information from victims. The next group comprises of researchers who investigate the vulnerabilities in different products and systems [17]. The next group consists of attackers who hire botnets from the botnet army keepers or use free attacking tools to perform the attacks. The next group is of consumers who use the stolen information to translate it into money [17]. Then there is a group of helpers, who assist the criminals in performing tasks like transferring money. One example is money mules that created bank accounts using fake documents.

3.2.2 The Cyber Theft Case

In this section, we describe in details the analysis of cyber theft case in which $70 million was stolen [6]. The criminals made surveillance on the different corporations and banks and found out those large corporations and large banks had strong online security. Therefore, the criminals decided to target medium sized companies and even churches. The assistant director of the FBI’s cyber division said this kind of crimes was a threat to the financial infrastructures [6]. They caught some of the criminals but it involved much resources and international cooperation. The director said it was not easy because different countries have different culture and cyber laws. It appears that the criminals made surveillance and discovered the weaknesses in the deterrence, prevention, detection, and response security measures in the computer systems involved. If the strong deterrence measures were present, the criminals could not have attempted to steal the money because the risk of being caught would have been too high. We describe the different steps that criminals followed during the crime.

In step 1, figure 76, a malicious coder created a Trojan horse called Zeus [6]. The hackers wrote official looking letters and sent them to small and medium sized companies. One employee of small Michigan company opened the letter and the Trojan captured the banking credentials and within a short time $650 000 had been transferred electronically to bank accounts in Finland, Estonia, Russia, Scotland and USA. In step 2, the hackers installed the Zeus Trojan in victims’ computers via e-mail attachments. The method that the hacker used to install the Trojan was social engineering in convincing the victim that the email and the attachment was an official letter from a fellow employee. At this stage, the adaptive model would have prevented the Trojan to run because no program without a special identity, authorization, and registration in the program database would be allowed to run in the computer. There are software agents in the adaptive model that monitor and check the authentication and authorization of every program, which tries to run.

In step 3, the Trojan horse captured bank accounts, passwords, and other credentials for login into financial accounts and stored them in a compromised collection server. The method used here is monitoring and recording the banking credentials. Our adaptive model has agents for monitoring the actions of the programs running on a computer. The adaptive model could have detected the actions of the Trojans. The victim’s computer and the collection server lacked deterrence, prevention, detection and response measures both social and technical measures. In step 4, the criminals retrieved banking credentials. In this step, the adaptive model has agents that detect the information that is sent out; the ports used, and check the programs that are sending the information. Here there was no program to detect what was sent out. In step 5, the criminals remotely accessed the compromised proxy. The compromised proxy lacked deterrence, prevention, and detection, and response measures. The identification, authentication, authorization, confidentiality security services are not working properly in the compromised proxy. Therefore, the hackers were able to compromise it, access it, and use it as a proxy to log to the victim’s bank. In step 6, the criminals log into victim’s online bank account and transfers money without authorization. The method used is impersonation using the banking credentials that were captured by the Trojan. The bank system lacks strong deterrence, prevention, and detection measures to scare away criminals, or prevent and detect their activities. In addition, the security services authentication, and authorization are not strong to detect the criminals. In step 7, money was transferred to money mules. The mules create bank accounts using fake documents and phony names. For example, the money from one customer of company called TD Ameritrade landed in a bank account belonging to a fake company called the Venetian Development Construction Service Corp. The mules had registered this fake company an address of an unmarked, building of two stories in Brooklyn [6]. The mules were given about 8 to 10%. In this step the identification, authentication, authorization, non-repudiation, detection, prevention, and response measures are weak. The systems were supposed to detect fake documents and phony names when creating accounts and they were supposed respond immediately. In addition, when the amounts that were supposed to be withdrawn using ATM cards were raised the banking detection systems were supposed to detect, react, and inform the bank. Money is then wired from mules to criminals or cashed and smuggled out of the country as outlined in figure 76.
At the airports, smuggled money prevention and detection services were weak because they did not detect the smugglers. The criminals in the cyber theft case were also organized as outlined in figure 76. There was a group of coders, who wrote the Trojan called Zeus. Then there was a group of keepers, who maintained the Zeus botnet army. There was a group of researchers [17], which discovered the vulnerabilities in different systems and servers exploited in the cyber theft case.

There was a group consisting of attackers who hired the botnets from the botnet army keepers (or used free). This group had a task to extract bank credentials from victims. In the cyber theft case, the criminals were the consumers who used the stolen information to steal money from victims’ bank accounts and transfer the money to accounts that were created by mules. The mules belong to a group of helpers who helped the criminals to transfer stolen money to other countries. The mules created banks accounts using fake documents. The stolen money was transferred from victims’ bank accounts to the accounts created by mules. The money was then wired or smuggled to the criminals countries [6].

4. RECOMMENDATIONS TO IMPROVE THE ICT SECURITY

To be able to prevent crimes we propose to use methods for identifying potential victims. We can identify victims by having a potential detecting model. We have created an adaptive information security systems model, which consists of critical sub systems that should be present in every information system. The critical systems include the deterrence, prevention, detection, response, and recovery sub systems. We made a survey on 60 master students in information security from France, Sweden, Sri Lanka, Libya, USA, Libya, Taiwan, Thailand, Uzbekistan, Spain, Peru, Pakistan, Nepal, Iran, India, Iceland, China, Brazil, Bangladesh, and Serbia Montenegro.

Every master student was to act as a security manager of a company. The security manager was to spend 100 000 dollars for information security in the company. Then we made the second survey with international master students in information security from Austria, Bangladesh, China, Greece, Hong Kong, India, Iran, Pakistan, Nigeria, Sweden, Tanzania, and Turkey. The aim of the surveys was to understand whether culture affect the decisions, which users make when deciding, which of the five security value-based chain functions were more important. The results are outlined in figure 78.

The results show that 18.75% of the total security budget would be allocated on deterrence sub system. 24.38% of the total budget would be allocated on the prevention sub system. 23.13% of the total budget would be allocated on the detection sub system. 14% of the total budget was to be allocated on the response sub system. 19.38% of the total budget should be allocated on the recovery sub system. It is interesting to note that all the students from China allocated less than 10% on the prevention, response, and recovery sub systems but allocated around 47% of the total budget on detection sub system.

![Figure 78: Average allocation of resources on different sub system](image)

Note also that Nigeria allocated nothing on the prevention and detection sub systems. Turkey on other hand spent 62% of the whole budget on detection sub system. There was an indication that culture of users affects decisions in allocating the security budget. Most crime-prevention theories appear to center on offender-oriented approach [9]. This implies that statics are collected on the categories of offenders, offender’s employments, their positions, time taken to do the crime, etc. Steinmetz suggests a victim-oriented approach and proposed a victimological risk-analysis model as outlined in Figure 79.
4.1 Victomological Analysis

This model was originally aimed at determining factors related to petty crimes in the Netherlands. Steinmetz suggests that potential victim create opportunities, which the potential offenders seek and can take. There are some factors that determine a potential victim. One of the factors is the attractiveness like the possession of antiques. In the ICT world, it implies that people who have unsecured computers and IT systems create opportunities for hackers. The other factor is the habits of an individual like certain habits of spending evenings out. The other is the exposure factor. Steinmetz further suggests that there are general influences like economical, social and physical factors influence the opportunities.

Steinmetz proposes three barriers that could be placed between the potential offender and the potential victim. These barriers are the technoprevention, socio-prevention, and environmental design. Steinmetz proposes techno and socio-prevention between potential victims and potential offenders. In the adaptive information security systems model we apply both socio-technical measures to deter potential hackers. If the deterrence socio-technical measures fail, we apply the response socio-technical measures. If all these socio-technical measures fail then we apply recovery social-technical measures. In this way, we defend ICT systems using a layered defense in analogy to immune systems. The immune system applies cells to protect bodies in the adaptive information security systems model we apply software agents.

5. CONCLUSIONS

We have presented an analysis of 41 ICT crimes. The crimes occurred because of the absence of deterrence socio-technical measures. In addition, the prevention and detection measures were weak which enabled the attacks to take place. In addition, response security measures were lacking or weak, which enabled the ICT criminals to succeed. We recommend that every information system should have the deterrence, prevention, detection, response, and recovery security measures. We also recommend that the security measures should include both social and technical security measures. This is because the hackers use both social and technical measures in attacking or in gathering information before the attacks. The hackers use social engineering to gather information. We also recommend especially to security administrators to detect potential victims by checking whether the
deterrence, prevention, detection, response, and recovery security measures are present and their strength. These functions could act as crime prevention features in ICT products and systems.

REFERENCES


Jeffry Mwakalinga received the M. Sc and Licentiate of Technology degrees from the Royal Institute of Technology, Stockholm, Sweden, in 1999 and 2003 respectively. He is currently PhD student at the Department of Computer Systems Sciences at the Stockholm University and the Royal Institute of Technology. His research interest includes holistic system security, cultural aspects of security, socio-technical security measures, smart card technology, information security architectures, secure mobile agents, and network security. He has published over 17 papers in information security. He has 11 years experience in information security science and technology.

Stewart Kowalski received his Ph D from the Royal Institute of Technology, Stockholm, Sweden in 1994. He has over 25 years of experience with security issues in computer and telecommunication systems. He has both extensive industrial and academic experience. He has worked for a number of major telecommunication players including Ericsson, Huawei, TeliaSonera, HP, and Digital. He has published over 40 papers in the information security
area and has taught IT security and information security courses at technical institutions, universities, and business schools. The major focus of his research is applied socio-technical analysis to security in ICT systems. He is currently an associate professor at the Department of Computer and Systems Sciences at Stockholm University.
PAPER XII
Architecture for Adaptive Information Security Systems as applied to Social Networks

Jeffy Mwakalinga and Stewart Kowalski
Department of Computer and Systems Sciences,
Stockholm University
164 40 Kista, Sweden

jeffy@dsv.su.se, stewart@dsv.su.se

Abstract – Users of social networks appear to want and need to share information online without necessarily thinking about the security consequences. Hackers and attackers have understood the potential vulnerabilities in social networks. This paper describes an architecture for adaptive information security systems, which could be applied to provide security services in social networks. The problem with most security architectures is that they do not provide adaptive security measures to environments and to culture of users. In addition, most security architectures provide technical security measures but fail to provide socio-technical measures. The enemies of ICT use both technical and social measures to attack ICT systems. This paper presents a security architecture that provides adaptive security measures and socio-technical measures in social networks.

Keywords – Deterrence; socio-technical security measures; value-based chain; social networks

INTRODUCTION

Social networks have been accepted widely and users put excessive trust on messages and applications sent by friends [16]. Hackers and attackers of ICT use social networks as a platform for finding and attacking victims. Social networks have become the channel of identity theft, spam distribution. It is easy to create a fake profile and users would join the fake profile without verifying the identity. For instance, two researchers created a fake profile at LinkedIn and within a day, 50 people had joined it [16]. Some of the threats in social networks include disclosure of private information, theft of intellectual property, theft of corporate secrets, damage of reputation of users, and identity theft [17].

A security architecture is generally concerned with protection of nodes and the communication protocols between the nodes. There are different types of security architectures in different contexts. A security architecture could be of an enterprise, an application, a product, or a system [8]. Enterprise security architecture provides security for operations, applications, processes, infrastructure, and management [8]. Application security architecture addresses security of applications and controls that are required outside the applications. Product security architecture takes care of the specific properties and requirements of that product or system. These architectures could be in the context of computer systems (for example CISCO [7]) or telecommunications system (for example Ericsson [9]).

When developing a security architecture it is recommended to create a team consisting of stakeholders, security experts, customers, and users [7]. The team should start with a threat and risk
analysis to identify the assets and the threats to the assets. In cases where the security architecture already exists, it is recommended to perform a gap analysis to identify the missing security measures in the existing security architecture. When the threats and vulnerabilities are identified, the planning team should analyze the security requirements to address the identified threats and vulnerabilities. Thereafter, the security services are identified to meet the requirements.

The next phase is to design the security architecture. In this phase, the development team would select the best platforms, capabilities, and best practices. The team should also analyze the standard security mechanisms that are necessary to provide the security services. The next phase is implementation, which include deploying the platforms, security mechanisms and hardening the infrastructure. The next phase is operation, which involves managing and monitoring the infrastructure. In addition, it includes collecting, monitoring, reviewing and responding to the security intelligence. The next phase is to maintain the architecture, which includes periodically reviewing and re-assessing the risks and threats, and performing the necessary modifications.

It appears that organizations and security experts do not have a general definition of a security architecture [8]. Traditionally, security architectures were supposed to describe which security services were available, where and how the security services were provided [8]. Zachman developed a classic concept of describing security architectures in different perspectives [10]. This concept is based on six different categories, which could be viewed from six different perspectives. The remaining sections of this paper will present the requirements for a security architecture, the related security architectures, the architecture for adaptive information security systems, securing social networks using the architecture for adaptive information security systems, and a conclusion.

2. Requirements for a Security Architecture

The requirements for a security architecture are presented by the National Institute of Standards and Technology (NIST) [11]. NIST describes the security services model in three main layers. The security architectures are to have at least three layers of defense to provide defense in depth strategy. The layers include prevention, recovery, and support. Every layer consists of the security services that should be provided. The goal of the first layer is to prevent security breaches from occurring in an enterprise, application, or system. The first security service in the prevention layer is transactions privacy. This security service protects privacy of a transaction that an individual is performing. The second security service is non-repudiation, which prevents repudiation of the performed transactions. The third security service in this layer is authentication, which provides the ability to verify identities of users or processes. The fourth security service in the prevention layer is authorization, which provides specification of the permitted actions to users or processes. The sixth security service in the prevention layer is the access control enforcement, which provides enforcement of the defined security
policies. The seventh security service is to protect communication from modification, disclosure, substitution, and replay. This service provides integrity, availability, and confidentiality of information while in transmission [11]. The goal of the second layer is detection and recovery. This layer is necessary because the prevention mechanisms are not perfect. Therefore, when prevention mechanisms fail, there should be measures to detect breaches and recover from them as outlined in figure 80.

![Image of the NIST Security Services Model]

**FIGURE 80: THE SECURITY SERVICES MODEL**

NIST [11]

The first security service in this layer is to detect an intrusion and respond in timely manner. The second security service is proof of wholeness, which provides measures for detecting when information or a system is corrupted. The third security service provides auditing of security relevant events. The fourth security service is to restore the system to a secure state. The aim of the third layer is to providing support services. The first service is to provide unique identification of users, processes, and resources in a system. The second security service in this layer is cryptographic key management, which provides secure key management services. The third security service is security administration for management of different security features in a system. The fourth security service in this layer is system protection, which include object reuse, least privilege, and process separation. Notice that in the NIST architecture there is no service for deterring attackers. The next section describes two related security architectures.

### 3. RELATED SECURITY ARCHITECTURES

This section presents the related security architectures of computer and telecommunication systems. We start by describing the security architecture for mobile networks [9].

#### 3.2. SECURITY ARCHITECTURE FOR MOBILE NETWORKS

The security architecture of Ericsson [9] consists of three planes as outlined in figure 81.
In figure 81, the first plane is called end-user security and is responsible for providing security of end-user data flows. Each plane is divided into three security layers. The first layer is application security layer. The assets in this layer are application data and software. The threats in this layer include virus infections, false data, unauthorized users, malicious programs, and file corruption. The countermeasures applied to address the threats include - virus protection, system access control, certificates, application layer gateway, deep firewall inspection, secure shell, simple network mapping protocol version three. The second layer is called network services security whose assets are routers, addressing units and data. The threats for this layer include corrupted router tables, denial of service, and interception of data. The security mechanisms applied in this layer are the Internet protocol security, the Virtual Private Network, Secure socket layer, and stateful inspection firewalls. The third layer is called infrastructure security whose assets are switches, communications links, and computers. The threats to this layer are electronic attacks, and destruction of relays. The countermeasures that are applied in infrastructure security layer include securing perimeters, limiting administrators, role based access control, layer two virtual private networks, and MAC filtering.

The second plane is called signaling and control security. This plane provides security of information, services, and applications across networks. The third plane is operation and maintenance security, which is responsible for protecting functions of business support, customer care, and other operations and maintenance services [9]. The security planes are separated logically and physically using firewalls, Virtual Private Networks, etc. The security services that are provided include accountability, authentication, authorization, availability, confidentiality, integrity, non-repudiation, and privacy.

The strength of the security architecture for mobile networks is that it provides most of the security services that are recommended by NIST [11]. The security architecture also provides security services at the application, network, and infrastructure making it more difficult for attackers. The weakness of this architecture is that it does not provide audit, proof of wholeness, restoration to a secure state, intrusion detection, and containment. In addition, the architecture does not provide adaptive security measures to
environments and to culture of users. The security architecture does not provide deterrence measures. Further, the security architecture does not provide the socio-technical measures. The next section describes the security control framework of CISCO [7].

3.2. SECURITY CONTROL FRAMEWORK

The framework of CISCO consists of four layers [7] as shown in figure 82. The first layer is business relevance, which include the business goals, objectives and the threats to goals and objectives. The second layer consists of security policies. The security policies consist of threat and risk assessment, and security operations. The third layer consists of security principles, which include visibility into the devices and events of the network. In addition, security principles include control of users, devices, and traffic in the network. The fourth layer consists of security actions. The first action for visibility is identifying and classifying users, services, traffic, and end-points. The second action in visibility includes monitoring behaviors, performance, and events. The third action in visibility includes collecting, analyzing, and correlating events. The first action in the control security principle is to harden applications, infrastructures, servers, and other systems. The second action is to isolate users, services, and systems when necessary. The third action is to enforce access controls, security policies and to mitigate security events. The security control framework is continuously reviewed. The review process includes planning, designing, implementing, operating, and maintaining it. The strength of the framework is that it provides two important principles of visibility and control.

![Security Control Framework of CISCO](image)

It also provides ways of planning, designing, implementing, operating and maintaining the control framework. It also provides defense in depth and uses a holistic security approach in securing the network environment. The weakness of this architecture is that it does not provide adaptive security measures even though there are plans for reviewing and improving the framework periodically. Further, the control framework does not provide deterrence security measures. The next section describes the architecture for adaptive security systems.

4. THE ARCHITECTURE FOR ADAPTIVE INFORMATION SECURITY SYSTEMS

The architecture is based on Systemic-Holistic Approach [3], immune system [1], and Socio-Technical System [4]. The first component of the architecture is the system manager, which is responsible for security administration. The system manager creates rules, identities, goals, and security policies of
operations, and monitors the behavior of all the components in the security architecture. The system manager activates and initializes all the components of the architecture. The second component is the integrated security system. This component performs identity management and provides security services in the whole architecture. We apply the principles of the immune system in this architecture. The principles of immune system that we use include multi-layered structure, local detection, diversity, autonomy, adaptability, dynamically changing coverage, and identification. The immune system applies the B-cells and T-cells to perform different tasks. In analogy to the cells of the immune system, we apply the software agents in this architecture. Components of the security architecture request specialized software agents from the agent creator for providing security services. The software agents are created based on the prior knowledge, which is stored in the gene information library. In the immune system, the bone marrow contains the gene library, which is called the DNA [1]. The gene library rearranges the genes to create pre-detectors, which are future B-cells. These pre-detectors are tested using the negative selection algorithm [1] before leaving the bone marrow. The aim of the negative selection algorithm is to determine whether the B-cells detect correctly. Those B-cells that pass the negative algorithm test are allowed to monitor in the human body. In this security architecture, the agent creator represents the bone marrow of the immune system as shown in figure 83.
are also called security value-based chain functions. The software agents are tested using negative selection algorithm [1], as outlined in figure 83, in the grey area, which shows a cross section of what goes on inside the agent creator. The software agents that pass the test are trained by the agent creator on how to monitor in the deterrence, detection, prevention, response, and recovery functions. The components monitor the performance of agents, record the agents, and inform the agent creator the software agents that are most successful, according to some criteria specified in the security policy. The successful agents are cloned using the clonally selection algorithm [1]. The features that enable the successful agent to succeed are stored in memory and would be applied to improve the properties of next generation of agents. The next component is the deterrence, which is responsible for scaring away attackers. It applies the principles of cybernetics feedback mechanisms, principles of immune system and other systems to deter attackers. The next component is the prevention to prevent breaches to a system. The next component is the detection. It applies neural networks, fuzzy logic, Cybernetic feedback mechanisms, principles from the immune system to provide measures for detecting attacks and intrusions to the attacks. The next component is response, which applies the software agents to respond to different attacks and intrusions to the security architecture. The recovery component is responsible for putting the security system back to normal after attacks and intrusions. The architecture provides socio-technical security measures at the application, transport, internet, and link layers.

4.1. ADAPTATION SERVICES

The security architecture provides adaption services, which are divided into three analyzers. The first is called the environment analyzer, which provides measures for making an information security system adapt to environments. The analyzer applies the Viable system model [6] and the Cybernetic structural model [13]. The second is called people’s value analyzer. It applies the informal cultural model [2] to predict the behavior and preferences of users of different cultures. Some behaviors and preferences of users of different cultures could create vulnerabilities in information security systems. The third analyzer of the adaptation services is called the threat analyzer. It analyzes the tools and methods that attackers apply to attack an information security system. The next component provides fault tolerance services, which include error detection measures, damage assessment measures, damage confinement measures, error recovery measures, fault treatment, locator, and continued service measures. The security management component uses the recovery function to perform risk management, security policy management, compliance management, and continuity planning management services. The special analysis performs special analysis of unknown and abnormal inputs as requested by the different components of the architecture.
5. SECURING SOCIAL NETWORKS USING THE ARCHITECTURE FOR ADAPTIVE INFORMATION SECURITY SYSTEMS

We apply the architecture for adaptive information security system to secure social networks in the following way. The first step is to analyze the threat agent using the threat analyzer to the social networks. It analyzes the tools and methods that attackers apply to attack an information security system. The threat agent seems to be organized in the following way. There are six groups in the threat agents’ organization. Researchers investigate systems to find vulnerabilities in social networks. Software coders write intelligent malicious toolkits and programs like Trojans for monitoring, capturing, retrieving information, and covering their activities as shown in figure 84.

![Figure 84: Organization of the Threat Agent](image)

The next group is botnet army keepers, which maintain and increase the army of botnets [18]. The next group consists of attackers, which include all kinds of hackers that perform the attacks. Some attackers use botnets, which they hire at prices that are set by botnet army keepers to gain information. The next group consists of consumers who use the stolen information to create fake credit cards, transfer money from victims’ online banking accounts and to create fake identities. The helpers group includes mules and entities who offer free hosting servers for storage of stolen information. Mules are a network of people who transfer stolen money from banks in one country to other countries at commissions.

The next step is to perform threat and risk analysis to identify the assets and the threats to the assets [7]. Thereafter we analyze the security requirements to address the identified threats and vulnerabilities. Then the security services are identified to meet the requirements. The next step is to analyze environments where the social network system is operating. We apply the environment analyzer to provide measures for making the social network system adapt to environments. The environment analyzer applies the Viable system model [6] and the Cybernetic structural model [13]. The environment analyzer collects data on environmental disturbances from environments and stores the data in a database. The analyzer applies the collected data to create probabilistic models that are used to forecast the future environmental disturbances and thereby foresee how the system will react to those future disturbances.

Social networks are used in different cultures and therefore the next step is assessing the effects of culture and other social issues of social network’s users regarding information security. We apply people’s value analyzer to predict the behavior and preferences of users of different cultures. Some behaviors and preferences of users of different cultures
could create vulnerabilities in social network systems. The Socio-Technical system [4] is applied to analyze the vulnerabilities created by cultural behaviors and preferences. The Security by Consensus model [4] is applied to remove the vulnerabilities. The vulnerabilities that were created by cultural behavior and preferences are dealt with by applying social and technical security measures [4]. As an illustration, a study on the effect of human behavior on systems security showed that people with low uncertainty avoidance tend to lack holistic approaches to security [5]. This implies that they lack security in depth measures and they lack attention to details. The architecture for adaptive information security systems provides security policies, which specify the holistic security measures to take care of the cultural vulnerabilities.

The next step is to analyze how to distribute economical resources to the deterrence, prevention, detection, response, and recovery security functions of a social network system. Kowalski and Nohlberg showed that since automated social engineering attacks were possible in social networks more efforts should be put in detection rather than prevention [14]. Engineering is about optimization therefore we need to optimize the security functions that are to be applied in securing social networks. The adaptive information security architecture provides deterrence, prevention, detection, response, and recovery functions. The average optimization on these security functions for a traditional network according to a survey was to spend 18.42% of the total security budget on deterrence, 26.33% on prevention, 25.95% on detection, 14.15% on response, and 15.15% on recovery as outlined in figure 85. In social networks, we optimize by putting more efforts on detection, response, and recovery functions. For instance, we could spend 30% of the total budget of security on detection, 20% on response, and 15% on recovery, 10% on deterrence, 15% on prevention as shown in figure 85. The reason for focusing on detection, response, and recovery is that we do not want to focus on preventing users from communicating. The detection, response and detection functions are applied in the following way. Assume that one user of one social network visits another user’s profile in another social network. If the result of the visitation is good, we note the user’s profile as clean.

![Value-based chain model](image)

**FIGURE 85: FOCUSING ON DETECTION, RESPONSE AND RECOVERY FUNCTIONS**

However, if the result of visiting another profile causes the state of the profile of the user to be corrupted, then we respond by rolling back the state of the profile of the user to the original profile of the user before going to visit the other user. We also record the visited profile as hostile and we forbid
visitations to it. For different cultures, we need to understand how different culture would like to put priority on how to optimize the deterrence, prevention, detection, response, and recovery functions. As an example, we made a survey on 60 international master students in information security. The students come from Bangladesh, Brazil, China, France, Iceland, India, Iran, Libya, Nepal, Pakistan, Peru, Serbia Montenegro, Spain, Sri Lanka, Sweden, Taiwan, Thailand, USA, and Uzbekistan.

The sample of results, figure 86, shows that Sweden would optimize the security functions in the following way. 12% of the security budget would be applied for deterring attackers. 27% of the total budget would be used for preventing attacks and intrusions. 26% of the budget would be used for detecting attacks and intrusions. 13% would be used to respond to attacks and intrusions. 24% of the total budget would be used to recover a social network system after attacks. The results show that the way respondents from different countries optimize the security functions differ significantly as shown in figure 86.

FIGURE 86: A SAMPLE OF RESULTS OF DISTRIBUTION OF A SECURITY BUDGET ON DETERRENCE, PREVENTION, DETECTION, RESPONSE, AND RECOVERY FUNCTIONS

Then we educate users of social networks electronically on social engineering and other security issues. In the last step we continuously evaluate the outcomes of the implementation of architecture based on the plan, do, check, and act process for continuous security improvement outlined in ISO27001 [15].

6. CONCLUSION

The paper has presented how to secure social networks by using the security architecture for adaptive information security systems. The architecture provides adaptation services to enable information systems adapt to environment and culture of users. The architecture provides socio-technical security measures. Surveys were made to understand how culture affects decisions of users from those cultures. Future work includes implementing the security architecture.

REFERENCES


APPENDIX A: INTERVIEW PREPARATIONS

A.1 LETTERS
Letters were prepared and sent to the nine candidate interviewees. Six responded while three did not respond. The following letter was sent to the candidate interviewees.

Dear Mrs. / Mr. …

I am a graduate student under the supervision of Prof Louise Yngström and Prof Stewart Kowalski at the department of Computer systems and sciences, Royal Institute of Technology in Stockholm in the last year of my studies. I am doing a research and the title investigating a framework for adaptive information security systems based on the principles of the Systemic-Holistic Paradigm and of the immune system. The last part of research is to validate the framework. I would appreciate the opportunity to meet with you and discuss the practicality of the framework. Your outstanding reputation and background has made me to be especially interested in your views regarding the practicality of the framework. Any further insights of you would be greatly appreciated. It will be a structured interview for about 30 - 45 minutes. The interview is voluntary and you have the right to withdraw from the study. You have the right to decide the terms of study and the terms of your participation. I will follow the research ethics and privacy laws regarding your data. I will contact your office the week of … to set up a mutually convenient time for this interview.

I thank in advance for your cooperation.

Best regards.

After responding, we set time for interviewing them. Presentation slides and an abstract were sent to the interviewees. The slides included goals and purposes of the thesis; research methodology; proposed Framework for adaptive information security systems.

A.2 THE RESPONDENTS
The information security experts were from the academia and from the industry. Three information security experts came from the industry while three came from the academia. They have good knowledge of the holistic approach, system theory, socio-technical system, which are the fundamental concepts in the research.

The next process was to select the security experts. Six information security experts in the industry and academia were interviewed on the usefulness and applicability of the security framework. The experts had to be academics or research students with some experience in the industry. The experts were also selected based on their knowledge and experiences in the information security and their holistic view of this area. The first information security expert is a professor and holds a doctorate degree in the area and has great experience in information security both technical and management security and is working as a lecturer at a university. This information security expert has great experience in security for mobile software agents. The second information security expert holds a doctoral degree in information security, owns a consulting company of information security, and has great experience in the area. The third information security expert is a research student at a university, has good experience in this area, and owns a
small consulting information security company. The fourth information security expert holds a doctoral degree in information security, has good great experience in information security and works as a lecturer at a university. This expert has good knowledge in mobile agents’ security technology. The fifth information security expert is a research student and has good experiences in information security. The sixth information security expert is research student and has good experience in the area, and owns a small information security company. These experts operate in Europe, Asia, and USA.

A.3. Method of Surveying

The interview started with a brief description of the thesis using slides. These questions were asked. Three information security experts were interviewed face-to-face; two information security experts were interviewed by telephone. One was interviewed through e-mail. The templates are shown in Tables 14 – 17.

A.3.1 Questions on the strength of the framework for adaptive information security systems

TABLE 14: CAN THIS SECURITY FRAMEWORK AND ITS SUBSYSTEMS BE APPLIED / USEFUL IN YOUR ORGANIZATION?

<table>
<thead>
<tr>
<th>Can it be implemented?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOT SURE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Need more information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE 15  HOW USEFUL WOULD THIS SECURITY FRAMEWORK AND THE SUBSYSTEMS CAN BE TO YOUR ORGANIZATION?

<table>
<thead>
<tr>
<th></th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments:

TABLE 16  HOW SATISFIED ARE YOU WITH THE ADAPTABILITY FEATURES OF THIS SECURITY FRAMEWORK TO ENVIRONMENTS?

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Somewhat satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not too satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at all satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments
TABLE 17 HOW SATISFIED ARE YOU WITH THE ADAPTABILITY FEATURES OF THIS SECURITY FRAMEWORK TO THE VALUES OF THE PEOPLE USING THE INFORMATION SECURITY SYSTEMS?

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Somewhat satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not too satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at all satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments:

5) Are there any particular features that are not covered in this security framework?

6) Do you have any other comments?

A.3. QUESTIONNAIRE TO A GROUP OF MASTER STUDENTS IN INFORMATION SECURITY AND BACHELOR STUDENTS IN COMPUTING SCIENCE

The survey was made to a 39 master students (11), bachelor students (28) were given a brief description of the security framework, and then they answered the questionnaire. The templates are shown on tables 18 – 23
<table>
<thead>
<tr>
<th>Success criteria</th>
<th>Questions</th>
<th>Security Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usefulness of the security framework in organizations</td>
<td>Question 1&lt;br&gt;This Holistic and immune security framework its subsystems will be useful in your organization</td>
<td>Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework</td>
</tr>
<tr>
<td>Adaptability of information security systems to environments</td>
<td>Question 2&lt;br&gt;The adaptability features of this holistic and immune security framework will make information systems learn to adapt to environments where the information systems operate.</td>
<td>Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework</td>
</tr>
<tr>
<td>Adaptability of information security systems to culture</td>
<td>Question 3&lt;br&gt;The adaptability features of this Holistic and immune security framework will make information system adapt to the values of the people (tradition, culture, laws, etc) using the information systems.</td>
<td>Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework</td>
</tr>
<tr>
<td>Strength of the security framework to resist attacks</td>
<td>Question 4&lt;br&gt;This Holistic and immune security framework will be successful in preventing an adversary of IT from attacking an information system</td>
<td>Deterrence, Prevention (Protection), Detection, Response, Recovery, and Whole Framework</td>
</tr>
</tbody>
</table>
### TABLE 19: THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS ITS SUBSYSTEMS WILL BE USEFUL IN YOUR ORGANIZATION

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do not agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Need more information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TABLE 20: THE ADAPTABILITY FEATURES OF THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS WILL MAKE INFORMATION SYSTEMS LEARN TO ADAPT TO ENVIRONMENTS WHERE THE INFORMATION SYSTEMS OPERATE.

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do not agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE 21: THE ADAPTABILITY FEATURES OF THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS WILL MAKE INFORMATION SYSTEM ADAPT TO THE VALUES OF THE PEOPLE (TRADITION, CULTURE, LAWS, ETC) USING THE INFORMATION SYSTEMS.

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do not agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TABLE 22: THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS WILL BE SUCCESSFUL IN PREVENTING AN ADVERSARY OF IT FROM ATTACKING AN INFORMATION SYSTEM.

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do not agree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOT SURE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The idea of this questionnaire is to understand the weight of different sub systems deterrence, prevention, and detection, response, and recovery sub systems. Imagine that you are a security manager of a company and the Director General of the company has given you 100 000 dollars to spend for information security in the company. How much
money will you allocate on each sub system deterrence (scaring away attackers), prevention, detection, response, recovery, following different sub systems of the company? The template is shown on Table 23

TABLE 23: ALLOCATION OF ECONOMICAL RESOURCES TO THE SECURITY VALUE – BASED CHAIN FUNCTIONS

<table>
<thead>
<tr>
<th>How much to allocate on each subsystem?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8) Do you have any comments?
APPENDIX B - TEMPLATE FOR THE SURVEY ON SOCIAL AND TECHNICAL SECURITY MEASURES

The purpose of this section is to receive comments from the reader on the usefulness of the holistic and immune security framework. The answers should be sent to the addresses provided below. Table 24 outlines the template on the survey of security measures.

<table>
<thead>
<tr>
<th>Specific Classification of security measures for the security-value based chain functions</th>
<th>Where possible name specific protection measure</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social security measures</td>
<td>Ethical-Cultural</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal-Contractual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrative-managerial</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operational - procedural</td>
<td></td>
</tr>
<tr>
<td>Technical security measures</td>
<td>Mechanical-electronic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operating System</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardware</td>
<td></td>
</tr>
<tr>
<td>Others (please specify)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments…
Return completed forms to:...
Stewart Kowalski or Jeffy Mwakalinga
Department of Computer and System Sciences
Stockholm University / Royal Institute of Technology
Forum 100, 164 40, Kista, Sweden.
Email: stewart@dsv.su.se, jeffy@dsv.su.se
APPENDIX C – RELATED WORK

C.1 RELATED WORK: THE FIRST GROUP

In this section models, paradigms and frameworks are classified into two main groups. The first group is of those paradigms and models that do not take much consideration of culture, traditions, ethics, and other social issues of users using systems and systems environments where systems operate. The second group is of those paradigms, frameworks, and models that involve culture, traditions, ethics, and other social issues of users using the systems and environments where information security systems run.

C.1.1 DISCUSSION TOPIC: WHAT IS THE OLD SECURITY PARADIGM?

Greenwald (Greenwald, 1999) presented this paper in New Security Paradigm Workshop in which he argues that if a new security paradigm is to be created there has to be a well-defined old security paradigm. This will help researchers and developers to have a reference point for comparing the new paradigms. It has to be understood that old security paradigms are still functional and will be for some time to come. Greenwald (1999) also comments that it is easier to learn the mistakes that have been made in the past when there is a well-defined old paradigm. An old paradigm can be used to keep security knowledge and as a teaching tool. Greenwald (1999) comments that Privacy, Integrity, and Availability (PIA) is an old paradigm and clearly states that there is not one single old security paradigm and logically there will never be one single new security paradigm. PIA existed in three contexts or administrative environments: government, military and intelligence community, and commercial. Greenwald (1999) divides computer periods as follows: Pre-Computer, 1880 to beginning of the Second World War, Age of Pre-Computer Information Processing (APCIP). In this period, manual controls and auditing were used to deter abusers. ID cards and separation of privileges were applied to protect information systems. Auditing was used to detect frauds and other irregularities. The authorities responded with punishment measures. Backup measures and disaster recovery plans were enforced to recover information.

Information management and processing were important in the military, government and in industries even before the invention of computers. The age of information processing is divided into the following periods: The first period is called The Age of Pre-Computer Information Processing (APCIP) and it is from 1880 to the Second World War. The second period is from the Second World War to the start of Korean War (1950) and it is called Age of Computer Emergence (ACE). The third period starts from 1950 to mid 1960s and it is called the first period of Jurassic Age Security paradigm (JASP). The fourth period is between mid 1960s to mid 1980s. This period is called the second period of Jurassic Age Security Paradigm. The fifth period is from mid 1980s through the modern age and beyond (Greenwald, 1999). Information security experts applied manual and automatic controls to deter abusers of systems in the first phase of JASP. They protected information systems by using passwords and encryption. The system administrators applied computer backups and disaster recovery measures to recover information in this period (Greenwald, 1999).

In the second phase of the JASP, military and governments recognized the importance of computer security. They allocated many resources for research of information security...
(Greenwald, 1999). As a result, many security models appeared in this period. In 1971, Lampson developed a control access matrix (Lampson, 1971). In 1973, Lampson (1973) again developed covert channels. Covert channels were mainly concerned with privacy issues so they added privacy principles to the PIA paradigm. In 1976, Denning (Greenwald, 1999) developed a lattice model, which added information flow to the access control matrix. Between 1973 and 1976, the Bell-LaPadula model was developed (Bell & LaPadula, 1974; 1976). This model added the military type of security and it added privacy principles to the PIA security paradigm. In 1977, Biba developed the integrity model (Greenwald, 1999) and this model added integrity to the PIA paradigm. In 1985, the department of Defense of the United States of America created the Trusted Computer System Evaluation Criteria (TCSEC) (TCSEC, 1985). The PIA paradigm lacked communication security.

C.1.2 WHY INFORMATION SECURITY IS HARD – AN ECONOMIC PERSPECTIVE

This section bases on the paper, why information security is hard – an economic perspective, by (Anderson, R., 2001). In this paper, Anderson (2001) explains security failures in a language of microeconomics. Anderson argues that security problems are partly due to “network externalities, asymmetric information, moral hazard, adverse selection, liability dumping, and tragedy of the commons” (p. 1). The Orange Book (1985) evaluations were made by a reliable party but now Common Criteria (Common Criteria, 2006) evaluations are made by commercial bodies that are paid by the vendor. Vendors look for evaluators with low information security requirements on their products. This implies that the bodies that are capable of protecting information systems are not the ones that suffer when there is a security failure. Denial of service attacks for instance result from the same liability principle. Owners of computers that are used for attacking other computers do not suffer and so they can spend much money to protect their computers but they are not prepared to spend money to make sure that their computers are not used to attack other computers in Denial of service attacks. Developers make sure that they spend less time and money in developing security measures because they are not going to suffer but the users are incurring support costs. Vendors can use less secure mechanisms to force customers to use and depend on for monopoly purposes. Anderson (Anderson, R., 2001) concludes that security fails because of the desire to exercise monopoly, and to charge different prices for different classes of users for the same products.

The article (Anderson, R., 2001) takes up an economic perspective of security that has been ignored by researchers and developers. Researchers and developers should look for more holistic approaches when solving information security problems. There is a need to deter market manipulators by using different regulations. The government and other bodies should protect end customers from being deceived by sellers and the government should provide measures of informing customers about different information security systems. Measures should be enforced to detect liability dumping, moral hazard, and deceiving sellers and respond with punishment measures. Anderson (2001) does not discuss ways for considering culture, traditions, ethics, and other social issues of users, learning measures of security for information systems, and does not cover measures for taking care of inputs from other environments where information systems operate.

C.1.3 THREE PARADIGMS IN COMPUTER SECURITY
Meadows (1997) presented a paper, three paradigms in computer security, in New Security Paradigm Workshop, which were results of the discussions on high assurance systems. The discussions Meadows presented were about: the good paradigms (sound and practical security solutions); the bad paradigms (sound but impractical security solutions); and the ugly paradigms (practical but messy security solutions with low assurance). Meadows discuss three paradigms: Live with it paradigm; Replace it paradigm; and Extend it paradigm. In the Live with it paradigms patches, like firewalls and antivirus programs, are continuously added to strengthen security. In the Replace it paradigm, a security system is completely replaced by another supposedly much more secure system. Meadows give as an example the Orange book (Department of Defense USA, 1985), which created a number of criteria for securing operating systems. She found however, no operating systems that met the criteria fully. Meadows discusses three paradigms at a very high level and it is not easy to see whether they include culture, traditions, ethics, and other social issues of users, adapting measures and they do not involve environments where information security systems run.

C.2 RELATED WORK: THE SECOND GROUP

C.2.1 INFORMATION SECURITY MANAGEMENT - A NEW PARADIGM

Mariki Eloff and Jan Eloff (Eloff & Eloff, 2003) describe a new paradigm for Information Security Management System (ISMS) as shown in Figure 87. In this paradigm they combine process Information Security Management System (ISMS) based on the ISO 17799 standard (ISO 17799, 2005) and product ISMS using Common Criteria. This paradigm also involves culture, traditions, ethics, and other social issues of users in the form of culture, ethical, social, and legal issues as shown in Figure 87. It takes into consideration both technical and non-technical measures in the development of security for information systems. This paradigm is very attractive because it marries: standards like ISO 17799; culture, traditions, ethics, and other social issues of users using the information security systems; procedure; codes of practice; audits, certification and accreditation of management systems; process ISMS; and product ISMS. A holistic paradigm can be applied to any information security system.
Zuccato established a Holistic Security Management Framework for Electronic Commerce as shown in Figure 88 (Zuccato, 2007). In this framework, two main administrative environments are identified: Society and Business environments. The society influences the business environment and Zuccato (2007) stresses the importance of looking at factors from the society that affects security management of e-commerce in business environments. This framework takes into consideration culture, traditions, ethics, and other social issues of users that can affect security for information systems. The culture, traditions, ethics, and other social issues of users from the society environment are in the form of ethics, legislation, standards, and privacy. The framework views security for information systems holistically by considering different aspects that affect security for information systems today. The framework also describes some measures of maintaining the framework. However, the framework does not discuss measures for making information systems learn to adapt to new environments nor does it describe how to make information security systems fault tolerant.
Kim (2002) describes integrating artificial immune algorithms for intrusion detection in a doctoral thesis. Kim presented an artificial immune model for network intrusion detection as shown in Figure 89. The model takes as input normal network traffic and transforms it into self-network traffic profiles. The gene library creates gene expressions. This system applies the self-normal profiles to test whether the immune detectors can match them. This process applies negative selection algorithm to match the immune detectors with self-network profiles. These immune detectors are not supposed to filter out the normal...
network traffic but are to detect only abnormal network traffic. The abnormal traffic includes intrusions, viruses, attacks, and so on. The system deletes the detectors that filter out normal traffic. The detectors filter out and detect correctly are called immature detectors and are kept for further testing.

FIGURE 89: CONCEPTUAL ARCHITECTURE OF THE ARTIFICIAL IMMUNE MODEL

The artificial immature system releases the immune detectors in the testing network environment to monitor traffic. Thereafter the artificial immune system selects and releases the immature detectors that detect abnormal network traffic in the normal environment. The artificial immune system keeps as memory detectors the mature detectors that are successful according to some criteria. An example of the criteria could be to clone the immune detectors that detect all the versions of the denial of service attack. The communicator sends the immune detectors to the gene library for cloning.
The artificial immune system applies dynamic cloning selection algorithm in this cloning process. The disadvantages of this system include it does not scale very well in sizable network systems and so modifications have to be made to make it scale; the system is dependent on the effectiveness of negative selection and cloning selection algorithms. This model has features for making systems adapt to environments but does not consider culture, traditions, ethics, and other social issues of users.

REFERENCES


APPENDIX D – CRITERIA ANALYSIS, RESULTS AND ANALYSIS OF SURVEYS

D.1. RESULTS AND ANALYSIS OF SURVEYS

The author made surveys on 141 respondents to understand the applicability of the framework for adaptive information security systems. The following sections describe the results and analysis of the surveys.

D.1.1 SURVEY OF INFORMATION SECURITY EXPERTS

Six information security experts in the industry and academia were interviewed on the usefulness and applicability of the security framework. The experts had to be academics or research students with some experience in the industry. The experts were also selected based on their knowledge and experiences in the information security and their holistic view of this area. The first information security expert is a professor and holds a doctorate degree in the area and has great experience in information security both technical and management security and is working as a lecturer at a university. This information security expert has great experience in security for mobile software agents. The second information security expert holds a doctoral degree in information security, owns a consulting company of information security, and has great experience in the area. The third information security expert is a research student at a university, has good experience in this area, and owns a small consulting information security company. The fourth information security expert holds a doctoral degree in information security, has good great experience in information security and works as a lecturer at a university. This expert has good knowledge in mobile agents’ security technology. The fifth information security expert is a research student at Asian and European universities and has good experiences in information security. The sixth information security expert is research student at Asian and European universities, has good experience in the area, and owns a small information security company. These experts operate in Europe, Asia and USA.
D.1.1.1 Usefulness and Applicability of the Holistic and Immune Security Framework

We asked the following questions to the information security experts. We present the results of the interviews in this section. Five information security experts of the information security experts replied that the deterrence subsystem could be useful in their organizations as shown in TABLE 26.

### TABLE 25: CAN THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK AND ITS SUBSYSTEMS ABLE TO BE APPLIED / IMPLEMENTED / USEFUL IN YOUR ORGANIZATION.

<table>
<thead>
<tr>
<th>Can it be implemented?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>NOT SURE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Need more information</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

One security expert needed more information before deciding whether to implement the deterrence subsystem or not. With deterrence sub system, it is important to do runtime checking (to check for programming errors at runtime). Six information security experts replied that the prevention, detection, and subsystems could be useful in their organizations. In the response sub system, it is advisable to have automatic response without manual intervention. Five information security experts replied that the response systems could be useful in their organizations. One information security experts replied that the response subsystem could not be useful in his organization. Four information security experts replied that the recovery subsystem could be useful in their organizations as shown in TABLE 26. Two information security experts needed more information before deciding whether to apply the recovery subsystem in their organizations. We recommended having snap shots of the state of the information system before attacks for the recovery sub systems.

The experts commented that in all the subsystems, it was advisable to have an integrated approach of humans and mobile agents. Automatic response in response subsystem was very useful for it to be more effective. For detection systems, they recommended to have pre requisites of combining intrusion detection tools with mobile agents. All six information security experts replied that the whole security framework could be useful in their organizations. Two information security experts replied that the deterrence subsystem could be 100% useful in their organizations as shown in TABLE 27.
TABLE 26: HOW USEFUL WOULD THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK AND THE SUBSYSTEMS CAN BE TO YOUR ORGANIZATION?

<table>
<thead>
<tr>
<th></th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>75%</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>50%</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>25%</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Two information security experts replied that the deterrence subsystem could be 75% useful in their organizations. One information security expert replied that the deterrence subsystem could be 50% useful in their organizations. One information security expert replied that the deterrence subsystem could be useful by 25% in their organizations. As for the prevention subsystem, four information security experts replied that this subsystem could be 100% useful. Two information security experts replied that it could be 75% useful. In the detection subsystem, three information security experts replied that the subsystem could be 100% useful. Three information security experts replied that this subsystem could be useful by 75% in their organizations. In the response subsystem one of the security experts replied that the subsystem could be 100% useful. Three information security experts replied that the response subsystem could be 75% useful. One information security expert replied that the response subsystem could be 50% useful. As for the recovery subsystem, four information security experts replied that the subsystem could be 100% useful. One information security expert said the subsystem could be 75% useful in his organization. One information security expert replied that the recovery subsystem could be 25% useful in his organization. Three information security experts replied that the whole framework could be 100% useful. Three information security experts replied that the whole framework could be 75% useful in their organizations.
D.1.1.2 Adaptability features of the new security framework

TABLE 27: How satisfied are you with the adaptability features of this holistic and immune security framework to environments?

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Somewhat satisfied</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Not too satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Not at all satisfied</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Four information security experts were very satisfied with the adaptability features of the deterrence subsystem to the environments as shown in TABLE 28. Two information security experts were somewhat satisfied with the adaptability features of the deterrence subsystem to the environments. Two information security experts were very satisfied with the adaptability features of the prevention subsystem to the environments. Four information security experts were somewhat satisfied with the adaptability features of the detection subsystem to the environments. Three information security experts were very satisfied by the adaptability features of detection subsystem to the environments. Three information security experts were somewhat satisfied by the adaptability features of detection subsystem to the environments. One information security expert was very satisfied with the adaptability features of the response subsystem to the environments. Five information security experts were somewhat satisfied with the adaptability features of the response subsystem to the environments. Three information security experts were very satisfied with the adaptability features of the recovery subsystem. Two information security experts were somewhat satisfied with the adaptability features of the recovery subsystem. One information security expert was not too satisfied with the adaptability features of the recovery subsystem. Four information security experts were very satisfied with the adaptability features of the whole framework to the environments. Two information security experts were somewhat satisfied by the adaptability features of the whole framework to the environments.
TABLE 28: HOW SATISFIED ARE YOU WITH THE ADAPTABILITY FEATURES OF THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK TO THE VALUES OF THE PEOPLE USING THE INFORMATION SECURITY SYSTEMS?

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very satisfied</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Somewhat satisfied</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Not too satisfied</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Three information security experts were very satisfied with the adaptability features of the deterrence, prevention, and response subsystems to the culture, traditions, ethics, and other social issues of users using the information security system as shown in TABLE 29. Three information security experts were somewhat satisfied by the adaptability features of the deterrence subsystem to the culture, traditions, ethics, and other social issues of users using the information security system. Two information security experts were somewhat satisfied by the adaptability features of the prevention subsystem to the culture, traditions, ethics, and other social issues of users using the information security system while one was not too satisfied. Two information security experts were very satisfied with the adaptability features of the detection subsystem to the culture, traditions, ethics, and other social issues of users using the information security system. Four information security experts were somewhat satisfied with the adaptability features of the detection subsystem to the culture, traditions, ethics, and other social issues of users using the information security system. Three information security experts were somewhat satisfied with the adaptability features of the response subsystem to the culture, traditions, ethics, and other social issues of users using the information security system. Four information security experts were very satisfied with the adaptability features of the recovery subsystem to the culture, traditions, ethics, and other social issues of users using the information security systems while two were somewhat satisfied with these features. Four information security experts were very satisfied with the adaptability features of the whole framework to the culture, traditions, ethics, and other social issues of users using the information security system while two were somewhat satisfied by the adaptability features of the whole framework to the culture, traditions, ethics, and other social issues of users using the information security system.

D.1.1.3 COMMENTS
The fourth information security expert commented, “Based on the information I have seen, this seems to be one of the few frameworks that take cultural behavior as an integral part of the design context. Since human behavior is one of the main sources of computer insecurity, I think that integrating this into the security framework should lead to much better results than just designing security systems from a strictly technical perspective.” The security of agents needs to be addressed. The software agents need to be secure before giving them the ability to defend others. The agents should be trained before being allowed to protect the information systems. It is advisable to add special features like intelligence that are feasible to apply. It is also recommended to create a selling package
process for the framework in a form of guidelines of how to work with the framework. This will help the organizations to have a good starting point when applying the framework. The fourth information security expert pointed out that “An adaptive framework like the one described would be very useful in a university environment where changes happen rapidly.” The first information security expert commented, “Assuming that all the people’s values are known then the adaptability measurers will be effective. As for the detection subsystem people’s behavior are dynamic and it is not easy to predict people’s behavior.”

Theoretically, the adaptability features to environments are sound but it is hard to evaluate the features until applied in their organizations. Theoretically, adaptability features to the culture, traditions, ethics, and other social issues of users are good but it is hard to say exactly how effective they will be when applied in the companies. The fourth information security expert said, “I think that adaptability is the main quality and characteristic of the whole framework. Being able to develop and insert new agents "on the fly" should make it possible to not only respond to threats quickly but also to support changes in network architecture and topology.”

The framework can be useful in an organization to structure the security work. It is a good framework for technical organizations. It is also a good model and it will be highly useful in a company. There are many technical solutions but there is no framework that can make them fit together which makes this framework very useful in fitting the different technical solutions together. We can apply the framework as a benchmark to see whether all the information security areas are there in an organization like control, centralized login and other areas. The security framework could be very useful for small and big organizations. In the small organizations where they don’t have many employees to tackle all the features of the subsystems they can let the little manpower that they have concentrate on the most important subsystems.

D.1.1.4 THE SUGGESTED ARCHITECTURE FOR IMPLEMENTATION
The first information security experts suggested the following architecture for implementation using software mobile agents as shown in Figure 90. The architecture has the following components. The identity management server (IDMS) manages identities of the security framework. The certification Authority (CA) server would be used for managing digital certificates of the security framework. The Policy Decision Point (PDP) would be applied for making decisions about authorizations in the security framework. The Universal Description Discovery and Integration (UDDI) server would be used for creating software mobile agents and registering their services using the Service-Oriented Architecture (SOA, 2009). The Extensible Access Control Mark-up Language (XACML) would provide access control services in the security framework (SOA, 2009). The Magnet platform was an agent platform where one could enquire available services at the UDDI server. If the agent providing the required service were available at the UDDI server would launch the agent from agents’ repository and the magnet platform. If the required agent were not available at the UDDI, the server would notify the magnet manager to create an agent. When probes appear, we need to detect and respond by deterrence. When attacks come, we need to detect them. When intrusions come, we need to detect them and protect /prevent them. When penetration occurs, we need to detect them and recover from damages.
We conducted this interview to ten master students in information systems security.

D.1.2 Survey of a Group of Master Students in Information Security
The first group of 11 master students was given a brief description of the security framework and then they answered the questionnaire. The following section presents the result of this survey.

D.1.2.1 Usefulness and applicability of the holistic and immune security framework
The majority of master students strongly agreed that the holistic and immune security framework and its subsystems would be useful in their organizations as shown in Table 30

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Agree</td>
<td>7</td>
<td>7</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Agree</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Do not agree</td>
<td>1</td>
<td>2</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Need more information</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

One master student did not agree that the deterrence system could be useful. Two master students did not agree that the prevention subsystem could be useful while one student
did not agree that the recovery sub systems could be useful. The minority of students needed more information before they could decide.

D.1.2.2 ADAPTABILITY FEATURES OF THE HOLISTIC AND IMMUNE SECURITY FRAMEWORK
We wanted to know the opinions of students on the adaptability features provided by the holistic and immune security framework.

TABLE 30: THE ADAPTABILITY FEATURES OF THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK WILL MAKE INFORMATION SYSTEMS LEARN TO ADAPT TO ENVIRONMENTS WHERE THE INFORMATION SYSTEMS OPERATE.

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>5</td>
<td>4</td>
<td>8</td>
<td>6</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>Agree</td>
<td>6</td>
<td>7</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Do not agree</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The majority of master students agreed that the adaptability features of this security framework would make information sub systems learn to adapt to environments as shown in TABLE 31. However, one master student did not agree that the adaptability features in this security framework would make the response sub system learn to adapt to environments.

TABLE 31: THE ADAPTABILITY FEATURES OF THIS HOLISTIC AND IMMUNE SECURITY FRAMEWORK WILL MAKE INFORMATION SYSTEM ADAPT TO THE VALUES OF THE PEOPLE (TRADITION, CULTURE, LAWS, ETC) USING THE INFORMATION SYSTEMS.
Do you agree?

<table>
<thead>
<tr>
<th></th>
<th>Deterrence Subsystem</th>
<th>Prevent Subsystem</th>
<th>Detect Subsystem</th>
<th>Respond Subsystem</th>
<th>Recover Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Agree</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Do not agree</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The majority of master students agreed that the adaptability features of this security framework would make information sub systems learn to adapt culture, traditions, ethics, and other social issues of users as shown in TABLE 32.

**D.1.2.3 Strength of the New Framework in Preventing Attackers**

**TABLE 32: This Holistic and Immune Security Framework Will Be Successful in Preventing an Adversary of It From Attacking an Information System**

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Agree</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Do not agree</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOT SURE</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

The majority of the master students strongly agreed that this security framework could prevent the attackers from attacking the information systems as shown in TABLE 33. Nevertheless, a good number of master students were unsure about this fact.
The idea of the following questionnaire was to understand the priority by users of different sub systems deterrence, prevention, detection, response, and recovery. Imagine that a security manager of a company has been given 100,000 dollars to spend for information security in the company. How much money would the manager allocate on each of the different sub systems of the security framework? The distribution will reflect the priority of different sub systems.

<table>
<thead>
<tr>
<th>How much to allocate economical resources on each sub system.</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st respondent Weight</td>
<td>20000 0.20</td>
<td>15000 0.15</td>
<td>30000 0.30</td>
<td>15000 0.15</td>
<td>20000 0.20</td>
</tr>
<tr>
<td>2nd respondent Weight</td>
<td>10000 0.10</td>
<td>30000 0.30</td>
<td>30000 0.30</td>
<td>10000 0.10</td>
<td>20000 0.20</td>
</tr>
<tr>
<td>3rd respondent Weight</td>
<td>15000 0.15</td>
<td>30000 0.30</td>
<td>20000 0.20</td>
<td>12000 0.12</td>
<td>23000 0.23</td>
</tr>
<tr>
<td>4th respondent Weight</td>
<td>25000 0.25</td>
<td>20000 0.20</td>
<td>20000 0.20</td>
<td>10000 0.10</td>
<td>25000 0.25</td>
</tr>
<tr>
<td>5th respondent Weight</td>
<td>10000 0.10</td>
<td>20000 0.20</td>
<td>35000 0.35</td>
<td>5000 0.05</td>
<td>30000 0.30</td>
</tr>
<tr>
<td>6th respondent Weight</td>
<td>40000 0.40</td>
<td>25000 0.25</td>
<td>5000 0.05</td>
<td>15000 0.15</td>
<td>15000 0.15</td>
</tr>
<tr>
<td>7th respondent Weight</td>
<td>15000 0.15</td>
<td>40000 0.40</td>
<td>15000 0.15</td>
<td>10000 0.10</td>
<td>20000 0.20</td>
</tr>
<tr>
<td>8th respondent Weight</td>
<td>15000 0.15</td>
<td>15000 0.15</td>
<td>30000 0.30</td>
<td>20000 0.20</td>
<td>20000 0.20</td>
</tr>
<tr>
<td>Average weight</td>
<td>0.1875 18.75%</td>
<td>0.24375 24.38%</td>
<td>0.23125 23.13%</td>
<td>0.1436 14.36%</td>
<td>0.19375 19.38%</td>
</tr>
</tbody>
</table>

The results show, Table 34 that prevention (protection) sub system has top priority, 24.38% of the total budget. Detection sub system comes at the second place in importance with 23.13% of the total budget. Deterrence and recovery have almost equal distributions. Response sub system has the least priority. Note that it is not easy to validate the answers that interviewees give; it is assumed that they answer correctly. When asked to comment on the results of allocation of economical resources on the security value-based chain, Assoc. Prof. Kowalski (Kowalski, 2008) commented that the allocation should depend on the decisions made by the owners of the information security system.
D.1.3 Results of a survey in a group of bachelor of science students in computer and engineering

We made a survey on 27 bachelor students in computer science and engineering, at University of Colombo School of Computing, Colombo, Sri Lanka. Results from the survey are described in the following sections (the results from 7 students were not correctly done and so we dropped them).

D.1.3.1 Usefulness and adaptability of the holistic and immune security framework

We asked the students on the usefulness and applicability of the holistic and immune security framework in the organizations. 19 students agree that the deterrence subsystem would be useful in their organizations as shown in Table 35. One student strongly disagrees that the deterrence system could be useful in the organization. All the 20 students agree that the prevention subsystem would be useful in their organizations. 19 students agree that the detection subsystem would be useful. One student does not agree that the detection system could be useful in the organization. One student strongly disagrees that the deterrence system could be useful in the organization. 19 as shown in Table 35.

TABLE 34: THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS ITS SUBSYSTEMS WILL BE USEFUL IN YOUR ORGANIZATION

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>6</td>
<td>11</td>
<td>10</td>
<td>5</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Agree</td>
<td>13</td>
<td>9</td>
<td>9</td>
<td>14</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>Do not agree</td>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

D.1.3.2 Adaptability features of the holistic and immune security framework

Most students agree that the adaptability features of the security framework would make information systems learn to adapt to environments. However, 4 students do not agree that the adaptability features of the deterrence subsystem would make information system learn to adapt to environments where they operate. Three, one, three, one do not agree that the adaptability features of the prevention, detection, response, recovery subsystems respectively would make information systems learn to adapt to environments.
TABLE 35: THE ADAPTABILITY FEATURES OF THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS WILL MAKE INFORMATION SYSTEMS LEARN TO ADAPT TO ENVIRONMENTS WHERE THE INFORMATION SYSTEMS OPERATE

<table>
<thead>
<tr>
<th>Do you agree</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>9</td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Agree</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>10</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Do not agree</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

17 students agree that the adaptability features of the security framework would make information systems learn to adapt to environments. One student does not agree that the adaptability features of security framework would make information systems learn to adapt to environments. Two students strongly disagree that the adaptability features of the security framework would make information systems learn to adapt to environments as shown in the Table 36.

12 students agree that the adaptability features of the deterrence would make information systems learn to adapt to values of people as shown in the Table 37. However, six do not agree that the adaptability features of the deterrence, prevention, detection, and response subsystem would make information system learn to adapt to values of users. Two students strongly disagree that the adaptability features of the deterrence subsystem would make information systems learn to adapt to values of users. 18 students agree that the adaptability features of the prevention would make information systems learn to adapt to values of people.
TABLE 36: THE ADAPTABILITY FEATURES OF THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS WILL MAKE INFORMATION SYSTEM ADAPT TO THE VALUES OF THE PEOPLE (TRADITION, CULTURE, LAWS, ETC) USING THE INFORMATION SYSTEMS

<table>
<thead>
<tr>
<th>How satisfied are you?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>4</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>Agree</td>
<td>8</td>
<td>12</td>
<td>11</td>
<td>13</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>Do not agree</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Two students do not agree that the adaptability features of the prevention subsystem would make information system learn to adapt to values of users. 18 students agree that the adaptability features of the detection would make information systems learn to adapt to values of people. Two students do not agree that the adaptability features of the detection subsystem would make information system learn to adapt to values of users. 17 students agree that the adaptability features of the response subsystem would make information systems learn to adapt to values of people. 20 students agree that the adaptability features of the recovery subsystem would make information systems learn to adapt to values of people. 19 students agree that the adaptability features of the security framework would make information systems learn to adapt to values of users. One student does not agree that the adaptability features of security framework would make information systems learn to adapt to values of users.

D.1.3.3 STRENGTH OF THE HOLISTIC AND IMMUNE SECURITY FRAMEWORK IN PREVENTING ATTACKS
18 students agree that the deterrence subsystem would be successful in preventing attackers of information systems as shown in the Table 38. One student does not agree that the deterrence subsystem would be successful in preventing an adversary of IT from attacking an information system. One student strongly disagrees that the deterrence subsystem would be successful in preventing an adversary of IT from attacking an information system. All the 20 students agree that the prevention subsystem would be successful in preventing attackers of information systems. 20 students agree that the detection subsystem would be successful in preventing attackers of information systems.
TABLE 37: THIS FRAMEWORK FOR ADAPTIVE INFORMATION SECURITY SYSTEMS WILL BE SUCCESSFUL IN PREVENTING AN ADVERSARY OF IT FROM ATTACKING AN INFORMATION SYSTEM

<table>
<thead>
<tr>
<th>Do you agree?</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
<th>Whole Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>9</td>
<td>10</td>
<td>8</td>
<td>8</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Agree</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>Do not agree</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17 students agree that the response subsystem would be successful in preventing attackers of information systems. Three students do not agree that the response subsystem would be successful in preventing an adversary of IT from attacking information systems. 17 students agree that the recovery subsystem would be successful in preventing attackers of information systems. Three students do not agree that the recovery subsystem would be successful in preventing an adversary of IT from attacking information systems. All the 20 students agree that this security framework would be successful in preventing attackers of information systems as shown in the Table 38.

D.1.3.4 ALLOCATION OF ECONOMICAL RESOURCES ON THE DIFFERENT SECURITY BASED CHAIN FUNCTIONS

The idea of this questionnaire is to understand the weight of deterrence, prevention, detection, response, and recovery sub systems. Imagine that you are a security manager of a company and the Director General of the company has given you 100 000 dollars to spend for information security in the company. How much money will you allocate on each sub system deterrence (scaring away attackers), prevention, detection, response, recovery, following different sub systems of the company?

The results are shown in Table 39

TABLE 38: RESULTS OF THE ALLOCATION

<table>
<thead>
<tr>
<th>Student</th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10000</td>
<td>35000</td>
<td>30000</td>
<td>10000</td>
<td>15000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>20000</td>
<td>35000</td>
<td>20000</td>
<td>10000</td>
<td>15000</td>
</tr>
<tr>
<td>3</td>
<td>20000</td>
<td>40000</td>
<td>15000</td>
<td>10000</td>
<td>15000</td>
</tr>
<tr>
<td>4</td>
<td>20000</td>
<td>27000</td>
<td>28000</td>
<td>10000</td>
<td>15000</td>
</tr>
<tr>
<td>5</td>
<td>10000</td>
<td>15000</td>
<td>35000</td>
<td>15000</td>
<td>25000</td>
</tr>
<tr>
<td>6</td>
<td>10000</td>
<td>30000</td>
<td>20000</td>
<td>15000</td>
<td>25000</td>
</tr>
<tr>
<td>7</td>
<td>15000</td>
<td>35000</td>
<td>20000</td>
<td>10000</td>
<td>20000</td>
</tr>
<tr>
<td>8</td>
<td>20000</td>
<td>10000</td>
<td>35000</td>
<td>20000</td>
<td>15000</td>
</tr>
<tr>
<td>9</td>
<td>20000</td>
<td>10000</td>
<td>35000</td>
<td>15000</td>
<td>20000</td>
</tr>
<tr>
<td>10</td>
<td>15000</td>
<td>30000</td>
<td>30000</td>
<td>5000</td>
<td>20000</td>
</tr>
<tr>
<td>11</td>
<td>10000</td>
<td>30000</td>
<td>30000</td>
<td>10000</td>
<td>20000</td>
</tr>
<tr>
<td>12</td>
<td>25000</td>
<td>30000</td>
<td>20000</td>
<td>15000</td>
<td>10000</td>
</tr>
<tr>
<td>13</td>
<td>15000</td>
<td>30000</td>
<td>30000</td>
<td>15000</td>
<td>10000</td>
</tr>
<tr>
<td>14</td>
<td>15000</td>
<td>30000</td>
<td>25000</td>
<td>20000</td>
<td>10000</td>
</tr>
<tr>
<td>15</td>
<td>15000</td>
<td>35000</td>
<td>20000</td>
<td>10000</td>
<td>20000</td>
</tr>
<tr>
<td>16</td>
<td>10000</td>
<td>25000</td>
<td>25000</td>
<td>15000</td>
<td>25000</td>
</tr>
<tr>
<td>17</td>
<td>25000</td>
<td>30000</td>
<td>15000</td>
<td>15000</td>
<td>15000</td>
</tr>
<tr>
<td>18</td>
<td>15000</td>
<td>35000</td>
<td>30000</td>
<td>10000</td>
<td>10000</td>
</tr>
<tr>
<td>19</td>
<td>5000</td>
<td>40000</td>
<td>30000</td>
<td>5000</td>
<td>20000</td>
</tr>
<tr>
<td>20</td>
<td>15000</td>
<td>30000</td>
<td>30000</td>
<td>5000</td>
<td>20000</td>
</tr>
<tr>
<td>Total</td>
<td>310 000</td>
<td>582 000</td>
<td>523 000</td>
<td>240 000</td>
<td>345 000</td>
</tr>
<tr>
<td>Average distribution</td>
<td>0.155</td>
<td>0.291</td>
<td>0.2615</td>
<td>0.12</td>
<td>0.1725</td>
</tr>
<tr>
<td>Average distribution</td>
<td>15.5%</td>
<td>29.10%</td>
<td>26.15%</td>
<td>12%</td>
<td>17.25%</td>
</tr>
</tbody>
</table>

**D.1.4 Survey of the Master Students on the Effects of Culture on Users Decisions**

We made a survey on 60 master students from France, Sweden, Sri Lanka, Libya, USA, Libya, Taiwan, Thailand, Uzbekistan, Spain, Peru, Pakistan, Nepal, Iran, India, Iceland, China, Brazil, Bangladesh, and Serbia Montenegro. Every master student was to act as a
security manager of a company. The security manager was spend 100,000 dollars for information security in the company.

TABLE 39 RESULTS OF DISTRIBUTION ON THE SECURITY VALUE-BASED CHAIN FUNCTIONS

<table>
<thead>
<tr>
<th>Country</th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>12</td>
<td>27</td>
<td>26</td>
<td>13</td>
<td>24</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>8</td>
<td>33</td>
<td>20</td>
<td>11</td>
<td>28</td>
</tr>
<tr>
<td>France</td>
<td>23</td>
<td>26</td>
<td>26</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>16</td>
<td>29</td>
<td>26</td>
<td>12</td>
<td>17</td>
</tr>
<tr>
<td>Pakistan</td>
<td>26</td>
<td>32</td>
<td>17</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Spain</td>
<td>10</td>
<td>30</td>
<td>25</td>
<td>10</td>
<td>25</td>
</tr>
<tr>
<td>Brazil</td>
<td>20</td>
<td>40</td>
<td>20</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>China</td>
<td>10</td>
<td>10</td>
<td>50</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Iceland</td>
<td>5</td>
<td>10</td>
<td>50</td>
<td>30</td>
<td>5</td>
</tr>
<tr>
<td>India</td>
<td>60</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>Iran</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Libya</td>
<td>10</td>
<td>40</td>
<td>30</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Nepal</td>
<td>35</td>
<td>25</td>
<td>15</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Peru</td>
<td>15</td>
<td>20</td>
<td>35</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Taiwan</td>
<td>30</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Thailand</td>
<td>25</td>
<td>18</td>
<td>23</td>
<td>19</td>
<td>15</td>
</tr>
<tr>
<td>USA</td>
<td>20</td>
<td>35</td>
<td>20</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>10</td>
<td>30</td>
<td>30</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>Serbia M.</td>
<td>5</td>
<td>15</td>
<td>30</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>Average</td>
<td>18,42</td>
<td>26,33</td>
<td>25,95</td>
<td>14,15</td>
<td>15,15</td>
</tr>
</tbody>
</table>

Every student was to decide how much to allocate on each sub system deterrence (scaring away attackers), prevention, detection, response, recovery, following different sub systems of the company. The results of the survey are shown in Table 40. We calculated the average distribution on the security value-based chain functions. The average distribution shows that the first priority is to the prevention function with 26, 33% of the total budget. The second priority is the detection function with 25, 95% of the total budget. Deterrence function is on the third place, recovery function is on the fourth place while the response function is on the fifth place as shown on TABLE 40

Thereafter another survey was made on 37 international master students of information security. The scenario was as follows.

TABLE 40: RESULTS OF OUTLINE OF BUDGET ON THE SECURITY VALUE-BASED CHAIN FUNCTIONS

<table>
<thead>
<tr>
<th>Number</th>
<th>Country</th>
<th>Deter</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Greece</td>
<td>20</td>
<td>25</td>
<td>35</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Pakistan</td>
<td>19,2</td>
<td>28,2</td>
<td>27,4</td>
<td>15,2</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>Bangladesh</td>
<td>26</td>
<td>20</td>
<td>25</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>China</td>
<td>26,5</td>
<td>7,5</td>
<td>47,5</td>
<td>8,5</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>Tanzania</td>
<td>16,7</td>
<td>16,7</td>
<td>43,3</td>
<td>20</td>
<td>3,3</td>
</tr>
</tbody>
</table>
The students come from Austria, Bangladesh, China, Greece, Hong Kong, India, Iran, Pakistan, Tanzania, Turkey and Sweden. Every student was to assume to be working for a Global Socio-Technical Security Group. The student was to setup a social technical security system to decrease plagiarism at the Stockholm University. The students were to outline a budget of how 10 million units would be spent using the security value chain of deter, protect, detect, respond, and recover. The results are displayed in Table 41.

**D.1.5.2 Survey of Information Security Experts, Master Students in Information Security, and Bachelor Students in Computing Science**

**D.1.5.2.1 Usefulness of the Holistic and Immune Security Framework**
All the information security experts, master students and bachelor students agree that the holistic and immune security framework is useful in providing security to information in organizations as shown in Figure 91. All the three groups agree that the prevention sub system is useful in providing information security in an organization. However, there a few respondents that do not agree that the holistic and immune security framework is useful in providing information security in organizations as shown in Figure 92. The deterrence, response, and recovery sub systems do not receive the same attention as prevention and detection sub systems. In most organizations, response systems are not part of the security systems.
D.1.5.2.2  ADAPTABILITY FEATURES OF THE HOLISTIC AND IMMUNE SECURITY FRAMEWORK ON ENVIRONMENTS
The information security experts, master students, and bachelor students agree that the holistic and immune security framework and its sub systems provide adaptability features to environments as shown in Figure 93. It is interesting to note that the score of information security experts and bachelor students is equal in all subsystems and whole framework except in one, the response sub system.

D.1.5.2.3 ADAPTABILITY FEATURES OF THE HOLISTIC AND IMMUNE SECURITY FRAMEWORK TO VALUES OF PEOPLE

The survey indicates that the three groups agree that the holistic and immune security framework and its sub system provide adaptability features to values of people as shown in Figure 94. The score on master students is less in all the sub systems and framework except in one sub system the recovery sub system. However, some respondents disagree that the deterrence sub system provides adaptability features to values of people as shown in Figure 95. This is possibly because they did not understand the adaptability features and their provision or they just do not believe that these features could be provided. Another explanation is that there is not enough teaching on adaptability of information systems in the educational system.
D.1.5.2.4 Allocation of economical resources to the security value-based chains of the holistic and immune security framework on environments
The survey shows that the master students and the bachelor students agree that top priority when allocating economical resources is the prevention sub system as shown in Figure 96 and TABLE 42 in US dollars. Master students allocated on average 24,380 US dollars on the prevention system. Bachelor students allocated US dollars 29,100 on the prevention system as shown in Figure 96. The second in priority is the detection system. The third system in priority is the recovery sub system, then the deterrence and lastly the response sub system. The dictators of countries usually allocate more resources in the deterrence system in the interior defense so that citizens should not even think about attacking it. Saddam Hussein, a former president of Iraq, spent 70% of the internal defense budget in deterrence system (Kowalski, 2007). It is interesting to note that the deviation in allocation is not so high.

**TABLE 41: ALLOCATION OF RESOURCES ON THE DIFFERENT SUB SYSTEMS**

<table>
<thead>
<tr>
<th>Sub system</th>
<th>Deterrence Subsystem</th>
<th>Prevention Subsystem</th>
<th>Detection Subsystem</th>
<th>Response Subsystem</th>
<th>Recovery Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average weight master students</td>
<td>18.75%</td>
<td>24.38%</td>
<td>23.13%</td>
<td>14%</td>
<td>19.38%</td>
</tr>
<tr>
<td>Average weight bachelor students</td>
<td>15.5%</td>
<td>29.10%</td>
<td>26.15%</td>
<td>12%</td>
<td>17.25%</td>
</tr>
</tbody>
</table>

Most organizations request for help from consultants to restore back to business the attacked systems. Some organizations put recovery functions on the shoulders of insurance companies. This is also reflected in the survey on how people allocate economical resources on the deterrence, prevention, detection, response, and recovery subsystems. In the survey on the bachelor students in computing science, 29.10% of all economical resources are allocated on prevention sub system. 26.15% of all economical resources are allocated on detection sub system, 17.25% of all economical resources are
D.1.5.2.5 Allocation of economical resources to the security value-based chains for students from different countries

We made a survey of 60 students from France (6.67 %), Sweden (11.7 %), Sri Lanka (1.67 %), Libya (1.67 %), USA (1.67 %), Libya (1.67 %), Taiwan (2 %), Thailand (1.67 %), Uzbekistan (2 %), Spain (1.67 %), Peru (1.67 %), Pakistan (18.3 %), Nepal (1.67 %), Iran (1.67 %), India (3.3 %), Iceland (1.67 %), China (1.67 %), Brazil (1.67 %), Bangladesh (8.3 %), and Serbia Montenegro (1.67 %), and unmentioned countries 20 % as shown in TABLE 43. We made this survey to understand whether culture affect the decisions, which users make when deciding, which of the five security value-based chain were more important. We also noted the differences in decisions between men and women. The results of the survey are shown in Table 43.

TABLE 42: DISTRIBUTION OF RESOURCES TO SUBSYSTEMS

<table>
<thead>
<tr>
<th>Country</th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>12</td>
<td>27</td>
<td>26</td>
<td>13</td>
<td>24</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>8</td>
<td>33</td>
<td>20</td>
<td>11</td>
<td>28</td>
</tr>
<tr>
<td>France</td>
<td>23</td>
<td>26</td>
<td>26</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>16</td>
<td>29</td>
<td>26</td>
<td>12</td>
<td>17</td>
</tr>
<tr>
<td>Pakistan</td>
<td>26</td>
<td>32</td>
<td>17</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Spain</td>
<td>10</td>
<td>30</td>
<td>25</td>
<td>10</td>
<td>25</td>
</tr>
<tr>
<td>Brazil</td>
<td>20</td>
<td>40</td>
<td>20</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>China</td>
<td>10</td>
<td>10</td>
<td>50</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Iceland</td>
<td>5</td>
<td>10</td>
<td>50</td>
<td>30</td>
<td>5</td>
</tr>
<tr>
<td>India</td>
<td>60</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>Iran</td>
<td>10</td>
<td>40</td>
<td>20</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Libya</td>
<td>10</td>
<td>40</td>
<td>30</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Nepal</td>
<td>35</td>
<td>25</td>
<td>15</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Peru</td>
<td>15</td>
<td>20</td>
<td>35</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Taiwan</td>
<td>30</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Thailand</td>
<td>25</td>
<td>18</td>
<td>23</td>
<td>19</td>
<td>15</td>
</tr>
<tr>
<td>USA</td>
<td>20</td>
<td>35</td>
<td>20</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>10</td>
<td>30</td>
<td>30</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>Serbia M.</td>
<td>5</td>
<td>15</td>
<td>30</td>
<td>30</td>
<td>20</td>
</tr>
<tr>
<td>Average weight</td>
<td>18.42</td>
<td>26.33</td>
<td>25.95</td>
<td>14.15</td>
<td>15.15</td>
</tr>
</tbody>
</table>

We also calculated the chi-squares for each country as shown on the table 43. We believe that chi-squares for different countries would be different reflecting the cultures in each country. It is interesting to note that countries like Libya, Iran, Brazil, allocate 40 % of the total budget on prevention sub system. The average weight is deterrence 18.42 %, prevention 26.33 %, detection 25.95 %, response 14.15%, and recovery 15.15 %. This implies that prevention is the most important function, followed by detection, then deterrence, recovery and lastly response. It is also interesting to note that Iceland and...
China would allocate 50% of the money on detection sub system. India has allocated 60% of the budget in deterrence sub system. We believe that culture of users plays an important role when users make decisions on the importance or priority of each of the security value-based chain functions deterrence, prevention, detection, response, and recovery.

We compared a number of results from Sweden, France, Sri Lanka, Pakistan, Bangladesh, and Sri Lanka as shown in Figure 97.

<table>
<thead>
<tr>
<th>Country</th>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>27</td>
<td>26</td>
<td>13</td>
<td>22</td>
</tr>
<tr>
<td>India</td>
<td>60</td>
<td>10</td>
<td>1</td>
<td>19</td>
</tr>
<tr>
<td>France</td>
<td>22,5</td>
<td>26,25</td>
<td>26,25</td>
<td>11,25</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>15,5</td>
<td>29,1</td>
<td>26,15</td>
<td>12</td>
</tr>
<tr>
<td>China</td>
<td>10</td>
<td>10</td>
<td>50</td>
<td>15</td>
</tr>
</tbody>
</table>

**FIGURE 97 RESULTS OF ALLOCATION OF ECONOMICAL RESOURCES FOR A SAMPLE OF COUNTRIES**

Here the results show that China would allocate 50% of the economical resources that allocated for security in detection. 10% of the total budget will be allocated on deterrence and on prevention. 15% of the total budget will be spent on the response and recovery functions. For Sweden, top priority is on prevention which 27% of the total budget is allocated on it. 26% of the total budget would be spent on the detection system. For France top priority is prevention and detection functions and the users from this country allocate equally on these functions. For Sri Lanka, top priority is prevention in which 29.1% of the total budget is spent of this function. Second in priority is detection in which the users allocate 26.16% on this function. For India, top priority is deterrence function in which users would spend 60% of the total budget while only 40% of the total budget is spent on the rest functions. The message here is if one spends many resources on deterrence then attackers would not even try to attempt to attack the information system. It is interesting to note that only 1% of the total budget would be spent on response.
The aim of the survey was also to understand how women and men differ in putting priorities in the value-based chain functions. The number of men was 39 and the number of women was 21.

The results show that the top priority for women is the prevention function in which 27.32% of the total budget is spent on this function as shown in Figure 98. The second in priority for women is the deterrence function in which they spend 25.42% of the total budget on it. The detection function is third in priority where they spend 21% of the total budget. The next in priority is the recovery function with 15.58% of the total budget. The last in priority is the response function in which they spend 10.68% of the total budget.

For men the first priority is prevention function in which they spend 29.3% of the total budget. Second in priority is the detection function with 23.22% of the total budget. Third priority is the recovery function with 17.4%, then deterrence 16.04% and lastly response 14.04%. Men and women agree that prevention is first priority but differ in percentages allocated to the prevention sub system. For women deterrence function has second priority while for men deterrence function has fourth priority. Men and women put the least priority on the response function.

Another aim of the survey was to understand the ratio of social security measures in comparison to technical security measures that people apply in the security value-based chain functions. Figure 98 shows the results. Results show that Sweden would spend 100% of the total budget for deterrence function on technical security measures. Sweden would spend 25% of the total budget for prevention function on social security measure and 75% on technical security measures. Sweden would spend 17% of the total budget for the detection function on social security measure and 83% on technical security measures. Sweden would spend 50% of the total budget for the response function on

FIGURE 98 DIFFERENCE IN ALLOCATION BETWEEN WOMEN AND MEN
social security measure and 50% on technical security measures. USA would apply only social security measures to in the deterrence function. However, USA would apply 28% social security measures and 72% technical security measures in the prevention function as outlined in Figures 101 and 102. USA would apply 25% of the total budget on social security measures and 75% of the total budget on technical security measures in the detection function. However, the results cannot be generalized we need to conduct more surveys to be able to generalize them.

FIGURE 99: RESULTS OF ALLOCATION OF TECHNICAL SECURITY MEASURES IN THE SECURITY VALUE-BASED CHAIN FUNCTIONS
The results show that 55 % , Figure 100, of the total security measures would be allocated to technical security measures while 45 % would be allocated to social security measures in the deterrence function. 70 % of the security measures for prevention function could be allocated to the technical security measures while 30 % could be allocated to social security measures. For the detection function, 72 % could be allocated to the technical security measures while 28 % could be allocated to the social security measures. For the response function, 57 % could be allocated for providing technical security measures while 43 % could be allocated to providing social security measures. 69 % of the security measures for recovery function could be allocated for providing technical security measures while 31 % could be allocated for providing social security measures.
The second survey was made on 37 international master students in information security from Austria (2.7 %), Bangladesh (16.2 %), China (10.8 %), Greece (8.1 %), Hong Kong (5.4 %), India (2.7 %), Iran (2.7 %), Nigeria (2.7 %), Pakistan (16.2 %), Sweden (5.4 %), Tanzania (8.1 %), and Turkey (5.4 %), other unmentioned countries 13.5 %.

The results of the second survey on 37 international master students are shown in Figure 102.
It is interesting all the students from China allocated less than 10% on the prevention, response, and recovery sub systems but allocated 47% of the total budget on detection sub system. Note also that Nigeria allocated nothing on the prevention and detection sub systems. Turkey on other hand spent 62% of the whole budget on detection sub system. In this scenario, the detection function was perceived to be more important than other functions with the average of 37% of the whole budget. The recovery sub system got the lowest allocation with average 10.4% of the whole budget. The Table 44 shows the difference in averages on allocation from the surveys on 60 master students and on 37 master students. In the 60 students survey the response function was the lowest while in the 37 students’ survey recovery was the lowest as shown in Table 45. The results show that priority on the different security value-based chains depends not only on the culture but also on the properties of an information system that is being protected.

REFERENCES
Kowalski, S. (2008). Lectures Research in Information systems security, scientific methodology course, Department of Computer systems sciences, University of Stockholm and Royal Institute of Technology, Stockholm, Sweden
APPENDIX E - OVERVIEW OF RESEARCH METHODOLOGIES

E.1 GENERAL RESEARCH METHODOLOGIES

According to philosophy of science (Curd & Cover, 1998), there are different methodologies for conducting a scientific research. However, it is interesting to note that major discoveries in science have not resulted from applying the scientific research methodologies that the philosophy of science recommends (Kjellin, 2008). For instance, when Albert Einstein (Kjellin, 2008) was conducting research on the speed of light, Einstein applied high imagination on how it would feel to travel at that high speed of light. Einstein got the idea from one adventure of Baron Münchhausen, in which Münchhausen was sitting on a bullet that was fired round the globe (Gascoigne, 1747).

Researchers apply two main general research methodologies, quantitative and qualitative (Patton, 2002). Dr Tarimo (2006, p. 31) wrote: “Quantitative researchers seek casual determination, prediction, and generalization of findings; qualitative researchers seek instead illumination, understanding, and exploration to similar situations.” Qualitative methodology is applied to investigate the reasons behind why and how decisions are made. There are different types of reasoning (argumentation) in scientific methodologies. Inductive logic is a type of reasoning in which one uses arguments to make generalizations based on individual instances. A researcher observes some phenomena, collects data, analyzes the data, and draws conclusions, which result, into a theory. For instance, a researcher observes that Ann is human and must communicate with others to survive. The researcher then generalizes that all humans must communicate with others to survive. Another type of reasoning is deductive, in which a researcher applies deductive arguments to make conclusions on individuals from general observations (Kjellin, 2008; Verhagen, 2008). One starts from a theory, makes a hypothesis, collects data, analyzes the data, confirms or casts the hypothesis, and draws conclusions. Hypothetical-deductive (Kjellin, 2008) is a methodology in which a researcher starts from a hypothesis, observes, and collects data to prove the hypothesis (Kjellin, 2008). Design science research methodology (Kjellin, 2008; Kuecher & Vaishnavi, 2007) is a new type of scientific methodology in which a researcher can design a model, a system, an interface, a framework as shown in Figure 103.
The design science methodology starts by having awareness of a problem and by defining the research problem. The next step is to suggest how to solve the research problem by drawing abductively from the knowledge that exists in the area (Kuecher & Vaishnavi, 2007). Thereafter a researcher develops an artifact. Then the developed artifact is to be evaluated based on the functional specifications. Development, evaluation and suggestions could be iterated a number of times. The arrows circumcision, operation and goal knowledge indicate that new knowledge could be acquired from the specific process or act of development. Circumscription is a formal logic method based on an assumption every piece of knowledge is valid only in certain situations (Kuecher & Vaishnavi, 2007). Lastly, a conclusion is drawn and knowledge is discovered.

Action research (Kjellin, 2008; Verhagen, 2008) is a reflective research methodology in which a researcher draws scientific conclusions in a process of solving problems. Grounded theory is a research methodology in which a researcher does not follow the traditional research steps (Kjellin, 2008). A researcher starts by collecting data. The data are then coded, classified and put into categories, and then theories are made from the conclusions (Kjellin, 2008). A case study is a research in which a researcher investigates a phenomenon in a real time context (Kjellin, 2008; Verhagen, 2008; Dul & Halk, 2008). The author applied qualitative methodology. The author applied qualitative research methodology because the methodology is concerned with values, attitudes and assumptions about how people think, and it focuses on the process and not just on outcomes (Martella, Nelson & Marchand-Martella, 1998). After discussing the general research methodologies, the author briefly describes the specialized methodologies for systems that were applied in the research.
E.2. Specific Research Methodologies for Systems

The author further applied research methodologies that are specific to systems. These methodologies include System thinking principles (Weinberg, 1975), Cybernetics theory (Wiener, 1948), holistic research process (Schwaninger, 2007), and Soft systems methodology (Checkland & Scholes, 1990; Stowell, 1995; Williams, 2005). The author applied the Soft Systems Methodology (Checkland & Scholes, 1990; Stowell, 1995; Williams, 2005), Figure 104, to observe the real-world situation in security of information systems.

![Figure 104: Soft Systems Methodology](image)

A survey was made on existing standards, models, paradigms, and fundamental theories and concepts. The models and standards were analyzed to determine and identify the fundamental theories and concepts, which can be applied to address the research problem. The author applied system-thinking principles (Weinberg, 1975) to explore systems holistically and to identify the critical systems of the framework for adaptive information security systems. The Cybernetics theory (Wiener, 1948) was applied to provide measures for controlling the information systems using feedback mechanisms (Schoderbek & Kefalas, 1990) and to provide adaptability of information systems.

E.3. Security Requirements

When developing an information security system there are a number of steps that a researcher should follow (Newman, 2003). The first step is to identify the threats and vulnerabilities. The second step is to analyze the security requirements based on the identified threats and vulnerabilities. Thereafter the researcher identifies the standard security services that would meet the security requirements. The next step is to identify the standard security mechanisms for implementing the security services. The next step would be to design security architecture of the information security system. Then the researcher would implement the design. The next step would be to audit the implemented system. Thereafter the researcher would evaluate and continuously evaluate the system. Notice that in designing an information security system, one has to thinks of two major
issues. The first issue is to secure a system from a sequence of attacks under a sequence of conditions (Kowalski, 2011). For instance, a researcher could specify the attacks and conditions under which the system is secured to in the form: system A is secured from attack 1 under condition 1; and from attack 2 under condition 2 ... and from attack N under condition N. The second issue is to secure a system to function to a series of conditions. For example, you develop a number of functions in a system and these functions are supposed to function under a series of conditions: function 1 will function under condition 1; function 2 will function under condition 2 ... function K will function under condition K.

The first security requirement according to Homeland security (2007) is traceability. The second requirement is to identify stakeholder security related needs. The third security requirement is asset protection, which implies that hardware, software, information, human and organization, and physical and computing assets should be protected. The fourth security requirement is threat analysis. In this case, threat entities and categories need to be identified, analyzed, and forecasted. The next security requirement is the interface and environment, which implies that a system should be able to interface and run both in friendly and hostile environments without compromising security. The next security requirement is usability needs. The next security requirement is reliability. The next security requirement is availability, tolerance, and survivability, which implies that developers need to know measures for making a system tolerant to violations. The next security requirement sustainability (maintainability) needs. The next security requirement is deception (hiding) which aim at making an illusion that the system could not be attacked. In addition, one could install systems like hone pots to mislead attackers. The next security requirement is validability, verifiability, and evaluatability, which help to perform diagnosis, repair, and assurance activities. The next security requirement is certification using the identified standards. The next security requirement is system accreditation and auditing using the relevant standardized approach.

Then one has to perform requirements analyses (Homeland security, 2007) in order to discover requirements that are relevant to the security system. The first is risk analysis, which aims at analyzing possibilities of attacks and their effects. The second type is feasibility analysis, which aims at understanding the feasibility of the security requirements. Some requirements are not feasible from technical, economical, organizational regulatory viewpoints. The next analysis is tradeoff. In some cases, the stakeholders may prioritize and perform tradeoff studies to understand the impact of security and privacy requirements. The impact on usability, performance, and other characteristics may be investigated. In addition, it is important to do an analysis of conflicts among security requirements that could arise because of differing viewpoints, policy models, and inconsistent possibilities of configurations.

REFERENCES


APPENDIX F - THEORETICAL ANALYSIS - FUNCTIONAL REQUIREMENTS OF COMMON CRITERIA

Common criteria provide a set of requirements for security products or systems. “While there are cases where a Target of Evaluation (TOE) consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these” (Common Criteria, 2009, p32). The author starts by mapping the framework against the criteria from the Common criteria in the form of security functional requirements (Common criteria, 2006). There are eleven classes of security functional requirements in Common Criteria. The first class is protection of target of evaluation of security functions.

F.1 CLASS PROTECTION OF TARGET OF EVALUATION OF SECURITY FUNCTIONS (TSF)

This class contains fourteen families of functional requirements (CC, 2006) for providing integrity and management of the mechanisms of security services. The first family is called fail secure, which aims at preserving a secure state during failure. This is provided by the fault tolerance system in this framework. The second family is availability of exported TSF data, which defines rules for preventing loss of data (keys, audit data) on transfer between products. Advanced Encryption Standard (FIPS 197, 2001) provides this feature in the integrated security system of this framework. The third family is confidentiality of exported TSF data, which defines rules for preventing data from unauthorized disclosure. It is implemented by the Advanced Encryption Standard (FIPS 197, 2001) in the integrated security system and is provided in all components by software agents. The fourth family is integrity of exported TSF data, which is implemented by the HMAC (NIST FIPS 198, 2008). The fifth family is internal TOE TSF data transfer, which provides protection requirement for data transfer in internal channels. This requirement is provided by the detection system using software agents. The sixth family is TFS physical protection, which defines rules for protecting TSF against physical attacks. This is provided by the security policies in the integrated security system of this framework.

The seventh family is trusted recovery, which aims at defining rules for trusted manual and automatic recovery of TOE and the functions. This is provided by the recovery system of the framework. The eighth family is replay protection, which defines rules for detecting replay and preventing replay of data. This is provided by the detection system using one time tokens and timestamps. The ninth family is state synchrony protocol, which defines a protocol for helping parts of a TOE to synchronize states after some security actions. This is not implemented in the security framework. The tenth family is time stamp, which requires a reliable time stamp mechanism in the TOE. The integrated security framework provides the time stamp. The eleventh family is inter-TSF TSF data consistency, which defines requirements for sharing consistency data. This requirement is provided by the directory system in the integrated security system. The twelfth family is testing of external entities which is a family intended for performing tests on external...
entities. The thirteenth family is internal TOE TSF data replication consistency. This family provides requirements for making sure that data is consistent in internal components of the TOE when some network connections are broken. This is provided by the directory system in the integrated security system of this framework. The last family is TSF self test which defines rules for self-testing to check correctness of functions and critical operations. Self-test can be done in the start up or periodically. This is provided by the fault tolerance system. The strength for this criterion in the framework is 3. The criterion can be provided by multiple mechanisms. For example, Hash-keyed Message Authentication Code (NIST FIPS 198, 2008) would provide integrity security service. Integrity could also be provided by secure hash algorithm or message digest algorithm. This criterion would also be provided by social and technical security measures.

F.2 CLASS SECURITY AUDIT

This class is used to recognize, record, keep, and analyze the security events. This class has six families (Common criteria, 2006). The first family is security audit automatic response, which defines the response to be taken when the detected events show security violations. The second family is security audit of data generation, which provides requirements for recording events that occur in a product or system. The third family is security audit analysis, which defines rules for automatic analysis of security events. The fourth family is security audit review, which defines the requirements for audit tools that are needed for review of audit data. The fifth family is security audit event selection, which defines requirements for selecting events to audit from all the events that occur. The last family is security audit event storage, which deals with requirements for creating and maintaining a secure audit trail. The special analysis component and the detection system of this framework provide the functions in this class. These systems perform security audit in all the components in the security framework. The events are protected and anyone accessing them must be authenticated and authorized. At the lowest level, software agents perform audit automatically. The software agents collect the relevant information and send it for analysis. The software agents raise alarms in accordance to the security policy. The ISO 27001 standard, which is the latest standard that is recommended for security audit, is applied to provide this security service. This criterion has strength 3 in the framework. Multiple mechanisms would provide this criterion. The security measures for providing this criterion would both be social and technical measures. The social security measures for providing this criterion could be in the form of laws and policies. This criterion would also be provided by social and technical security measures.

F.3 CLASS COMMUNICATION

Communication class has two families. The first family is called non-repudiation of origin. This family defines requirements for providing evidence on the originator of some message. The second family is called non-repudiation of receipt. This family defines requirements for providing evidence that the recipient received a message. These functions are provided by the integrated security system in accordance to the Public Key Cryptographic standards (RSA, 1998). Software agents provide these security services in all the components. The criteria would be provided by multiple security digital signature and notary mechanisms. The criterion would also be realized by the social and technical security measures. Social security measures for providing this criterion could be in the form of laws and policies. The strength for this criterion in the framework is 4.
F.4 CLASS CRYPTOGRAPHIC SUPPORT
This class defines requirements for high-level cryptographic objectives like authentication. This class has two families. The first family is cryptographic key management, which defines requirements for management aspects of keys. The second family is cryptographic operation for providing requirements for operational use of cryptographic keys. These functions are provided by the public key infrastructure (PKI) in integrated security system component of this framework. The key management bases on the National Institute of Standards Technology (NIST) (NIST-key, 2000). Multiple mechanisms like NIST-key, Diffie Hellman could implement this criterion. Social security measures in the form of policies or managerial could provide the criterion. The criterion would be implemented using technical and social security measures. The social security measures for this criterion would be the key policies and procedures. The strength of this criterion in this framework is 4.

F.5 CLASS USER DATA PROTECTION
This class defines requirements for protecting user data in a TOE, during import, export, and storage. This class has thirteen families. The first family is access control policy, which defines access control policies and the scope of control. The second family is access control functions, which define rules for the specific functions that can implement access control policy. The third family is data authentication, which defines a method for providing a guarantee of the authenticity of information. This family is provided in accordance to the NIST standard (NIST FIPS 198, 2008). The fourth family is export from TOE, which defines rules for exporting user data. The fifth family is information flow control policy for identifying information flow control policies and defines the scope of control. The sixth family is information flow control functions, which describe the rules for the specific functions that can implement information flow control. The seventh family is import from outside of the TOE for defining the mechanisms for importing and protecting user data. The eighth family is internal TOE transfer, which addresses requirements for protection of user data while in transfer from separated parts of the TOE using an internal channel. The ninth family is residual information and it is responsible for defining requirements for taking care of user data when a resource is re-allocated to another object. The tenth family is rollback for addressing requirements for undoing an operation or a series of operations to preserve integrity of user data. The eleventh family is stored data integrity for defining requirements for the integrity of data that is stored. This family is realized based on the Hash-keyed Message Authentication Code (HMAC) standard. The twelfth family is inter-TSF user data confidentiality transfer protection for providing requirements for confidentiality of user data when in transfer using external channels. The last family is inter-TSF user data integrity transfer, which addresses integrity of user data when in transfer using external channels. The integrated security system of this framework provides this family in accordance to the ISO/IEC 9594-1 (2005) directory system standard. These requirements are provided by the integrated security system using the Security Assertion Markup Language (SAML) standard (OASIS, 2003), Advanced Encryption Standard (FIPS 197, 2001). Multiple security mechanisms would realize the criterion including multi-authentication mechanisms with certificates, biometrical, and challenge-responses. Technical security measures would be applied to realize this criterion but it will difficult to realize this
criterion with social security measures. The strength of this criterion in the framework is 4.

F.6 CLASS IDENTIFICATION AND AUTHENTICATION

The identification and authentication class addresses requirements for establishing and verifying user identities. There are six families in this class. The first family is authentication failures for provision of requirements to define values of unsuccessful authentication attempts and actions to be taken. The second family is user attribute definition, which defines requirements for associating user security attribute with users. The third family is specification of secrets for addressing requirements for mechanisms that enforce defined quality metrics on provided secrets. The fourth family is user authentication for defining the types of mechanisms supported by the TOE and the user attributes that user authentication is to be based on. The fifth family is user identification for defining conditions under which users are required to identify themselves. The last family is user-subject binding which addresses the requirements for creating and maintaining associations between user security attributes and users. The functions in this class are provided by the integrated security system based on the ISO/IEC 9594-8 (2005) standard, Digital Signature Standard (DSS) and digital certificates X.509 standards. The criterion would be provided by and multi-mechanisms. The criterion would be provided by the technical security measures. The strength of this criterion is 4 in the framework.

F.7 CLASS SECURITY MANAGEMENT

Security management class specifies management of several aspects of security attributes data and functions. This class has seven families. The first family is called management of security attributes for allowing authorized users to manage security attributes. The second family is management of TFS data for allowing authorized users control over management of TFS data. The third family is called revocation and it is for addressing revocation of security attributes. The fourth family is security attributes expiration for enforcing time limits on the validity of security attributes. The fifth family is specification of management functions for allowing the TOE to provide specification of management of functions. The sixth family is called security management roles and it is for controlling the assignment of different roles to users. The last family is management of function in TSF for allowing authorized users to control management of functions. The functions in this class are provided by the integrated security system based on the ISO/IEC 9594-1 (2005), ISO 27001 (2008), and SAML (OASIS, 2003) standards. This criterion has strength of 3 in this framework. Multiple mechanisms would provide this criterion. The criterion would be realized by social and technical security measures. The social security measures would be in form of policies and procedures.

F.8 CLASS PRIVACY

Privacy class defines requirements for privacy. “Privacy protects the personal information of individuals from misuse by governments or corporations. Privacy principles include the lawful use of personal information, the accuracy of that information, and the disclosure, consent, and secure transmission of that information” (Homeland security, 2007, p 68). There are four families in this class. The first family is anonymity, which defines requirements for users to be able to use a
resource without disclosing their identity. The second family is pseudonymity for defining requirements for protecting user’s identity but still being accountable for the use of a resource. The third family is Unlinkability and it provides requirements for allowing users to make multiple uses of resources or services without others being able to link these uses. The last family is unobservability for addressing requirements to ensure that when a user is using a resource or a service, a third party cannot observe the actions. The requirements in this class are provided by the integrated security system of this framework based on ISO 22307 (2008) standard. The strength of this criterion is 3 in the framework. Multi mechanisms could implement privacy. Privacy class would be provided by both social and technical measures. The social security measures would include laws and policies.

F.9 CLASS RESOURCE UTILIZATION

Resource utilization class is for providing requirements for supporting the availability of required resources. There are three families in the class. The first family is fault tolerance for defining requirements for maintaining correct operations even during failures. The second family is priority service for addressing requirements to ensure that high priority services are always performed without interference from low priority services. The last family is resource allocation, which defines requirements for making sure that denial of service does not occur because of some unauthorized monopoly on resources. The criterion is provided by the fault tolerance system in the framework. The strength of this criterion is 3 in this framework. The criterion would be implemented by multi mechanisms. The class would be realized by social and technical security measures. The social security measures would be in the form of policies.

G.10 CLASS TARGET OF EVALUATION ACCESS

This class provides requirements for controlling the establishment of user’s sessions. There are six families in this class. The first family is limitation on scope of selected attributes for providing requirements to limit the scope of security attributes that a user may select for a session. The second family is limitation on multiple concurrent sessions for addressing requirements to limit the number of concurrent sessions that belong to the same user. The third family is session locking for defining requirements for capability of locking, unlocking, termination of interactive sessions. The fourth family is TOE banners for addressing the requirements to display n advisory warning to users on the appropriate use of the TOE. The fifth family is TOE access history for defining requirements to display to a user upon successful session establishment the history of successful and unsuccessful logon attempts to access user’s account. The last family is TOE session establishment, which addresses requirements for denying a user to establish a session with the TOE. This security framework partially provides this class. It could also be provided by social and security measures. The social security measures could be in the form of policies and procedures.

F.11 CLASS TRUSTED PATH/CHANNELS

The trusted path/channels class addresses requirements for a trusted communication path between users. There are two families in the class. The first family is inter-TSF trusted channel, which defines requirements for creating a trusted channel between TOE security functions (TSF) and other trusted IT products. The second family is trusted path for
providing requirements for establishing and maintaining a trusted communication between users and TSF. The functions in this class are provided by the integrated security system. The strength of this criterion in the framework is 3. Technical security measures would also implement this criterion.

REFERENCES


NIST 800-86 (2006). Guide to integrating forensics techniques into incident response, special publication SP 800-86


OASIS, (2003), Assertions and Protocols for the OASIS Security assertion Markup Language, 1(1)
APPENDIX G: CULTURE AND MOTIVATION

G.1. OVERVIEW

Motivation theories are necessary for helping us understand how to de-motivate the enemy of information systems not to attack systems. The problem addressed by the paper is whether we could apply the same theories for motivating employees to do good security actions and to motivate deviant employees not to do bad security actions. Culture is responsible for shaping motivations of individuals. Culture affects the mindsets of individuals. Van Dam, Evers, and Arts define culture as a set of values, attitudes, and behaviors that people learn or are passed over to them over a period of time [3]. Organizational culture is defined as a system of shared characteristics that distinguish the organization from other organizations [4]. The shared characteristics include how employees are encouraged to innovate and take risks, to pay attention to details, to focus on outcome or the process to achieve outcomes. It also includes whether the management considers the consequences of outcomes to employees, and whether the focus is on team or individual activities. Other characteristics include the degree of employees’ competitiveness and aggressiveness, and also whether the focus is on growth or stability.

G.2. RELATED THEORIES

G.2.1 INNER PERSON, SOUL, AND OUTER PERSON

Plato, following teachings of Socrates defined the soul as the essence of a person consisting of the mind, the emotions and the desire [2]. Psychologist James Hillman, who is the founder of archetypal psychology, comments that the soul and the spirit are different parts in a human being and are not synonymous. Hillman argues that psychology is a study of the soul and criticizes the 20th century’s psychologies for making psychology to be reductive, materialistic, and literal making them to be psychologies without psyche and without soul [1]. Every person consists of an inner person, the outer person, and the soul a shown in figure 105.
The inner person is also called spirit as Psychologist Hillman comments has a language that is called consciousness or intuition. The outer person consists of the physical body with five senses. The soul is the link between the inner person and the outer person and the soul controls the physical body. The soul consists of the mind, the emotions, and the will power (decision maker). The mind consists of memory, understanding, wisdom, intelligence, and knowledge. The emotions consist of hating, loving, happiness, and desire to be loved and respected; to be sad, hurting, desire to be praised and appreciated. The soul acts as a link between the inner person and the outer person. The soul is like the middle fielders in football, or centers in basketball. The soul takes messages from the outer person to the inner person. The inner person has the ability to lead the outer person through the soul. And the outer person has the ability to lead the inner person though the soul. This implies that there are two types of people those that are led by the outer person and those that are led by the inner person. All these types have their own needs. The inner person has the spiritual needs like worshipping. A person is supposed to worship the true God in order to have peace and to fulfill the true needs of the inner person. However, people have the ability to worship any kind of beings or things like money, ideas, or people. That is why people have movie or sport stars as idols. They tend to have the same attitudes as their idols. This implies that a person would have the same attitudes as the one the person worships. This is exploited by the advertisement industry when they promote products is media by using stars. The soul has psychological needs like love, respect, joy, contact, freedom, power, and achievement. The outer person has physical needs like food, shelter, sex, clothes, and others.

This is the base of motivation, perception, and people’s attitudes and behaviors. When an incident happens to a person that hurts a person the mind records the incident and all the people and circumstances involved in memory. When the person in future
meets the people and circumstances that caused this person to get hurt the mind tends to bring up the incident from memory and the will power makes decisions to have negative emotions to the people involved. It the incident caused the person to be happy then the mind will record the people and circumstances involved in the memory. If the people and circumstances were to show up in future the mind will bring this up and the will power will cause the emotions to be positive like being happy. Over the years from childhood the mind records a lot of issues and incidents. When a child is 5 years old, there are 50% of the beliefs needed for make decisions. When a person is 18 years old, there are already 85% of the beliefs needed for making decisions in place.

G.2.2 THE PRAXIS OF EDUCATING ACTION RESEARCHERS - THE POSSIBILITIES AND OBSTACLES IN HIGHER EDUCATION
Levin and Martin presented praxis of educating action researchers [7]. Action research is a strategic approach to producing knowledge that integrates different methodologies for solving practical problems. The goal of action research is to solve practical problems. Their approach is from two angles. The first angle is how you teach someone to be an action research. The second angle is how anyone could learn to become an action research. It is important to highlight the assumptions that educators have on how people learn action research. According the authors action researchers should have the following capacities. The first capacity is to be able to reflect critically on the process and outcome of a research. The second capacity is to share the knowledge generated during a research. The third capacity is to initiate and support self-involvement is a research. Lastly action researchers should have intervention and research skills. In order for an action researcher to learn these capacities we need to train and educate the action researchers. Training is focused on teaching on particular skills for a desired role. Educating is to teach an action research more comprehensively in wide areas. Herr and Anderson comment that action research is like designing an airplane while flying it at the same time. Levin and Martin suggest four ways in which action research is leaned. The first way is that action research is learned through four components. These components include learning in action, reflecting with others, reflecting on what is written, and interaction through language. The second way is that learning should be organic and consistent with what students are asked to learn. The third way is the role of literature survey in action research. They comment that a student cannot learn by reading about being an action researcher. However, it is in literature one gains theory, scientific and philosophical fundamentals for epistemology that inform about the approach to action research. The fourth way that action research is learned is by testing the theories because experience is linked to testing. It is through testing that we discover and recognize knowledge.

The next issue that they discuss is adult education and action research teaching. The main principles in adult education focus on learners to be self-directed and autonomous focus on the process of learning to build on experience, for the content to be relevant and practical. Emphasis is put on learning in practice because although skills can be taught they can only be developed through experience. Action research could be compared to project-based programs in engineering and architectural colleges.
G.2.3 TOWARDS A THEORY OF ONLINE LEARNING

Anderson reviews general theory of learning and then sorts out the attributes that are necessary to develop deeper and useful theory in online learning [7]. Anderson starts by presenting the three functions of good educational theory as presented by Wilson. The first function of a good educational theory is to envision new worlds. The second function helps individuals to make things like investing time more effectively. The third function of a good theory is that it builds on existing knowledge and helps to interpret and plan for the unknown. Anderson discusses four attributes of learning. The first attribute is learner-centered, which requires awareness by the teacher of the different aspects of a learner like culture, language, expression types, and prerequisite knowledge. The second attribute is knowledge-centered, in which it is understood that effective learning is defined and bounded by the epistemology, language, and context of disciplinary thought. The third attribute is assessment-centered in which teachers are encouraged to apply evaluation and summative assessment that helps to motivate, inform, and provide feedback to both learners and teachers. The negative side of assessment-centered is that it increases the work load of the already pressed teachers. The fourth attribute is community-centered in which students are encouraged to collaborate in order to create new knowledge in online learning. However the negative side of online learning communities is lack of attention and participation.

Anderson discusses the issue of affordances of the net. In developing nations (2005) only 33% have broadband connectivity while in developed nations it was between 67 to 95%. Anderson also examines interaction in online learning which takes the form of video conferencing, audio conferencing, computer conferencing and others. Interaction could be between student to content, student to student, student to teacher, teacher to content, or teacher to teacher. Anderson developed a model of online learning as outlined in figure 106. The model illustrates how students and teachers interact with each other, and with the content. The model also shows the two major modes of online learning which are collaborative, community-of-inquiry models, and community-of-learning models. The interaction in the first model (left on the figure 106), community of inquiry, can be net-based synchronous and asynchronous using video, audio, computer conferences. The second model (right on the figure 106) outlines the structured learning tools in independent learning. These tools include search and retrieval, tutorials, simulations and games, virtual labs, and e-Books. The student is supported by different members both family and professionals. Anderson presents how students learn different moments in their study as developed by Mark Prensky. Prensky said that students learn behavior through imitation, feedback, and practice. They learn creativity through playing.
We learn facts through different associations, drill, memory, and questions. Students learn how to judge through reviewing cases, asking questions, making choices, receiving feedback and coaching. Languages are learned through imitation, practice, and immersion. We learn to observe by viewing examples and feedback. The procedures are learned by imitation and practice. We learn about processes by analyzing, deconstructing, and practicing systems. Students learn about systems by discovering principles and tasks. We learn to reason by solving puzzles, problems and by examining examples. Skills are acquired through imitation, feedback, continuous practice, and increasing challenge. Students learn speeches and performance roles by memorization, practice, and coaching. We learn theories through logic, explanations, and questioning. Anderson also discusses online learning and the semantic web. Anderson suggests that there are two technologies that enhance the capacity of Net. The first is a set of formal technologies designed by Tim Berners-Lee who called it the Semantic Web. The second technology is the
development of social network technologies which enables self-organization capacity to the Net.

Anderson concludes by presenting an overview of the theory of online learning interaction. It is suggested that different forms of interactions among students can substituted for each other without decreasing quality of learning. High levels of deep and meaningful learning can be achieved if one of the three levels of interaction (student-teacher, student-student, and student-content) is at a very high level.

G.2.4 DECEPTION AND DESIGN: THE IMPACT OF COMMUNICATION TECHNOLOGY ON LYING BEHAVIOR

Hancock, Thom-Santelli, and Ritchie reports the results of a diary study in which they recorded the lies from the social interactions for seven days. The lies include attempts to be polite like pretending to love one’s hair cut to serious lies like denying an affair. It was observed that students tell at least two lies a day while normal people tell at least one lie a day [12] [13] [15]. Research shows that most lies are spontaneous and not planned. When designing systems of communication it is recommended to consider synchronicity of the interaction, recordability, and whether the speaker and the listener do not share the same physical space. There are some lies that occur more often in face to face communication when questions like how do does one like one’s hair cut or dress. This type of opportunities is less likely to occur during e-mail communication. When participants do not share the same physical space it lies on which one pretends to be writing case report when one is just browsing the Internet. A survey was made 30 students involving 1198 interactions. 310 lies were recorded by the participants over a seven day period. 26 % of the interactions involved a lie.

The study implies that the design of communication technology affects every day lying behavior. In order to reduce deception designers should aim at creating asynchronous and recordable communication technology systems. The study shows that people lie in 14 % in their emails and 21 % in their instant messages. However, the study is based on data in which participants were recording how much they lied, it is difficult to measure whether they recoded few lies or more lies. The results indicate that the participants lied mostly during the telephone conversations and least on e-mails. They also noted that lying during the face-to-face an instant messaging was almost equal. One third of the daily communication involves some form of deliberate attempt to deceive as reported by [11] [12] [13] [14].

G.3. THEORIES OF MOTIVATION

Motivation is defined as the processes that account for intensity, direction, and persistence of an individual’s effort toward achieving a certain goal [4].

G.3.1 HIERARCHY OF NEEDS

Maslow’s hierarchy of needs is one of the earliest theories on motivation. Maslow studied people who were considered to be well established like Einstein [Kowalski 75] and presented in a book called Toward a psychological of being. Maslow hypothesized that
every human being has the following needs [4]. Physiological needs are those needs for food, a home, sex, and other needs of the body. Safety needs include the need for security and protection from physical and mental harm. Social needs include affection, acceptance, the need to belong, and friendship. Esteem includes those needs like self-respect, autonomy, achievement, status, recognition, and attention. Self-actualization is the need to grow, achieve potentials, and self-fulfillment. Maslow put these needs in a hierarchy starting with physiological, safety, social, esteem, and self-actualization. Maslow suggested that it is important the level that the person is in before attempting to satisfy the needs of an individual. If an individual has physiological and safety needs, one should satisfy the social needs that are next in the hierarchy. There is however not much supporting evidence and so it was not possible to validate the theory scientifically. However there are managers who use this theory in practice. Flanders criticized Maslow in the book *Practical psychology* [5] for using self-actualization instead of social-actualization. Flanders made observations that motivation was on the humans need for freedom and human contact.

G.3.2 McCLELLAND’S THEORY OF NEEDS
Another motivation theory is of McClelland’s theory of needs that focuses on three needs [4]. The first is the need for achievement, based on a set of standards. The second is the need for power which implies making others behave in the way they would not have behaved otherwise. The third is the need for affiliation, which is the desire to belong to a group or something. There has been research support for this theory but the theory has little practical. This is due the arguments by McClelland that these needs are at a subconscious level which implies that an employee could have them without knowing. This implies that it is difficult to measure in individuals.

The next section presents the current motivation theories. The first is called Cognitive evaluation theory and it is about different kinds of rewards. The theory suggests that tangible rewards tend to undermine the performance of employees because they tend to focus on the reward instead of focusing on the task. Verbal praises however tend to keep employees to focus on their tasks. However it is difficult to generalize whether this works for all kinds of employees and all kinds of jobs. People accept employments for all kinds of reasons and probably based on the Maslow’s needs. The next theory is goals setting theory which suggests that specific goals are very good motivations and there is evidence to support the theory.

As an example a survey on motivation was made on 57 international master students of security management at the department of computer systems sciences in Stockholm University.
The survey aimed at understanding what motivated them in studying security management. The questionnaire based on the McClelland’s theory of needs of achievement, power, and affiliation. The results for needs for achievement are shown in figure 107.

67 % of the students completely agreed that they were motivated by the need for achievement. 21 % of the students agreed that they were motivated by the need for achievement. 6 % of the students were satisfied that were motivated by the need for achievement. 2 % of the students disagreed that they were motivated by the need for achievement and 4 % completely disagreed.

The second class of needs was the need for power as shown in figure 108. 22 % of the students completely agreed that they were motivated by the need for power. 17 % of the students agreed that they were motivated by the need of power. 35 % of the students were satisfied with the idea that they were motivated by the need to achieve power. 7 % disagreed that they were motivated by the need for power. 20 % of the students completely disagreed that they were motivated by the need for power.
FIGURE 108: RESULTS FROM THE SURVEY ON THE NEED FOR POWER

When it comes to the need for affiliation the results are displayed in figure 109.

FIGURE 109: RESULTS FROM THE SURVEY ON THE NEED FOR AFFILIATION

26 % of the students completely agree that they are motivated by the need for affiliation. 21 % of the students agree that they are motivated by the need for affiliation. 40 % of the
students are satisfied that they are motivated by the need for affiliation. 14% of the students disagree while that the motivation could be the need for affiliation.

G.3.3 Why do people deviate?
Kowalski explained the deviance phenomenon by answering questions why do people deviate, what is deviance, and what socio-cultural conditions produced different rates of deviance [5]. Kowalski received two calls from individuals that brought light to the question why people deviated. The first person was intensely worried about the possibility of a nuclear war after reading about the instability in the Middle East. From the conversation Kowalski learned that this caller had analyzed the political situation and as rational evidence that nuclear war was coming soon. Another person called to Kowalski and was convinced to be a knight of the roundtable. This person had created an irrational trap. Kowalski realized that there the motivation of both callers was the same. Kowalski presents the conclusion made by Lorenz, in the book Civilized man’s eight deadly sins, who said that human behavior whether normal or deviant could be reduced to the basic motivation of survival. In other words Lorenz considered human motivation as a form of instinct. Another psychologist, Murry, concluded that motivation was based on psychological or biological needs. Murry’s theory was criticized by scholars who argued that the theory describes motivation but does not explain motivation. Nevertheless Murry laid down a foundation that there were certain social and ecological factors that led individuals to act deviant. Kowalski comments that individuals are motivated to satisfy biological needs. The biological needs can be put into two categories survival and belonging needs. The psychological needs could be classified into belonging and freedom needs. Needs could satisfied through interaction between individuals and society in the form of commodity or personal interaction. Kowalski developed a model in order to explain the interaction between the individual and society as outlined in figure 110.

![Figure 110: Model of Needs, Means and Ends](image)

The model consists of individuals and their needs, society and its ends or resources and interaction or means between an individual and a society. The individual has the need for freedom, to belong, and to survive and outlined in figure 110. Ends or resources in a society could be in a form of people or things as shown in figure 111.
The interaction could be direct with people in different relationships or roles. Indirect interaction could be in the form of exchange of commodities or some kind of public experience. In the need for survival human strives to have food and shelter. The need for freedom is achieved expressed through unity. Kowalski applied the model in the following as outlined in Figure 112.

FIGURE 111: NEEDS AND INTERACTION MEANS

FIGURE 112: APPLICATION OF THE MODEL IN SOCIETY
Kowalski explains the model by comparing theoretically between the Hopi and modern American culture. Hopi was a group of people who were the farmers of the desert. The American culture has greater need for freedom. The means to reach that freedom would be money. Ru stands for the resources for unity. The model describes that the greater the discrepancy between the means and the resources in a society the greater the rate of deviance. Kowalski points out that the aim of the model is not to define deviance because deviance behavior does not obey any norm. Deviance in the model is a function of the angle of anomie with the principle that the greater the angle the greater the rate of deviance. Deviance is an abnormal use of means whether it is alcohol or money.

This model shows that the Hopi and Modern American culture have different needs. In the model Ru stands for resources for unity, Nu stands for need for unity.

G.3.4 Other Motivation Theories
One of theories of the modern theories in motivation is the goal-setting theory [4]. Specific goals are more effective than general goals because it increases performance of people. It was also understood that difficult goals direct all the attention to the task and ignore all distractions. The difficult goals have a tendency to energize employees because they encourage us to work harder to attain them. The difficult goals trigger the mind to find solutions for more efficient methods and also help to persist. Goal setting theory could be implemented by management by objectives which imply objectives are translated in different levels [4]. The first level is where the overall organizational objectives of a company are set. The second level is to have those overall objectives be translated to divisional objectives. The next level is when the divisional objectives are divided into objectives of a department. The last level of objectives is where departmental objectives were translated into individuals.

The other motivation theory is Self-Efficacy theory [4]. This theory is about the belief of an individual for being able to perform a task. The higher the belief of being able to perform a task the more likely an individual is to succeed in performing a task. There are four ways in which self efficacy could be increased. The first one is by enactive mastery which is increased by gaining relevant experience. The second one is by seeing someone do the task and gaining the confidence this way. The third way is by being confident to do a task because someone convinced an individual of having the skills needed to perform the task. The fourth way is to increase the belief because one has been psyched up to perform better. Another motivation theory is called equity which is about employers comparing the inputs that were put in the job and the outputs [4]. If the inputs or efforts put into the job seem to be higher than the outputs then employees tend to have lower motivation. Another theory is expectancy in which it is believed that the individual effort in a task will lead to a good performance. The good performance will in turn lead to organizational rewards, which will lead to personal goals.

These theories could be used by a security manager when motivating employees to do actions and behave in accordance to the security policy of an organization. It is good practice to study the needs of employees to find out what kind of needs motivates them.
G.4 Could we apply the same theories to motivate people to do have good security behavior and to motivate people not to have bad security behavior?

There are two types of employees normal and deviants. Both these groups have been values that come were accumulated in their minds as a result of cultural influence on them. The distribution curve for normal employees and deviant employees is outlined in figure 113. The percentage of deviants is usually not high but they could cause much damage. As an example, consider the hackers who terrorize users of information systems but they are not high percentage.

![Diagram showing distribution curve for normal and deviant employees.](image)

**FIGURE 113: DEVIANTS CURVE**

G.4.1 Motivating the normal employees to do good security management

The culture has a set of ideas which enter individuals mind though different channels of the culture. The words that are spoken produce a set of thoughts. The set of thoughts produce decisions on different issues. An individual decides to behave or speak in a certain manner because of the words and thought that are in the mind. These behaviors produce a mindset or a habit. In order to change the bad mindsets, we have first to break the bad mindsets that are present in an individual. Second we need to teach the good id and then teach the good mindsets.
The mindset of individuals can be compared to a wall that is protecting a value as outlined in figure 114. A security manager should be able to affect the motivation, perception, and learning of an employee so that the employee should have good security behavior as outlined in figure 115.

The culture produces values like attitudes, personality, and ability. Values are important in organizational behavior because they help to understand the motivation and attitudes of
individuals. Values have two main attributed content and intensity. The content attribute is responsible for determining whether a certain conduct is important or not. The intensity attribute specifies how important a certain conduct is. Individuals assign different weight to issues like religion, freedom, self-respect, honesty, obedience, etc. This is called a value system which is not very flexible [4].

Rokeach created the Rokeach Value Survey consisting of the terminal values and instrumental values [4]. Terminal values are end states to be achieved while instrumental values are means of achieving the terminal values.

Perception is a way which by individual uses to organize and interpret impressions received through the five senses in order to give meaning to their environment. This perception could be right or wrong. Perception is important because people behave according to what they perceive and not according to reality. There are three main factors influencing perception. The first factor is the characteristics of a target. We tend to observe targets together with background. People who have special features are noticed first. The second factor is the perceiver’s characteristics. The interpretation of a perceiver is based on the knowledge or expectations that the individual has. If a perceiver expects a certain person behave in a certain way it will perceived so independent on the reality. The third factor is situation, which include time, location, light, and other issues. The context in which we observer objects are important.

The next issue is how we can apply perception in security management. The Attribute theory presents explanations that our behavior is based on internal or external factors. When we observe behavior of others we tend to ask whether the behavior is caused by internal or external factors. Internally caused behavior is believed to be under the control of an individual while externally caused behaviors are not [4].

G.4.2 Motivating the deviant employees not to do bad in security management

The deviants as Kowalski points out in [5] are as a result of special needs not being met by the society and as a result of certain environmental conditions. When motivating the deviant employees there is another dimension that we should consider. The deviant have a mindset as a result of the cultural wall that protects the values of a certain culture as shown in figure 116.
The deviant have other values which are as result of their special needs not being met by the society so these special needs are protected by another wall called deviances wall. So in this case we have the outer wall which is a cultural mindset wall and inside this wall there is another wall called the deviancies mindset wall. The normal motivation theory that we use today are for removing the first fall and renewing the minds of employees so that they could gave mindset of doing good in security management. These theories are not enough to remove the second wall of deviant employees. We need to develop new theories that would have the ability to remove the deviancies wall.

G.4.2.1 Using negative and positive value-based chain functions to teach deviants
One of the methods we could apply to motivate the deviant employees when teaching security management is to use the negative and positive value-based chain functions as outlined in figure 117.
The negative value-based chain functions are aimed at training deviants while they fear knowing that if they try to do bad security actions the security manager will know it and identify those who did it. The negative value-based chain functions consist of deterring the deviants so that they should not even consider doing bad. The second function is to prevent the deviants when we fail to deter them. The next function is to detect deviant actions. The next function is to respond in cases where we fail to detect the bad actions of the deviants. The last function is to recover from the bad actions of the deviants.

Thereafter after using the negative value-based chain functions for a specified time, which will depend on the results of some survey to be conducted, the security managers could start using the positive value-based chain to educate the deviants that it pays to do good security actions. The first function in the positive value-based chain is to encourage the deviants to do good actions according to the security policy. The next function is to allow the actions of the deviants instead of preventing them. The next function is to monitor the actions of the deviants and then reward the deviants when they perform good actions. The last function let the deviants operate ethically in accordance to the security policies.

In teaching employees to do good security actions it is good practice to use the attributes outlined in figure 118 which include motivation, entertainment, informing, and controlling [9].
When teaching security management how much should a teacher motivate ($M_1$), inform ($I_3$), entertain ($E_2$), and control ($C_2$)? Individuals have different learning styles and are motivated differently. If an employee is motivated following the security policy will tend to be not difficult. But which motivation theory is supposed to be used to motivate employees. Entertainment is important because the signal has to be more than interference to create more medium. We need to entertain more in teaching deviants to motivate them to not to do bad security actions and this could be done by using knowledge bots [8].

G.4.2.2 Designing Security System That Discourage Lying Behavior
Another method for reducing deviant behavior involving lying is by designing information security which have asynchronous and recordability attributes as recommended by Hancock, Thom-Santelli, and Ritchie. When deviant employees are aware that communications are recorded would tend to reduce the lying behavior.

G.4.2.3 Entertaining Using Knowledge Bots
One way that could be used to teach and entertain deviant employees is by using knowledge (ro) bots [8] as shown in figure 119. The student can access the presentations, audio, video, and other materials that are provided via a knowledge bot. The student will have to be authenticated by the system. Then the student has to be authorized before
being permitted to access the materials. The integrity non-repudiation security services have to be provided as shown in figure 119.

![Diagram of Knowledge (Ro)bot]

**FIGURE 119: KNOWLEDGE (RO) BOT FOR TEACHING AND ENTERTAINING DEVIANT EMPLOYEES**

In teaching the deviant employees by entertainment we could higher the scale of entertainment in comparison to the scale we have for normal employees. The knowledge bot has a number of components on the same page. On the left upside we have a section with presentations, audios and videos. On the left side below the presentations we have the background theory for anyone who wants to browse on the theory behind the related subject. This will also help those who prefer that material be presented in textual format than visual format. On the right side of the page we have the demonstration of what is being presented on the left side. Under the demonstration we have tests which an employee could do voluntary basis.

The knowledge robots could have a lot of features that help an employee to gain knowledge in an effective way. For example the knowledge bot could suggest to the employee as outlined in figure 120 to take a break. The reason behind is that to one can concentrate effectively in 20 minutes so after this time an employee could take a break by choosing the activities as suggested by the knowledge bot. during the break a student could decide to choose one of the listed music videos, watch a movie of choice, do physical exercises of do something else.
You have been listening for 20 minutes; the normal effective concentration time is 20 minutes, so please take a 10 minutes break by:

- Watching these music videos of choice
- Watching these movies of choice
- Doing these physical exercises
- Doing something else

FIGURE 120: THE KNOWLEDGE BOT SUGGESTS A BREAK TO THE EMPLOYEE

A study made to understand the time used when studying by using knowledge chatbots in comparison to the time used when studying using quick guides [8]. The time used when employees were using a quick guide was higher than when an employee was using a chatbot as shown in figure 121.

FIGURE 121: TIME USED WHEN USING A QUICK GUIDE AS COMPARED TO WHEN USING A KNOWLEDGE CHATBOT [8]
G.5 CONCLUSION

This paper has discussed the different theories for motivating normal employees to do good actions as specified by the security policies. However, when dealing with how to motivate deviants we need new motivation theories because of the sources that caused the employee to be deviant. One of the methods that a security manager could use is to apply the negative and positive value-based chain functions. These functions could be used by first training the deviant employees with some elements of fear of being exposed if they do bad security actions. Thereafter, the security manager could apply the positive value-based chain functions to educate the deviant employees that it pays to do good actions that are specified in a security policy.

REFERENCES

[6] T. Anderson, Towards a theory of online learning, Distance Education, Athabasca university, Canada
[10] J.T. Hancock, J. Thom-Santelli, T. Ritchie, Deception and design: the impact of communication technology on lying behavior, Department of Communication, Cornell University, New York, USA
APPENDIX H: AUTOPSY OF ICT REPORTED CRIME CASES

H.1 SUMMARY OF THE REPORTED ICT CRIMES

This section briefly describes the ICT crime cases and the results of the analysis. The information on crime in this section is from the US department of Justice (US Justice, 2010). 41 ICT crime cases were analyzed to study the cause in relation to the deterrence, prevention, detection, response, and recovery measures. The first ICT crime case involves Jeanson James Ancheta, in about a computer fraud using federal government in the national defense. Ancheta accessed the computer systems without authorization. Ancheta used servers; Ancheta controlled the servers, and scanned for vulnerable computers systems. Ancheta then directed the servers to a channel of internet relay chat, where the servers were instructed to scan more computers and remain zombies (US Justice, 2010). Ancheta earned $ 3000 for selling access to his botnets. Customers that bought the services used the servers for DDOS. Ancheta discussed with clients what type of spamming they were interested. He instructed them how to maintain the botnets. Downloading adware for more than 400 000 infected computers and $107 000 the advertising companies paid him for every installation of adware. Ancheta received a sentence 5 years in prison.

The second ICT crime was committed by Andre Everton Grant. Grant accessed payroll accounts of US service men using personal information to obtain credit and debit cards. Grant diverted to his bank accounts about $23000. Grant received a sentence of ten years in prison in Maryland. The third crime involves a Michigan man was sentenced to 30 months in prison for conspiring to conduct highly destructive computer attacks on competitors of his online sportswear business. The next crime is an ATM fraud in which criminals used cloned ATM cards to steal $9 million from 2100 ATM machines in 280 cities of US, Canada, Italy, Hong Kong, Japan, Estonia, Russia, Ukraine. One person from Moldavia learned of certain computer network vulnerability in a credit company in Atlanta. The criminal passed the information of the vulnerability to a hacker in Estonia. They raised the money that could be withdrawn and created counterfeit ATM cards. They withdrew the money and tried to delete files to covers their tracks. The next crime involved a former employee to Alta Vista who hacked the Internet search engine using another employee’s credentials.

The next crime case involves Mark Wayne Mille from Ohio who sexually exploited minors. Mille convinced the minor aged girls to perform sexual action this person in for of web cameras. Mille secretly intercepted and recorded the sexual actions and distributed to others. The criminal developed relationship to the minors via chat rooms. It was discovered when one of the girls sent a love letter to the former place of employment of Mille. The next crime is about stealing 26669 credit cards. Juan Javier Cardenas bought stolen credit card numbers and resold the numbers to others. The next ICT crime involves a 38 people network of credit cards thieves. They used the credit cards to purchase airline tickets. The credit card numbers were stolen from banks and hotels in
Kansas City. The next crime refers to a Californian resident, Christopher Maxwell, who attacked a hospital using botnets. Maxwell instructed the botnets to install adware programs on behalf of advertising companies and was paid for the services. Maxwell used the servers from California state university, Michigan and Los Angeles.

The next crime is about William Shea who was a former program manager of a debt collecting company in Silicon Valley. Shea installed a malicious code, which modified and deleted financial records of more than 50000 accounts. The next crime involves Briana Salcedo who hacked Lowe Company and downloaded credit card numbers. Salcedo installed a Trojan horse to capture credit card numbers of customers. The next ICT crime is about Sandra Teague, a former employee of the education department in Iowa. Teague accessed, without authorization, the records of Barack Obama in the students’ database during the election of 2008. The next crime involves botnets that were used to launch a DDOS against eBay. Anthony Clark used a remote procedure call vulnerability to direct the botnets to password protected internet relay chat. The next crime refers to Barbara Denenburg who hacked private boxes of a company that provides voice and person advertisement services to newspapers. Denenburg accessed and changed passwords of 200 customers. The next crime involves a hacker group that was conducting a dark market of selling stolen credit cards and identities. The dark market had 2500 registered members. An undercover FBI agent infiltrated the hacker group and worked as one of the administrators. Millions of dollars were exchanged in the different transactions.

The next crime refers to Reno Jean Daret IV who working with Xbox 360 solutions. Daret advertized modifications of XBOX 360 and when customers came, they were offered to buy copies, which were pirated copies of video games. The next crime involves $70 million cyber banking fraud. A group of criminals target companies that did not have strong protection mechanisms of their computer networks. They installed a Trojan horse called Zeus, which was used to capture bank credentials of victims. The criminals used the stolen bank account information to take over bank accounts and transfer money to mules. The mules transferred the money to criminals. They attempted to steal $220 million but were able to steal $70 million. The next crime involves a network of six people who operated an online market for stolen credit cards and identities. The online site was called www.shadowcrew.com. This group had 18 million e-mail accounts and had commit bank frauds of about $4 million. The next ICT crime refers to the creator of a spy program, Carlos Enrique Melara, called Lovespy. Lovespy was applied to break into computer systems and intercept communications without authorization. The next crime involves a teenager, Juvenile, who released a worm that launched a DDOS attack to a web site of Microsoft. The teenager was sentenced to 300 hours of community work. The next crime is about massive data theft from a company called Acxiom Corporation. Scott Levine stole information worthy millions. The information included personal and financial records belonging to companies. The next crime involves Rajendrasinh Makwana a UNIX engineer wrote a malicious script to Fannie Mae computer servers after being fired. The script was supposed to destroy all financial information, securities, and mortgages of a certain day. The next crime refers to a hacker group called Krogeniks, who disrupted...
services at Comcast Corporation. The hackers Michal Nebel and Christopher Allen Lewis directed all traffic coming to Comcast Corporation to their websites. The next crime involves a former chemist, David YenLee, who stole formulas, valued $20 millions from one company in Illinois YenLee was planning to work for another company in China where was to be president. The next crime was committed by Larry Lee Rupp, who was a former employee of Anaheim insurance company. Ropp wiretapped, without authorization, the secretary to a company executive by installing a keystroke logger.

The next crime involves David Kernell from Tennessee, who accessed e-mail of a former governor of Alaska Sarah Palin. The next crime was committed by Robert Lytle who was a member of a deceptive duo hacker group. Lytle hacked into government computer, defense, NASA, Office health affairs. Thereafter, Lytle defaced government websites with material that was illegally acquired from the attacks. The next crime involves economic espionage with intention to benefit a foreign government. Hexue Huang was arrested for transporting secrets to China while working as a scientist. The next crime is about a bank fraud that was committed by Kenneth Flury. Flury obtained stolen debit card account numbers, PIN codes and personal identifies of true account holders. Flury put the information onto blank ATM cards and obtained $384000. The next crime was committed by Ryan Fisher from Utah who brought down the wireless internet services. Fisher applied the credentials from a company that employed Fisher to reprogram the access points of customers so that they could not reach the Internet. The next crime was committed by Jerome Heckenkamp who hacked major corporations. Fisher defaced the web pages of the major corporations and installed sniffer programs to steal passwords. The next crime involves a former computer security specialist, Kenneth Kwak, who hacked the department of education. Kwak gained access without authorization to the department and placed malicious software on computers belonging to the supervisors. This enabled Kwak to access the computers of supervisors anytime.

The next crime refers to computer intrusions to CariNet computers. Andrew Shelmut changed configurations of networks of CariNet and possessed child pornography. Shelmut also deleted the log files to remove evidence. The next crime is about Alexey Ivanov who hacked into computers in the US and was responsible for a loss of $25 million. Ivanov committed computer fraud, credit card fraud, wire fraud, computer intrusion, stole passwords, and usernames.

The next crime refers to damages to a protected computer system of Interstate communications. Richard Benimeli had demanded to be paid 20% for the past services. When the company refused to pay, Benimeli accessed without authorization the computers of the company and installed a program to deny authorized users from accessing the servers. The next crime involves a Silicon Valley engineer, Suibin Zhang. Zhang committed computer fraud, stole, and transmitted trade secrets about Maxwell’s switches. The next crime was committed by a network administrator who worked as a penetration tester. Eric McCarthy used a SQL injection attack to attack a sequel database and bypassed authentication. McCarthy accessed applicant records without authorization. The next crime involves Bruce Raisley was convicted of attacking media outlets. Raisley sent malicious code that instructed media outlets to publish stories that mentioned
Raisley. The next crime refers to the stealing of secrets GM trade valued at $40 million. The secrets were related to the hybrid vehicles. Yin Qin and the wife had plans of selling the secrets to Chery automobile, a Chinese manufacture, and a competitor of GM. The next crime is about hacking providers of voice of IP and reselling VOIP services for profits. Edwin Pena and Robert Moore collaborated in transmitting over 10 million minutes of unauthorized telephone calls. Pena reprogrammed the networks to accept voice of IP telephone traffic. The telephone calls were routed to the customers. The next crime involves Google Inc that was planning to stop censoring its search engine in China because someone had tried to hack into Gmail accounts of human right activities.

H.2 RESULTS OF ANALYSIS

We made an autopsy of 41 ICT crime cases (US Justice, 2010) using this framework for adaptive information security system and the Socio-Technical system (Kowalski, 1994). The Socio-Technical system consists of social and technical parts (Kowalski, 1994). The social part consists of culture and structure. Structure refers to the power structure in an organization. People using an information system have culture like ethics, traditions, laws, and other social values. The technical part consists of methods and machines. In an IT system, the social part can include ethical/cultural, legal/contractual, administrative managerial and operational procedural layers. The technical part includes the following layers: mechanical/electronic; hardware; operating system; application data, store, process, and collect information. Every system is required to be in balanced state to be able to reach the goals set for the system. When the methods change in a socio-technical system the machines, culture and structure may have to change to sustain the balance. When a new machine is introduced in a company, it can lead to changes in procedures, ethical, legal, and administrative issues.

Table 45 outlines the ICT crimes (US Justice, 2010). The first column lists the crimes. The second column shows the whether the deterrence measures were present or not. If the deterrence measures are present then the author indicates the strength of the deterrence measures. The third column shows the presence of prevention security measures and the strength of the security measures. The fourth column outlines the detection security measures and their strength. The fifth column shows the response security measures and their strength. The sixth column shows the recovery security measures and their strength. The letter N indicates that the security measures are not present. If the security measures are present then the letter S or W are in the table. Letter S indicates that the strength of the security measures is strong. Letter W indicates that the strength of the security measures is weak.

The seventh column shows the breached security service. A1 stands for availability security service. A2 stands for authorization security service. A3 stands for authentication security service. C stands for confidentiality security service. I stands for Integrity security service. NP stands for non-repudiation security service.

The eighth column shows the measures that were applied in attacking the victim’s computer system – social or technical measures. The ninth column indicates the methods and tools that were used in attacking or compromising the victim’s computer system.

322
<table>
<thead>
<tr>
<th>Crime</th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Breached Security service</th>
<th>Technical or social measures</th>
<th>Methods And tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>selling (ro)botnets</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>AC, AV</td>
<td>Technical and social measures Using govt. servers as botnets keeper of botnet army</td>
</tr>
<tr>
<td>Id theft</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>C, AV, AC, P</td>
<td>Social engineering, diverting salary of others to his accounts</td>
</tr>
<tr>
<td>Attack on business</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>AV, NP</td>
<td>technical DDoS</td>
</tr>
<tr>
<td>Competitors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Social engineering, automation</td>
</tr>
<tr>
<td>ATM fraud in 280 cities</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>W</td>
<td>C, I, AV, AC</td>
<td>Social and technical</td>
</tr>
<tr>
<td>Hacked into a Search engine</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>AC, AU, P</td>
<td>technical Stealing program code by impersonation</td>
</tr>
<tr>
<td>Porno of minors</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>C, A,</td>
<td>Social and technical Recording porno of minors</td>
</tr>
<tr>
<td>Stolen credits Cards numbers</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>AC, P, AU, I</td>
<td>Social and technical Stealing credit card numbers</td>
</tr>
<tr>
<td></td>
<td>Event Description</td>
<td>Indicator</td>
<td>Indicator</td>
<td>Indicator</td>
<td>Indicator</td>
<td>Methodology</td>
<td>Measure</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>8</td>
<td>Multi-million Black Travel agents</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>P, AC, AU, I</td>
<td>Social</td>
</tr>
<tr>
<td>9</td>
<td>DDoS Hospital</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AV, NP</td>
<td>technical measure</td>
</tr>
<tr>
<td>10</td>
<td>Time bombs Silicon valley manager</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AV, AC, AU, I,</td>
<td>Technical</td>
</tr>
<tr>
<td>11</td>
<td>WAN attack</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AC, AU</td>
<td>Technical</td>
</tr>
<tr>
<td>12</td>
<td>DB Presidential Election, loans</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AC, AU, I</td>
<td>Social, and technical measure</td>
</tr>
<tr>
<td>13</td>
<td>eBay DDoS</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AV, AU</td>
<td>Technical</td>
</tr>
<tr>
<td>14</td>
<td>Hacking Private boxes Changed passwords</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AU, AC, I, P</td>
<td>Social and technical measure</td>
</tr>
<tr>
<td>15</td>
<td>Dark market FBI undercover</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AC, AU, I</td>
<td>Social and technical</td>
</tr>
<tr>
<td>16</td>
<td>XBOX 360 Game piracy</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AC, AU, I</td>
<td>Social and technical</td>
</tr>
<tr>
<td>17</td>
<td>$ 70 million</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>AC, AU</td>
<td>Social and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>-------------------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Credit card numbers stolen</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>C, AC, AU, P</td>
</tr>
<tr>
<td>19</td>
<td>Lovespy</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>C, AC, I, AU</td>
</tr>
<tr>
<td>20</td>
<td>Microsoft web attack</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>C, AU, AC</td>
</tr>
<tr>
<td>21</td>
<td>Massive data theft</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>C, AU, I, P</td>
</tr>
<tr>
<td>22</td>
<td>Destroying Financial records</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>W</td>
<td>C, AC, I</td>
</tr>
<tr>
<td>23</td>
<td>Traffic redirecting</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>AC, I, AU</td>
</tr>
<tr>
<td>24</td>
<td>Formulas stolen</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>C, AU, AC</td>
</tr>
<tr>
<td>25</td>
<td>Keystroke wiretapping</td>
<td>N</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>C, AU, AC, P</td>
</tr>
<tr>
<td>26</td>
<td>Accessing Governor’s e-mail</td>
<td>N</td>
<td>W</td>
<td>W</td>
<td>N</td>
<td>N</td>
<td>AU, AC, P</td>
</tr>
<tr>
<td>27</td>
<td>NASA, Defacing govts webs</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>W</td>
<td>AV, AC, I</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Location</td>
<td>Nature</td>
<td>Technique</td>
<td>Social or Technical</td>
<td>Remarks</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------</td>
<td>------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>economic espionage</td>
<td>N W W N N</td>
<td>AC, AU</td>
<td>Social</td>
<td>stealing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Citibank ATM fraud</td>
<td>W W W N N</td>
<td>C, AU, I</td>
<td>Social and technical</td>
<td>Encoding blank ATM cards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Bringing Down WAN</td>
<td>N W N N N</td>
<td>AV, AC, AU</td>
<td>technical</td>
<td>Reprogrammed access points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>E-bay defacing</td>
<td>W W W N N</td>
<td>AU, AC, C</td>
<td>Technical</td>
<td>Flash and PHP script</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Attack on Eddo. dept. supervisors</td>
<td>N W W W N</td>
<td>AC, AU, C</td>
<td>technical</td>
<td>Installed a backdoor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>CariNet</td>
<td>N W W N N</td>
<td>C, AU, I</td>
<td>Social and technical</td>
<td>Changing network configuration, deleting logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Hacking US companies</td>
<td>W W W N N</td>
<td>Social,</td>
<td>botnet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Benimeli – 20%</td>
<td>N W W N N</td>
<td>C, I, AV,</td>
<td>Social and technical</td>
<td>Threatening, dos attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Stealing trade secrets of Maxwell’s switches</td>
<td>N W W N N</td>
<td>AU, AC, I</td>
<td>Social</td>
<td>staged SQL injection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>SQL injection attack</td>
<td>N W W N N</td>
<td>AU, AC, I</td>
<td>SQL injection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Attacking media outlets</td>
<td>N W W N N</td>
<td>AC, AU, I</td>
<td>Releasing a virus</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Socio-Technical system [1] contains the social and technical parts. Criminals appear to use both social, like social engineering, and technical measures to attack information systems as outlined in Table 46. Criminals used social attacking measures in 26.8% of the crimes. In 31.7% of the crime cases criminals used both social and technical attacking measures. The criminals used technical attacking measures in 41.5% of the crime cases as outlined in Table 47.

### Table 45: Social and Technical Security Measures in the ICT Crime Cases

<table>
<thead>
<tr>
<th>Social Measures</th>
<th>Attacking Social Measures</th>
<th>Technical Attacking Measures</th>
<th>Social-technical Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>17</td>
<td>41.5%</td>
<td>31.7%</td>
</tr>
</tbody>
</table>

The author analyzed also the security services that were breached in the crimes. In 9 out of 41 ICT crimes, it was a breach in availability security services. In 17 crime cases, confidentiality service was breached. In 24 cases, authentication security service was breached. In 32 cases, an authorization security service was breached. In 22 cases integrity security service was breached. In two cases, the non-repudiation security service was compromised. Moreover, in 9 crime cases privacy was compromised as shown in Table 47.

### Table 46: Security Services Breached in the ICT Crime Cases

<table>
<thead>
<tr>
<th>Availability</th>
<th>Confidentiality</th>
<th>Authenticity</th>
<th>Authorization</th>
<th>Integrity</th>
<th>Non-repudiation</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>17</td>
<td>24</td>
<td>32</td>
<td>22</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>
We analyzed 41 computer crime cases to see how many systems had deterrence, prevention, detection, response, and recovery measures as outlined in Table 48.

**TABLE 47: VALUE-BASED CHAIN FUNCTIONS IN THE ICT CRIME CASES**

<table>
<thead>
<tr>
<th></th>
<th>Deterrence</th>
<th>Prevention</th>
<th>Detection</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weak</td>
<td>6: 13, 17, 27, 29, 31, 34</td>
<td>39</td>
<td>37</td>
<td>4, 9, 13, 22, 27, 34, 41</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>34</td>
<td>1 (6)</td>
<td>4 (6, 25, 30, 40)</td>
<td>30</td>
<td>34</td>
</tr>
</tbody>
</table>

In addition, we analyze using the socio-technical system the methods and tools that the hackers applied in attacking the information systems. We present the structure or organization of criminals at the end of the analysis. Out of 41 cases, no system that was attacked had strong deterrence measures to scare away attackers. Seven systems had weak deterrence measures, which could not scare away attackers. 34 systems had no deterrence measures, which could not scare away attackers.

34 systems had no deterrence measures. When it comes to prevention measures, 40 systems had weak prevention measures, which could not prevent attackers. One system had no prevention measures at all. 31 systems had no response measures at all, while 10 systems had weak response measures. As to the recovery, systems 34 systems had no recovery measures while 7 had weak recovery measures. 18 of the cases did weak confidentiality measures. In 31 of the cases authentication, security service was not strong. In ten cases availability security service was weak. In 32 cases, access control was not strong enough. 23 cases had breaches in integrity security service. 9 cases had breaches in privacy security service.

**REFERENCES**