Nomadic Computing
- Security assessment of remote access to workplace systems

Johanna Karlsson
This thesis is submitted to the Department of Software Engineering and Computer Science at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author:
Johanna Karlsson
Address:
Västra Vallgatan 37 B
291 31 Kristianstad
Sweden
E-mail:
johanna-k@telia.com

University advisor:
Professor Rune Gustavsson
Department of Software Engineering and Computer Science

Assisting advisor:
Andreas Jacobsson
Department of Software Engineering and Computer Science

Department of
Software Engineering and Computer Science
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Internet : www.bth.se/ipd
Phone : +46 457 38 50 00
Fax : + 46 457 271 25
ABSTRACT

Nomadic computing is about communication on an anytime anywhere basis. Security in this area is today not high enough and at the same time nomadic computing is increasing.

In this thesis, security in the area of nomadic computing and remote access to company systems is assessed. The purpose is to investigate the security in this area today but also in the future in order to answer the main question of how and when secure nomadic computing can be offered.

For this purpose a futuristic scenario has been used as a method to identify challenges within nomadic computing. After looking at the state of the art of wireless communication and security techniques, evaluating the focused techniques and looking at future trends, some preliminary conclusions could be made.

A model of technology uptake has been used. The main concept of the model is to show that the uptake is depending on a co-evolution between different parts and not only the technique.

One conclusion is therefore that the users must have confidence in the technique, but also in the organisation and the organisational use of the technique or else they will not use it. Security is important in order to create this trust and is thus of decisive importance to the technology uptake.

Another conclusion is that the three focused techniques; rule-based access, authentication and policy/contract can be used today, but also in the future to increase the security for remote access.

Finally, education and user awareness seems to be important in the future, even though the users interact less in the security management.

Keywords: Remote Access, Security, Mobile Device, Wireless Communication
ACKNOWLEDGEMENT

First of all I would like to thank my supervisor Professor Rune Gustavsson for his inspiring and creative ideas and for his support during the whole thesis.

Second I also want to thank my assisting supervisor Andreas Jacobsson who helped me with his research thinking and methodology awareness.

Finally I want to thank Jimmie, my family and friends for being supportive and encouraging.
# CONTENTS

ABSTRACT .......................................................................................................................................... I

ACKNOWLEDGEMENT ..................................................................................................................II

CONTENTS ....................................................................................................................................... III

1 INTRODUCTION ................................................................................................................... .... 1
  1.1 GUIDELINES FOR THE READER ............................................................................................... 1
  1.2 INTRODUCTORY SCENARIO .................................................................................................... 1
  1.3 SCENARIO DISCUSSION .......................................................................................................... 2

2 METHOD ..................................................................................................................................... 4
  2.1 INVESTIGATION FOCUS AND PURPOSE ................................................................................... 4
  2.2 METHODOLOGY DISCUSSION ................................................................................................. 4
  2.3 INVESTIGATION MODEL ......................................................................................................... 5
  2.4 STRUCTURE OF INVESTIGATION ............................................................................................. 6

3 CHALLENGES IN NOMADIC COMPUTING ....................................................................... 7
  3.1 CHALLENGES IN NOMADIC COMPUTING DERIVED FROM THE SCENARIO................................ 7
  3.2 ASSESSMENT OF CHALLENGES............................................................................................... 8
  3.3 TECHNICAL FOCUS............................................................................................................... 10

4 STATE OF THE ART OF WIRELESS COMMUNICATION ............................................. 11
  4.1 INTRODUCTION TO WIRELESS COMMUNICATION ................................................................. 11
  4.2 SECURITY THREATS ............................................................................................................. 12
  4.3 SECURITY PROTECTION MECHANISMS ................................................................................. 13

5 EVALUATION OF THE PROPOSED TECHNIQUES ........................................................ 18
  5.1 CONCEPTUAL MODELS OF REMOTE ACCESS ........................................................................ 18
  5.2 ASSESSMENT OF THE TECHNIQUES USED IN TENTATIVE SOLUTIONS................................. 20

6 FUTURE TRENDS FOR NOMADIC COMPUTING AND SECURITY ............................ 23
  6.1 NOMADS .............................................................................................................................. 23
  6.2 SECURITY TODAY ................................................................................................................... 23
  6.3 SECURITY TRENDS............................................................................................................... 23
  6.4 FINAL DISCUSSION OF THE FUTURE SCENARIO PROBLEMS .................................................. 25

7 SUMMARY AND CONCLUSIONS ........................................................................................ 27
  7.1 NOMADIC COMPUTING AND REMOTE ACCESS ................................................................. 27
  7.2 THE TECHNIQUES................................................................................................................. 27
  7.3 CONCLUSIONS ...................................................................................................................... 28

8 REFERENCES..................................................................................................................... ...... 29
  8.1 LITERATURE ........................................................................................................................ 29
  8.2 PROCEEDINGS AND ARTICLES .............................................................................................. 29
  8.3 WHITE PAPERS AND REPORTS .............................................................................................. 30

GLOSSARY ........................................................................................................................................ 31

APPENDIX A.................................................................................................................................. 32
  PENTAGON AREA COMMON INFORMATION TECHNOLOGY (IT) WIRELESS SECURITY POLICY ....... 32
1 INTRODUCTION

1.1 Guidelines for the Reader

The intended readers for this thesis are persons with different interests in social, behavioural, economic or market areas, persons in the companies that provide remote access for their employees and system developers.

The structure of the thesis is based on a scenario that introduces the readers to the subject and sets up the scene for the rest of the thesis. After the scenario the method and the model for the work are described. In the section about challenges in nomadic computing, problems from the scenario are identified and investigated. A decision of the technical focus follows. In chapter 4, the area of wireless computing and security is introduced. After this section, the techniques are analysed and in chapter 6 the future trends for nomadic computing are highlighted. This chapter also contains a discussion where the problems are evaluated. The thesis ends with summary and conclusions.

In order to understand some terms and abbreviations used throughout the work, a glossary can be found in the end of this thesis. Words that are explained in the glossary can be recognised in the text as italic words. Additional words not found in the glossary are instead explained in the current text.

1.2 Introductory Scenario

Peter is sitting on the train on his way home. It has been a long day and he is very tired. He tries to remember the last time he was home, it must have been more than two weeks now. Travelling is a part of his job and he is more often away, than in the office. The last years it has been better, since he can continue his work even if on the move. Suddenly his mobile phone rings and with a sigh he answers. It was from his company telling him that he has to perform a presentation at an international conference tomorrow, since his colleague got ill. At least he doesn’t need to create a new presentation, since he already has one that he used a month ago. Peter uses his mobile device to book a last minute flight ticket to Oslo where the conference is and a hotel room so that he can attend both days. Then he takes up his laptop and modifies his presentation for the conference before he arrives.

The next day at the airport, he gets his tickets pushed to his mobile device and boards the plane. During the flight he goes through his email and reads company information and company news that he retrieved before the takeoff. Arriving to Oslo he goes directly to the conference. The presentation went well and the whole day was actually more interesting than he first expected it to be. During the conference he also decided to meet up with some of the participants later on at the evening in order to eat together with them. After the conference Peter goes to his hotel. He uses his mobile device to find the way, since he has a GPS service that can point out his location and the position of the hotel. Then, it is only to follow the map with direction arrows. Peter goes to his hotel and checks in. The room is quite nice and he lies down on the bed, changes the security level to low on this mobile device and sends a get well card to his colleague.

After a while he gets up, grabs the mobile device as usually and hurries away. He meets the others and they decide to go to a restaurant nearby that matches their search criteria of evening buffet that the search agent on his device finds. The food tastes good and they are talking for a long time. Instead of going to a boring hotel room they
Peter wakes up. He tries to remember the evening and how much he drank, hopefully not too much. He starts to get ready for the second day and then he takes off to the conference. Peter chooses a seat at the back and turns off the sound on his mobile device. He also closes the IR port that was open. Strange, since he usually closes the port after he has been using it. The presentation begins and he tries to listen, but the only thing he can hear is the beating in his own head. The presentation does not seem to be any interesting so he grabs the mobile device again and opens the email program. He reads the new mails but he can not find the budget mail that he received yesterday, why should he have deleted that one he wonders. He changes the security level back to high and his thoughts begin to wander in his head. Finally, a break, Peter grabs a cup of coffee and a sandwich. Then his mobile phone rings. He is told that there has been a trespassing on the company. Someone has accessed their database and probably retrieved a lot of information. Peter tries to remember who borrowed his device, but he can’t remember if it was someone from the conference or someone they met at the pub. He starts to look at his files and finds his password file where he keeps his different passwords and access information to the company. The file was last accessed yesterday. Peter did not access this file during the whole day and he can feel the panic coming. The mobile phone rings again, this time they have found out that the unauthorized access was made from a cellular phone equipped with a temporary cash card that is untraceable and that it was his access information that was used to enter the company system and that his device was in a pub in Oslo the whole evening. Peter’s fear turned out to be true.

1.3 Scenario Discussion

The functionality in the mobile phones is increasing and today it is not only possible to make phone calls but also to use organizers and documents as well as downloaded software programs. Thus the mobile devices approach more and more desktop computers with help from increased processing power and memory, and also with an increased number of functions. [Shn03] This makes mobile devices more sensitive for attacks since they are becoming more private for the users. The more valuable things you have in your house the more you need to protect it from burglary. In the same way it is important to consider the security for the future use of mobile devices.

In the scenario we can follow Peter, a young employee who is on the move much of his time. In order to work he uses his laptop and for the communication he uses his mobile device. Some people predict that we in the future will have many different wireless devices for different tasks. However a common view is also that it should be possible to only use one wireless device for many different things. It is this view that defines Peter’s device that is a cellular phone combined with a handheld computer, which can communicate without wires over both short and long distances.

It is to be able to communicate when and wherever you are that characterizes nomadic computing. For Peter it is important to be able to access company information when needed.

As seen in the scenario it is important with a high level of security when the users have an ability to remotely connect and access the company system with their devices. Otherwise valuable information can get in the wrong hands.
Security is also important as the wireless devices and their users are becoming more and more mobile. [Shn03] Computers are therefore introduced to new places and situations in which the security can suffer.

The connection from wireless devices to the Internet is increasing and security has to be investigated from this aspect as well.

Analysts mean that also privacy will be a great concern in the future for example in the third generation mobile networks (3G) due to the increased possibilities of positioning as one example. [Gar02]

The purpose with the scenario is to show in a simple and quick way what this thesis is about, but also to understand the focus and the delimitations.

The scenario is a futuristic description of possible events. Perhaps it is unlikely for all these things to happen at one time, however even if only one of them occur it is necessary to investigate them in order to see if something can be done to prevent them from happening. There can also be other situations not included in the scenario that can cause problems. However, this scenario covers many different security issues, is relevant to remote communication and gives a good representation of a future reality. Finally, the scenario is focused on concerns that are, according to my own opinion, interesting to highlight.
2 METHOD

2.1 Investigation Focus and Purpose

The focus in this thesis is on the area of nomadic computing and security. The function that is highlighted is remote access to company systems from mobile devices. It is not behavioural or economical changes of nomadic computing that is investigated but the technical aspects and the security. This, since they are the most interesting aspects for the purpose of this thesis. Security is also considered to be the most important factor in order to gain trust among users and to adopt upcoming techniques. Remote access to companies will be more common [Mas99] and therefore it is relevant to investigate the security situation today and in the future. The specific question that is investigated in this thesis is how and when secure nomadic computing can be offered.

The purpose is to give the users an increased understanding of security when accessing company networks. It is also important to identify existing techniques and evaluate them and compare them to future trends. We must be prepared for possible changes in security requirements and other security adjustments that can be needed for nomadic computing in the future. It is especially important to identify possible problems of the future and to see if there is something missing in the security area. This work is thus important both for users and companies.

Previous investigations in the area are mostly concentrated on technical perspectives of the communication, such as standards and protocols. Works that have been written on security are concentrated partly on standard and transmission security in the telecommunication area, partly on security concerns on the Internet. This thesis is concentrated on nomadic computing and security, which involves security in wireless communication and mobile devices. Also new angles of security are highlighted, since nomadic computing is changing the way we live and our behaviour.

2.2 Methodology Discussion

The method used in this thesis is a scenario driven approach, which is in accordance with the paper written by Lyttinen and Yoo [Lyy01]. They state that research methods in the area of nomadic information environments must be changed compared to the traditional way of performing research. This since nomadic information environments is an area that deals with both social and technical elements and there is no given research methodology for this, compare as described in figure 1 page 5. They mean that new tools need to be developed and research in nomadic knowledge need to focus more on environments than applications. Sometimes access to personal knowledge is needed or bodily experiences.

The focus on nomadic computing and remote access security is technical, but can also be said to be behavioural and dependent on contexts as explained in figure 2 page 5. However, in this thesis the focus is on technical aspects, i.e. T in figure 1.

2.2.1 Scenario

In order to investigate the security today and in the future in this area, a scenario is used as a starting point. To use a scenario is a recognized method that is used for
example in a document produced by the AMSD\textsuperscript{1} project funded by the European Commission. [IST03] In this document many different prospective scenarios are presented and used as “tools for ordering ideas and for supporting the consequent analysis”.

In the scenario in this thesis a futuristic nomadic life is presented and used throughout the work as a model of a future reality. In this reality a number of problems are derived and investigated. The scenario therefore forms the ground for the whole thesis and is continuously referred to in different situations.

### 2.3 Investigation Model

#### 2.3.1 Model of Technology Uptake

In this thesis a model is used when looking at the uptake of the technology. A technological uptake is not only depending on the technique but also on other influencing parts. When the technology is developed for the users also the users and the organisations have an influence. This forms a co-evolution between the technique, the organisation and the persons.

![Figure 1: General model of the co-evolution between Techniques, Organizations, Persons (users) for a technology uptake.](image)

In this triangle of effecting parts there are driving forces of different factors that spin round. Generally all factors must exist since they all have a decisive importance to the uptake, see figure 2.

#### 2.3.2 Model of Technology Uptake in this Thesis

The model is used in this work as a way to look on the uptake of nomadic computing, which is done from a technical point of view. When the technology is brought to the user, the uptake is depending on the users and if the users have trust in it. In the same way the users must be able to trust that the organisation is using the technique in the right way.

![Figure 2: Thesis model of the uptake that is influenced by the driving forces spinning inside, for example that the users have confidence in the technique and the organisation.](image)

\textsuperscript{1} AMSD is short for Accompanying Measure System Dependability
By using a scenario as a method we can find examples of driving factors. Except trust, there must also be a need and it must be financially possible.

1. Trust
From security you can gain trust [Sig01], which also can be seen in the scenario. By looking at in what extent Peter uses nomadic computing we can see that he probably trusts the security or else he would not have been using his device as much.

2. Need
The need for nomadic computing can be seen in the scenario where it is used in many different contexts and for many different things. Peter communicates, navigates and works with help from his mobile device and wireless communication.

3. Economy
In order for organisations to be able to develop something they have to have economical means, it must be financially possible for the organisation to provide remote access to their system and to support and supply their employees with fully equipped devices, there must be companies that develop services for nomadic computing and so on. Also the users have to be prepared to pay for the techniques and services that are introduced, thus the prices have to be at a reasonable level for the users.

The economical factors are not included in this work, but are not less important. All the three factors are of vital importance to the evolution of nomadic computing and if nomadic computing is going to be used in the future.

2.4 Structure of Investigation

\[ \text{Scenario} \rightarrow \text{Problem types} \rightarrow \text{Technical solutions} \]

- Today
- Upcoming
- Research

Figure 3: Plan of the structure, starting with the scenario, problem types and technical solutions.

With this figure the structure of the investigation is outlined. The scenario is the starting point from where the problem types are derived. From this point the technical solutions are investigated by looking at the existing techniques today. Finally the future trends are highlighted for possible upcoming techniques.

With this structure the goal is to be able to reach certain conclusions concerning future problems and how and when secure nomadic computing can be offered. The conclusions must however be considered to be preliminary since we never can know for sure how the future will be like.
3 CHALLENGES IN NOMADIC COMPUTING

3.1 Challenges in Nomadic Computing derived from the Scenario

3.1.1 Possibilities with Nomadic Computing

As seen in the scenario the nomadic life implies new possibilities as well as new problems. Besides the possibility to work even if not at the office there are also other situations with upcoming possibilities. In the scenario there were examples when Peter booked a flight ticket and a hotel room and it is not unlikely that it in the near future also will be possible to have the tickets pushed directly to the mobile device. Peter also used the global positioning system (GPS) that makes it possible to point out locations of users and places. Another example is search agents that can retrieve information that suits the users’ criteria, while the user is on the move.

3.1.2 Problems with Nomadic Computing

There are also some problems that should be addressed. In order to give the users remote access to companies the security level has to be as high as possible. In the scenario it is possible for the user to self adjust the security level on the device. This functionality does not exist today, but can be good if handled in the right way. However it may not always be clear to the user what level to choose for different situations. It is reasonable to think that different situations need different security levels, so the problem is how to handle the security in the right way and to reach a high level of security for remote access to companies.

Another issue to discuss is that many users tend to bring their mobile devices with them almost all the time, which introduces computers to new places and new situations. The problem is that the users might not be aware of potential threats that might arise. In the scenario Peter brings his device to the pub without taking any precautions, instead he changes the security level to low and forgets to change it back. He does not even reflect over what can happen or even what he self might do after a few drinks.

However there are also many situations that the users can not predict, like theft for example. This problem involves how to keep a high security level even though the devices are in hands of unauthorized users. In the scenario Peter lends his mobile device to an unknown person. Also in this situation the problem is how to feel safe even though he don’t know the person.

There is always a problem with so called hidden affordances. This term means that a function might be used in a way that it was not intended to. The IR port is in the scenario used by an impostor for short range transmission of small files to another device. The information in the files is retrieved with the purpose of accessing the company system in a later attack. The problem is how Peter could have foreseen that the port was to be used for this purpose and been prepared. This is also a problem of how to prevent access to mobile devices from unauthorized users.

The next problem deals with responsibility. In the scenario we can see that it is with help from Peter and his device that the intruder can gain access to the company database. Therefore it is possible that Peter is the one who is to be blamed for the trespass, even though he would probably not have noticed anything if they hadn’t told...
him. The problem is that when it comes to company access also the company itself should have a certain responsibility.

One of the possibilities presented earlier was about so called search agents. These agents can save time for the users and find exactly the information needed at a certain moment. However on the Internet today it is common to gather different kinds of information about the users in order to process it with profitable purposes. This is only one of many situations in which the integrity of the users might be violated. Another example with the wireless technique is the new possibilities of positioning, which can also be used in ways that violates the integrity. The last problem is therefore about the integrity being threatened. In the scenario Peter has his private time, but his integrity suffers when the company finds out his location after working hour. The problem is how to guarantee that GPS is not used for the purpose like the one in the case.

3.1.3 Challenges Summarized

The discussed problems are summarized in six points. These points are going to be examined as an essential part of the way to answer the main question of how and when secure nomadic computing can be offered.

1. Peter changes the security level
   It is a problem to let the user have all the control of the security level, especially when communicating with the remote company.

2. Peter brings his device to the pub
   The user should be aware of possible threats due to new situations and places.

3. Peter lends his mobile device to an unknown person
   The problem is how to maintain a high level of security even though the wireless device is not in the right hands.

4. Peter discovers that the IR port is open
   This problem involves how to prevent unauthorized access to wireless devices and be prepared for hidden affordances.

5. Peter is responsible without knowing it
   Both the user and the company have a responsibility and the problem is how to manage the security issues from both sides of the communication and also the responsibility.

6. Peter can not hide where he was on his private time
   The last problem area is that Peter’s integrity is threatened.

These problems are already known today or are reasonable problems that can occur in the near future. Even if not all of them will happen, it is still important to see if something can be done in order to prevent them. The next step is to find out the characteristics of the identified problem and discuss how to deal with them.

3.2 Assessment of Challenges

The identified problems above are all of different kinds. They will now be further investigated one by one to see what can be done in order to deal with them.
1. Security Levels

The first problem is about the security level settings. The new functionality of users being able to choose the security level must be managed in the right way. The users might not always know what security level that is needed in a certain situation or for a certain task. This can be a question of education, but the most common way to deal with these kinds of questions is to use policies that define the rules for the users.

A technical way could be to automatically adjust the security level at the remote company. This can be done in terms of access permissions. The user can choose a high level of security and then access critical information. If the user chooses a low level of security, the access to information at the company will be limited.

Policies are something that is common and often used in different situations today. However in order to automatically adjust the security level at the remote company a communication protocol is needed where the access permissions are decided for each session.

2. New Situations and Places

As seen nomadic computing is not only about technology but also about changes in the user’s life and their behaviour. The users might not be aware of these changes and therefore it might not always be good that the control is entirely managed by the users. The security level can also be managed by the company. To use GPS can be seen as a threat to the users’ privacy, however used in the right way with the right purpose it can be a help to manage the security level and instead protect the employees. With GPS the position of the user is known and can be evaluated in order to decide the right security level. The company can also provide the connection at the company side with a firewall that monitors the traffic and use this information for the same purpose. Company information concerning the users’ job specifications can also be used and much more.

This problem about changes in situations and places can also be said to be behavioural, instead of technical. Then, in order to increase the security the users need to be educated and learn how to best preserve the security in different situations.

3. Device Security

The third point is dealing with device security. The mobile devices are small and always a target for theft. It should not be possible for unauthorized persons to change the security level with the purpose of retrieving company information. So if the user chooses a higher level of security there must be precautions in terms of user identification. With help from the upcoming devices that combines telephones, in-built cameras and touch-screens there are many possibilities of authentication. These devices make it more easy to use eyes scanning, voice recognition or finger prints than an ordinary computer. This kind of authentication can therefore with advantage be used for different situations like changing the security level on the device.

4. Hidden Affordances

Authentication like this can also be used for the problem with hidden affordances. Opening a port on the device for access is also a security risk. If the device is not in the right hands it can not be possible to open and use IR-ports or Bluetooth transmission.

5. Responsibility

The problem with responsibility is another type of problem, which is about organizational management and social contracts with the employees. If the users follow the company policy and manage their device as they should, then the company has to take the responsibility if something happens. There can for example be a contract similar to an insurance that says that the users are not responsible if they have followed the rules. Like in every office at every company it is not the individual but
the company that is responsible for accidents. The idea of a contract would solve many problems of insecurity and control and is advantageous for both the users and the company.

6. User Integrity
The last problem is how to guarantee that the company follows integrity issues concerning their employees. This issue must be dealt with in the company policy for remote access or in a contract that is established between the company and the employee. Also laws can be needed in this question to protect the integrity of the users.

3.3 Technical Focus

The issues that were previously identified to deal with the problems can be summarized into five points, namely rule-based access, education, authentication, policy/contract and laws. These points will be listed and matched with the problems in order to see if they cover them or if they can deal with more than one of the problems.

<table>
<thead>
<tr>
<th>Scenario problems</th>
<th>Tentative solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Peter changes the security level</td>
<td>A. Rule-based access</td>
</tr>
<tr>
<td>2. Peter brings his device to the pub</td>
<td>B. Education</td>
</tr>
<tr>
<td>3. Peter lends his mobile device to an unknown person</td>
<td>C. Authentication</td>
</tr>
<tr>
<td>4. Peter discovers that the IR port is open</td>
<td>D. Policy/Contract</td>
</tr>
<tr>
<td>5. Peter is the responsible</td>
<td>F. Laws</td>
</tr>
<tr>
<td>6. Peter cannot hide where he was on his private time</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 4: A mapping between identified problems and tentative solutions*

As seen in the figure rule-based access can be used to deal with both the first and the second problem, since the security level can not only be decided by the user but also by the company. Authentication can be used for the third and the fourth problem. Policies or contracts can be used to manage the last two problems as well as the first two. Education (B) and laws (F) are redundant and will not be focused in the actual research of the thesis. By using Rule-based access, authentication and policy/contract, all the six problems can be managed. Education and laws are therefore not necessary.

Rule-based access, authentication and policy/contract are all technical points that are relevant and interesting to highlight in the investigation. Therefore the concentration in this thesis will be on evaluating these techniques and assess them to the area of nomadic computing and security.

The next step contains an introduction to the area of wireless computing and security, which includes an investigation of the state of the art of the focused techniques that can be used to manage the problems.
STATE OF THE ART OF WIRELESS COMMUNICATION

4.1 Introduction to Wireless Communication

4.1.1 Wireless Communication Standards

In the scenario Peter is using wireless communication in order to connect to the company and continue his work even if he is away. This possibility also exists today even if it is not a common occurrence yet. Today it is most common to use WAP and GPRS when accessing the Internet and company intranets. However UMTS will probably be the dominating standard when released due to the higher speed. [Nor01] High speed is a necessity, since wireless access to Internet is becoming more common and the data rates are compared to the data rates in wired networks that the users are accustomed to. If the speed is not high enough in wireless communication, no one will use it. [Fen01]

The goal with wireless communication today is to have a continuous connection even if the users move around between networks. The advantage is that we do not need to pay for the time that we are connected, but instead for the amount of information that is sent. [Lin01a] The established session has to be maintained without interruptions, which is essential also when connecting to company systems. [Nor01] GPRS is a packet switched standard that allows IP traffic directly to the mobile terminal. This means that with GPRS it is possible to have a continuous connection. [Sig01] The protocol used is Mobile IP which is an extension of IP and used for the purpose of supporting physical migration of computers between networks. [Mil99]

4.1.2 Wireless Local Area Networks

Another wireless technology that is growing fast is Wireless Local Area Network (WLAN), which is based on the IEEE 802.11 standards. These standards support applications that are using higher data rates and wireless station addressing for example. Instead of a wired LAN, it is possible to connect computers and components to a WLAN access point, which in turn communicates and connects to a wired Ethernet network. WLAN provides a more flexible and portable solution than wired LAN. In the scenario there could have been a WLAN at the airport or at the conference building. Peter could have accessed the WLAN and used its services, for example received his tickets or accessed information or even the Internet. Peter could also have accessed the company network, since WLAN in turn can communicate with other networks. [NIST]

Another type of WLAN is Bluetooth, which is a radio technology that also enables wireless data connections between devices or components. The Bluetooth connection has the purpose of being used over short distances. [Coy01]

In the scenario the person who borrowed the mobile device from Peter also used another kind of short distance communication, namely Infrared (IR) transfer. IR can be used to transfer data or programs from one mobile device to another. It was with this technique that the person in the scenario could get hold of the connection information concerning the company and then use it later for the intrusion. [Coy01]
4.1.3 Third Generation Mobile Networks
As seen there are many possibilities that can be used to achieve wireless communication, but in order to give the users access to the full content on the web, better range is needed. The upcoming third generation (3G) technologies, like UMTS for example, will enable a high speed, always-on connection with high coverage. Users can travel around the world and maintain a high bandwidth access since it does not matter if networks are based on different underlying 3G interfaces. [Coy01]

4.2 Security Threats
Any sorts of data networks can be target for different attacks that pose a threat to the security. For example, there are people who want to steal money or information and there are competitors, unhappy customers, former employees or criminals who want to damage the company system. [Nor01] The focus in the scenario is mostly concentrated on the users’ devices and the connection to remote companies, but not so much on the actual transmission.

4.2.1 Wireless Communication
Wireless data communication is in many ways more exposed than communication over wires. The communication media is open and could be intercepted by anyone with the right equipment. There is also a lack of trust among users towards wireless networks since there are problems like jamming, radio shadows and lower bandwidth. [Sig01] The fact that the data in wireless communication is broadcasted through the air poses a security threat since it is hard to control that the data is only available to intended users. [NIST]

4.2.2 The Mobile Device
A threat to mobile devices is, as mentioned before, that they are more exposed to theft due to the portability. This involves a high need for protection for unauthorized use of the device. [Sig01] The person in the scenario did not steal the device, but he tricked Peter that he should do something else than his real malicious intention. In this way he could easily get hold of the access information without being exposed. Independent of the situation, the device must be protected, for example with authentication, so that lending it would not pose a threat. The attack might involve stealing passwords like in the scenario in order to prepare for a later attack against the company system.

As the devices are becoming more and more powerful and have access to the Internet, they are as vulnerable as a stationary PC with access to the Internet and can be target for different attacks like virus attacks. Viruses can come from an e-mail, downloaded software, from the synchronization with the PC or from the IR transfer. [Coy01]

Since many new devices have GPS capabilities, the location of users can be seen independently of where they are in the world. This possibility poses a threat to the users’ integrity that should not be ignored. [NIST]

4.2.3 The Network
Except the device there are also other threats that could affect the user. The target can also be different components in the network like routers, switches, and servers. [Nor01] Security problems can arise when data systems or other terminals connect to the wireless data communication. [Sig01]
One type of attack is the Denial of service (DOS). It is when the resources are disabled and prevents the network or application to operate correctly. [Nor01] Distributed denial of service (DDOS) is an attack on multiple resources or locations on the Internet that is disabled [Duk02], or an attack from multiple machines. The owners of the machines might not be aware of that an attack has been launched from their computer. This is possible through an earlier software attack on those machines. It is thus more difficult to trace the origin of the attacker in DDOS and also to prevent these attacks. [Kar03a]

There can also be a loss of privacy and data integrity if there is an attack against data that is transmitted, for example when important company information is tapped or modified.

The attack called masquerade involves pretending to be a legitimate host in order to trick the remote users. In the scenario it was the company that was tricked by a person pretending to be a legitimate user which is a threat to the company. [Nor01]

4.3 Security Protection Mechanisms

As mentioned before security is important in wireless communication in order to gain trust from the users. According to investigations made, there are a majority of users with a lack of trust towards mobile connections, since they don’t think that they are secure enough. If the users do not trust the communication they will not use it. The security must be adjusted to the users and the usage. At the same time the security becomes worthless if the users can not understand it and use it in the right way. It should be possible to use a mobile device for transactions and authentications and other unauthorized persons should not be able to use the device if it is lost or lent as in the scenario. [Sig01]

The best way to reach a high security is to operate at a number of levels. The layers referred to are the seven protocol layers in the OSI Reference Model, defined by ISO². [Nor01]

4.3.1 Security Policy

Security policies are a very good ground. An example of a security policy can be found in appendix A. It is the Pentagon Area Common Information Technology (IT) Wireless Security Policy that is used with the purpose of demonstrating how a policy could look like.

In the policies it can be defined what needs protection and how the protection should be provided for example. [Nor01] The policy should include approved users, the type of information they are allowed to store, what programs they are allowed to install, how to store the device and associated modules when they are not used, how to select and use a password, how to report a lost or stolen device and disciplinary actions that may result from misuse. [NIST] The important factor with policies is to ensure that they are operated correctly.

One example when it is important to create a security policy is when a WLAN is setup. The network assets have to be identified in the policy as well as who has access to the WLAN. It must also be defined what is allowed to be accessed when and where. [Nex02] It is often good to use a security model to set up security policies and its significant entities and rules. The models can be concentrated on different security issues like confidentiality and integrity, and they can be applied to policies that are both for static or dynamic environments. [Gol99]

² ISO is short for International Organization for Standardization.
The next step is to implement security techniques at different levels in the communication. Several layers of protection are considerably more difficult to get past for a hacker. [Nor01] When talking about security, the terms confidentiality, integrity and authentication are often used.

4.3.2 Confidentiality

Confidentiality is about ensuring that data is protected from loss of privacy. This can be done with the use of encryption. [Nor01]

Encryption

Encryption is used in order to ensure the privacy of transmitted data across public networks. Different algorithms are used for this purpose together with secret keys. The keys define the rules for the encryption algorithm and therefore it is also important to protect the keys. End to end encryption is hard to accomplish, but it is desirable to have encryption in the end system hosts and terminals as well as in transit. [Nor01] Many wireless systems have a limited performance and bandwidth, and the process of encrypting data is severe, which leads to a difficult balancing between what is technically possible and the level of security. For wireless applications this means that cryptography has to have special solutions. Hardware encryption is not very flexible, but quick and uses low processor power and effect. If software encryption is used, the algorithm has to be made less complex and the size of the encryption keys might need to be limited. [Sig01]

One way to encrypt the traffic in WLAN is to use WEP, in which the cryptography is done in the physical link layer and the data link layer (layer 1 and 2). However, if using WEP, the traffic is not encrypted the whole way if communicating over different networks. In order to keep the cryptography also between nodes and networks the cryptography should be at network layer (layer 3) instead. This technique is therefore not often used within the same LAN, but rather to establish a secure connection between two LANs. In order to have a high security level the whole way between applications, there should also be cryptography in the transport level (level 4). Often the protected transmission of websites, HTTPS, is encrypted at this level. In the transport layer encryption techniques like SSL, TLS, and WTLS are common. [Sig01]

Virtual Private Network

A Virtual Private Network (VPN) is a technology that uses encryption to create a private connection over the public Internet. [Coy01] By sharing the public network infrastructure, a virtual private network is created between the organization’s network and the mobile device. The access to this private network is secured and only the authorized users can gain access. A VPN is often used when the employees want to access company information with their mobile device, for example in the scenario with the use of the right equipment Peter could have accessed a WLAN and then used VPN to access the company network. [NIST] One goal for the future is the ability for all networks to be bound together and thereby provide a possibility to seamlessly roam between networks with the use of a wireless VPN. In order not to lose information the session has to be maintained and secure even though the users roam between networks. This is not done at the transport layer but instead at the session layer where you are no longer dependent of the IP address. [Sig01]

4.3.3 Integrity

Integrity is in this context about protecting the data against modification. This can be done at the application layer by adding software using electronic signatures in order to secure messages. [Nor01] Electronic signatures can be used to guarantee the content
but also the identity of the sender. The techniques used are hashing for the integrity and private keys to decide the identity. An important part when dealing with public and private keys is the management, since it is crucial for the security that the keys are managed in the right way. One way to store the secret private key is to use smart cards. A smart card can contain own memory and processing power and for example be a chip in a cellular phone. [Coy01] Smart cards can for example be used together with username or passwords or in combination with biometrics. [NIST]

The implementation of integrity protection can also be done at different levels. Error discovering and error correction coding can be used at the lowest layers and packets at the higher levels can use checksums and sequence numbering. [Sig01] It is common to have session-oriented applications, which means that the user system sets up a session binding with the host system. Thus the integrity of the sessions has to be guaranteed, so that the original user is not cut off in the middle of a session. This can also be accomplished by using message sequence numbering, but also by other checks, such as periodic status polling. [Nor01] The general idea behind these integrity protection techniques is to find out if there have been any changes in the files that violate the integrity of the data. If checksums are used, as one example, the files are compared, before and after transmission, to discover changes in the checksum. [Gol99]

4.3.4 Authentication

The process that identifies an individual or a unit, for example a terminal, is called authentication. [Sig01] You can also say that authentication is about protecting against direct attacks by ensuring that the users are who they say they are. There can also be a protection against masquerade by testing that the host systems are genuine. At the application layer users will be required to log on to operating systems and applications. Often are user names and passwords used for this purpose. In order to improve the security further there should for example be rules regarding password length, design and lifetime, since this makes the passwords more difficult for the attacker to crack. [Nor01]

It is important to be able to identify individuals especially for access to public networks like GSM or private networks like WLAN. Authentication must be used and is accomplished by passwords, hardware and biometrical techniques. This includes something that the user knows, the password, something that the user has, the hardware, and something that the user is, namely biometrics. Together they provide an even higher level of security. Example of a password for authentication could be the PIN-code, example of hardware can be the SIM card and finally a biometrical example could be voice recognition or fingerprints. [Sig01] The interfaces on mobile devices have changed due to new technologies like touch screens, inbuilt cameras, handwriting recognition and voice recognition which make biometric methods possible to use. [Nor01] Today fingerprint readers exist that can be attached to the mobile device through a serial or USB port. The reader can for example block the whole device, a specific application or a connection to a remote database. Handwriting recognition, as another example, measures the shapes of the signatures, but also aspects that are more difficult to copy, like rhythm and timing. [NIST] In addition to these three authentication methods also GPS can be used to check where the user is in order to take this into count for the login. [Gol99]

4.3.5 Global Positioning System

GPS is a system used for geographic orientation. With a number of satellites, the GPS equipment can decide a specific position. GPS and positioning is often used in different services in order to gather geographical information, used for advertising related to locations, or many other things like the examples in the case. [Lin01a]
4.3.6 Firewall

Firewalls are common security mechanisms. Networks that are connected to the Internet are most commonly associated with firewalls. This kind of protection might also be needed for a special part within an organization. A firewall is a protection mechanism which contains access lists which defines what traffic that is permitted and not. Often only traffic from predefined locations is permitted to pass through. If the traffic comes from an unknown mobile host it should be rejected and denied access to the company system. In the scenario only traffic from Peter’s device should have been allowed and not from the unauthorized person’s device. Some firewalls are more sophisticated and works at higher layers in the communication stack. [Nor01] A firewall should be used by the remote company in order to monitor all the traffic from remote users. Also mobile devices are beginning to support firewalls. [NIST]

4.3.7 Antivirus Software

Another important security mechanism is antivirus software that now also can be downloaded from the Internet and used on mobile devices and not only on stationary computers. These applications should be able to scan e-mail and data files and remove malicious code from files when transmitted to the device. The ports shall also be scanned since data is imported to the device through these ports. [NIST]

4.3.8 File Protection on the device

Files that are important like password files should be encrypted and some mobile devices allow users to mark certain records as “private” and hide them. This makes the files hidden to a malicious user and in order to see them again a password must be entered. [NIST] If Peter had used these methods in order to protect his important file in the scenario, the impostor had not have retrieved the information as easy as he did.

4.3.9 Access Control

Another important part in security over networks is access control. Entities or resources like host systems or applications need to have a controlled access in order to prevent security damage. [Sta00] In other words only those who are authorized to access a restricted system should gain access. [Yua01] Often security policies are used to define who has access to which resources in the systems. [And01] It is not only persons but for example also processes or machines that have to be identified or authenticated to receive access rights. [Sta00] The access rights can imply which files that can be read, which programs can be executed and so on. Access control mechanisms can also be used at different levels in a system, in applications down to hardware. For smart cards as one example or other hardware devices it is important to have a controlled access.

When it comes to organizations, access permissions can be formed into groups or functional roles. [And01] Groups or roles are used to simplify the definition of access control policies. Users with similar access rights are collected into groups and access to objects are then given to the group, instead of to each user. Roles are more depending on the jobs or operations that the users perform, and the employees receive their access rights accordingly. [Gol99] If the user successfully logs on to a specific host system this might not always be sufficient. If a company system keeps data that are sensitive in databases, also the access to the database has to be managed. This is important if the users only should have access to certain records in the database. In those cases it is not only the user’s identity, but also what parts of the data that are accessed and previously accessed data, that is checked. All this information can be stored in a user profile that is associated with the user. [Sta00] A common way to
manage access rights is to use *ACL*, which could simplify the storing of the access control matrixes. However there are also disadvantages with this form of management for example in situations when the users are frequently changing. [And01] It can also be difficult the get an overview of permissions given to a user, since a wide search has to be made that covers all ACLs. [Gol99]

Access control can not prevent authorized users form intentional misuse of resources. [Yua01]
5 EVALUATION OF THE PROPOSED TECHNIQUES

The tentative solutions rule-based access, authentication and policy/contract, see figure 4 page 10, are here evaluated.

5.1 Conceptual Models of Remote Access

In order to evaluate the proposed techniques two of the problems derived from the scenario have been used, namely the first two that concerns the new security level function.

Hypothetically both the user and the company can initiate a change of the security level. In the first conceptual model it is the user that wants to change the security level, i.e. problem number one. In the second model it is the company that wants to adjust the security level, i.e. problem number two.

In both examples it is the communication between the user and the company that is focused, i.e. P and O in figure 2 page 5.

5.1.1 Initiation made by the User

First the initiation is taken by the user and in this conceptual model it is investigated if the two techniques rule-based access and policy/contract can be used as mapped in figure 4.

![Diagram of Conceptual model of a security level change initiated by the user.](image)

*Figure 5: Conceptual model of a security level change initiated by the user. The company checks the identification of the user and the user’s access rules together with other processed info, before the security level and access rights are decided and shared to the user.*
In the case the user wants to set the security level, he or she must first be authenticated on the device. Then a request is sent to the company that automatically checks the user’s identification and access rules, namely if the changed rules are needed in order to perform job instructions. Also other available information is processed before the security level is decided and the access regulated. The user is notified if the security level is changed or not. During the whole session, the user can access information allowed by the security level.

In this example the policies, i.e. D in figure 4, forms the ground on which the user makes a decision to change the security level. Access rules, i.e. A in figure 4, are used to evaluate the request and decide the security level for the user.

Since the user expects the company to automatically handle the request and evaluate it, this shows that also the company must take responsibility in the co-evolution. As described in figure 2 page 5, the user must trust the company and that the company is responding in the right way.

5.1.2 Initiation made by the Company

A security level change can also be initiated by the company, which can be good when nomadic computing is introduced to new places and situations, i.e. problem number two.

In the scenario Peter went to the pub without changing the security level. This is a situation in which the security level change might be initiated from the company side. The company can process significant information and with this information assist the user and maintain a high level of security.

Another reason for the company to change the security level can be that the user is not involved in any project at the moment and do not need access to as much information as before.

The purpose is however to maintain a high level of security and make it easier for the users to manage the security level. The users are assisted by the company in the decision of security level instead of having all the responsibility of the communication. The company must however follow the privacy policy in order not to violate the integrity of the users.

Here is one example where the company initiate a change in the security level for the access.

![Conceptual model of a security level change initiated by the company.](image)

*Figure 6: Conceptual model of a security level change initiated by the company. The company gathers information in order to decide appropriate security level and access rules. When the sec level for the user is changed, the user is notified and a message is sent back to the company as a confirmation.*
In this example the company gathers information from the firewall that monitors all traffic, but also from user whereabouts and from company information concerning the user. Also other information can be useful like the time of the day. The user decides what information that can be used. Then all this information is processed in order to decide appropriate security level and access rules. If the security level must be changed, the user is notified. When the change is carried out a message is sent back to the company as a confirmation.

A policy or a contract, i.e. D in figure 4 page 10, is used in this model to define what information that is allowed to be processed in order not to violate the integrity of the users. The access rules, i.e. A in figure 4, are decided from this information, which can initiate a change of the security level. Even if the users do not interact when the security level is decided, they should be aware of the process. Education, i.e. B in figure 4, is thus important in order for the users to understand that the security level is changed.

The co-evolution between the organisation and the user can be seen also in the second example. The user must trust the company and that the security level is handled in the right way. Therefore also this situation is an example of how O and P, in figure 2 page 5, have an influence on the technology uptake.

5.1.3 Discussion of the conceptual models

The two examples deals only with the first two problems derived from the scenario. Also the other problems can be evaluated in the same way. However through these conceptual models we can see that the techniques can be very useful. Also authentication, i.e. C in figure 4, can be used in both examples as a part of the rule-based access.

One interesting observation is that the relation between the organisation O and the user P, see figure 2, is probable to be very important for the uptake of nomadic computing. The users are using the technology through the organisation.

5.2 Assessment of the Techniques used in Tentative Solutions

The three techniques, rule-based access, authentication and policy/contract are know further evaluated. References to the scenario and the conceptual models in figure 5 and figure 6 are also included for this purpose.

5.2.1 Rule-Based Access

In order to control the access to the company, the company must set up access rules. These rules must ignore mobile users that are not authorized, as the intruder in the scenario, and also decide what security level to choose for each access request. Authentication is needed for this part of the communication as well as other available information concerning the user, see figure 5 and 6. Other information that should be evaluated is what the user wants to access, the purpose of the access, what assignments the employees have, together with what is needed in order to perform their tasks. It can also be interesting to evaluate the time of the access, since it is not likely that the employee, e.g. Peter in the scenario, is working in the middle of the night. The position of the device can also be used to compare to travel appointments. A problem is to make sure that the privacy policy is not violated. It must be the users that decide what information that can be used. Peter could have permitted the company to use GPS to find out his location during the day, but not after working hour.
Economically this technique is fairly easy and cheap to implement and provides a high level of security. However it has to be maintained and updated on a regular basis, which can be a complicated procedure. Rule-based access can be used for many different purposes and in many different situations. Not only for access to companies, but also for access control to resources and specific services, e.g. when accessing a WLAN or an airport check-in service in the scenario.

As described in section 4.3.9, there are also other methods that can be used for the same purpose, like role-based access. However rule-based access is a good way for a company to manage a wide number of accessing users, all with a variety of adjusted rules for access permissions.

For the user it is convenient to automatically receive access permissions when accessing the company network, compare as described in the conceptual models of remote access. Especially if the company conform only to the information, agreed by the user.

5.2.2 Authentication

When accessing the company system, authentication is vital for many situations. First authentication can be used if the user wants to change the security level, see figure 5. In order to prevent unauthorized use and access to the device, authentication is also needed before opening a port or initiating a Bluetooth transmission. One upcoming possibility is to use a fingerprint reader that can be attached to the device and used for the different situations where authentication is needed. When and for what authentication is needed, should be regulated in the policy for remote access. In the policy there can also be information concerning the storage of access information and passwords used for authentication. As seen in the scenario, the company should not allow the user to store this important information on the device, at least not unencrypted and unhidden.

The question is not if authentication is needed, but what kind of authentication technique to use. The decision of authentication methods is likely to depend on economical factors besides the level of protection. There are many possibilities to choose from even though biometrical authentication methods are considered to be the most expensive, but at the same time the ones that provide the highest security level. Biometrical methods are known to be difficult when used, due to problems finding the level where all unauthorized users are rejected and all authorized users are verified and not the other way around. Another example of a commonly used authentication method is to use usernames and passwords. It is often difficult for the user to remember and use these in the right way, hidden from others, which also could be seen in the scenario.

A potential problem for the future use of authentication can be cultural differences and acceptance. There is a possibility that fingerprint verification as one example is not an accepted method in certain cultural environments. Unpredicted things like this should not be forgotten. It might be easy to deploy different authentication methods, but then the users might not want to use them.

5.2.3 Policy/Contract

When it comes to security policies, remote access is just one of many contexts in which they can be used. As we could see in the conceptual models, figure 5 and 6, a policy can be used for many different purposes and for many different situations. They must however be formed and adjusted to each company and their needs. The company may need many different policies, for example one concerning the remote access in general, one to support the users when changing security levels and one privacy policy. The privacy policy can point out what the company is allowed to do and what
information concerning the users that the company is allowed to access, without violating the users’ integrity, as described in figure 6. One disadvantage with policies is that someone has to make sure that they are operated correctly. This is the weakness of policies, even if the company or the users want to follow the policies, they might not always succeed. The consequences might be severe.

Contracts are something that does not exist today, but can be a good complement to policies. The purpose is to increase the responsibility of both parts and thus also increase the security level. The company has to increase their security precautions and provide security means for the remote access and the users have to take their responsibility and use the techniques in the right way. Also the integrity can be regulated in the contract, which should push the company to take responsibility also in this area. The purpose with the contract is also to make the company responsible if something happens, like in the scenario. The condition is that the user has followed the rules in the contract. The idea is to create mutual satisfaction from both the user and the company.

Both policies and contracts can easily be adopted and almost does not cost the company anything. The security level can be higher if they are followed. For the company it is important to follow policies in order to reach a better reputation. However for the employees it can be easier to forget or ignore some points in a policy. With a contract everyone must take the security more seriously.

5.2.4 Additional Techniques

Except these three techniques there are also many other mechanisms that can be used to reach a high security level for the remote access. As mentioned, firewalls are good for the purpose of monitoring the traffic, as in figure 6, and to regulate what traffic that is allowed to pass through. Communication information can also be gathered to decide the security level for the access.

Another good tool for companies is to use VPN for the actual transmission and have a secured tunnel as long way as possible between the end nodes. If possible the company should provide all its employees and their devices with VPN software.

Together with all these different techniques, the important issue of handling them in the right way remains. The user must understand and be able to use the security mechanisms in the right way or else the security protection will fail. Education is therefore of great importance in all areas. Even if there are mechanisms that can decrease the interaction of users, they are still the ones that handle the device and should be aware of possible threats.
6  FUTURE TRENDS FOR NOMADIC COMPUTING AND SECURITY

6.1 Nomads

Peter in the scenario is a good example of how a future nomad can come to live, since nomads are defined for the future as itinerant people that use mobile techniques. [Lin01b]

Nomadic computing is increasing and the way people live is changing due to new patterns in life, this according to an article about people going back to be nomads again. It is a technologic and social change in which the mobile networks and wireless local networks makes it possible to live differently from today, more like nomads. The time might not be divided in working hour and spare time like today, but involves new possibilities and challenges. [Kar03b] As a nomad the employees and other users can, regardless of geographic location, access information, network resources and the Internet. [Bro01]

6.2 Security Today

There is evidence that shows that security in the area of wireless computing is very important. The National Institute of Standards and Technology state in a document about wireless network security that “the risks provided by wireless technologies are considerable”. [NIST]

There is also evidence that shows that security in this area is not high enough today. When looking at the Wireless Security Policy from the Department of Defence in America, see appendix A, it is clear that they do not trust any of the wireless technologies. They mean that even if the wireless technology and devices can provide increased connectivity, they also provide an increase in security vulnerabilities and risks to their information and operations. Another proof that they do not trust wireless computing is that the use of wireless devices in the Pentagon and swing spaces is only allowed for unclassified data. [DoD02] Although the classified information is extremely important to keep safe also companies have information that is sensitive to competitors for example. Therefore it can be said that if the Department of Defence do not trust the security in wireless communication why should anyone else. Wireless communication is increasing and security in this area is thus very important to consider not only today but also in the future. The question is if the security requirements will change in the future or will it be the same issues that remain important.

6.3 Security Trends

6.3.1 Security in the Third Generation Mobile Networks

A believable way to communicate in the future is to use the third generation mobile networks. [NIST] One question is if this has any effect on the security for remote access. Known is that also for 3G, security and privacy will be of great concern. [Gar02]
There will be a convergence of Internet and telecommunication technologies and 3G systems will be more heterogeneous. Also when it comes to security, 3G systems will use security solutions inherited from both areas and be secured by using a combination of disparate security technologies. [How01]

It is important to consider that the devices have a continuous connection when connected to an IP network. Since the devices are always on, they must be authenticated before each network request. [NIST] The networks for 3G are getting smaller and more numerous, which means that hackers and other abusers of networks also have increased opportunities. [Bla00]

The next-level technology is said to offer more bandwidth, security, and reliability, which is suitable for multimedia, e-commerce, videoconferencing and other advanced applications. [Gar02] Since mobiles will be more used for e-commerce and other high-value services, it is likely that application layer attacks will be more common. The capabilities for terminals are becoming increasingly flexible and more software-based. This might also lead to the possibility of more attacks on the terminal software and operations using viruses for example. Therefore some mean that security mechanisms in 3G often will be provided at the application level. Another example of a security issue in 3G is all the separate terminal components that might be allowed to be added and removed on an ad-hoc basis. [How01] According to Howard et al in [How01] the devices must continually be regarded as insecure.

6.3.2 The Proposed Techniques for Remote Access

Wireless remote access will be the first application that is widely adopted according to some analysts. The reason to this is because of its high value, low technical barriers and market demand. [Mas99] Rule-based access, authentication and policies are techniques that can be used today to increase the security protection for remote access. However it is reasonable to think that these techniques also can be used in the future. It shouldn’t matter if the underlying transmission standards are changing it is still remote access that the security concerns. Also the conceptual models, in figure 5 and 6, show that the techniques can be useful also in these future protocols for remote access.

6.3.3 Privacy Concerns

It is possible that devices in a larger extent will be equipped with GPS-enabler. Also in this situation the device are subject to new security threats. Primarily it is the privacy concerns that in contact with a network can be violated due to the disclosure of users’ locations and activities to third parties. Scenarios, when advertisers and other service providers have agreements with the cellular telephone providers, are not impossible. The reason is that the user location information is valuable. The privacy policies of the cellular phone companies are therefore important to consider. [NIST]

6.3.4 User Interaction

Some state that the user should have as little interaction as possible when it comes to security. The operation of security features should however be transparent to the user and be easy to understand for them. [How01] The important point is still user awareness. [Wri99] Today as well as in the future education seems to be an effective way to increase the security level.
6.4 Final Discussion of the Future Scenario Problems

The problems derived from the scenario are possible futuristic problems. After looking at tentative solutions, evaluating them and looking at future trends, it is necessary to assess these problems again and discuss how to best solve them in the future.

1. Security Level

One idea in the futuristic scenario was the use of security levels on the user device. The question is if security levels are a good way to manage the security on mobile devices or not. If the user should have the control of changing security levels it will be very important with the assistance from policies. There should also be some kind of automatic response from the company side when the user changes the security level. The access rules should be automatically adjusted to the request and the situation. An authentication mechanism is also needed. As mentioned, some people also mean that the user should not handle the security level, but instead observe and be informed. If so, it is the company that must deal with the security level.

My opinion is that security levels are a good way to handle the security. The trends are showing that it is probable that this will be managed automatically by the company, or built in, in the device. Even though the users interact less in the security management, it is still important with awareness from the users in order to understand how the security is handled.

2. New Situations and Places

With nomadic computing comes communication on an anytime anywhere basis, which introduces mobile devices to new situations and places. If these situations and places are not secure enough, the users’ behaviour and awareness are of decisive importance to the exposure of their devices. This problem can be technically solved with help from security levels as well. If the company monitors the movements of the users and evaluates different situations, they can automatically adjust the security level accordingly and thereby increase the security.

3. Device Security

There are many tools that can be used to increase the security on the device. The company that developed the device can provide security mechanisms that are built-in in the device, like login password or key-board locking for example. The operating system can provide a possibility to hide files for example.

Authentication can be used for different purposes on the device. For the highest protection, biometrical methods are recommended due to the new upcoming devices and tools for this purpose.

Besides this, the user can download different software programs designed to increase the security. Also a mobile device needs virus protection, firewalls and other security software. If the company wants to protect their system they should provide its employees with these programs and regulate the use in policies or contracts. The best protection is provided if the company server automatically updates the protection on the user device, if it is needed, each time the user connects to the company system.

In similarity to stationary computers, knowledge is the determining factor. Security mechanisms and software always exist, but it is of vital importance that they are used in the right way. If they are not used as they are supposed to, the protection fails.
4. Hidden Affordances

To prevent hidden affordances, security mechanisms for device security as above must be used also here. The awareness and responsibility of the user are important in order to prevent unauthorized access and usage of the device. The best solution is therefore education of the users, in order to as far as possible protect the information on the device and prevent problems with hidden affordances.

Another angle is to see the device in the same way as a wallet. Users normally do not lend their wallet to an unknown person. Instead it can be wiser to value information just as high as money. The most intelligent thing to do is actually not to lend a mobile device to someone that you do not trust. However both a wallet and a mobile device are still a target for theft, which the user has to be prepared for.

5. Responsibility

The users have a responsibility of handling the security on the device. This is especially important when they are in contact with a company. When it comes to remote access both the user and the company are responsible for the security. The problem is to make both sides taking their responsibility seriously. One solution is to use policies when dealing with remote access. However contracts with agreed rules can have a more forcing effect on both parties. The important thing is to make the company responsible for possible incidents, as long as the users follow the rules.

6. User Integrity

There are many examples indicating that it is becoming more common with techniques and services that threaten the integrity of the users. This is alarming for the users, why extra focus must be given on integrity protection. Integrity of the users in the area of nomadic computing can be recommended as subject for future research.

Between the employee and the company, a policy or a contract is a good solution. Then both parties know what is allowed to do and what information that is allowed to use, since this is regulated in the document.

For the users, it is not only for this situation protection is needed. Every time they are using the Internet for example, information can be gathered and stored that threatens the users’ integrity. Cellular telephone providers and various other companies will have the capacity to violate the integrity. In this situation it is the user self that must be observant of how the information about them are handled. Policies are often used today and are likely to continue to be the only way to know how the information is used by the different actors. The users must however look these things up for themselves, which is why user awareness is crucial.
7 SUMMARY AND CONCLUSIONS

7.1 Nomadic Computing and Remote Access

Nomadic computing is becoming more and more common today. There is a need
to be able to move around and continue working, people are getting used to mobile
phones and to have information available at all times.

Except need, there is also important with trust according to the co-evolution
model. Trust can depend on the security, which is why security is of decisive
importance to the future use of nomadic computing.

Remote access will soon be possible from many different types of wireless
networks. Security is very important since the companies open up doors that should
only be open for authorized employees. However, it is obvious that the companies
have the responsibility to preserve the security in these situations. A company system
contains a lot of information, some of high value for the company. Remote access will
be of great importance for the employees when they are working on the move, since
they can access the information that they need when they need it. This is thus
profitable for the company as well as for the employees.

Remote access does only exist in a small scale today, but is expected to be one of
the first and widely used fields of application within nomadic computing.

7.2 The Techniques

The three techniques that are focused in this thesis are here summarized together
with other mentioned techniques. The purpose is to schematically see possible
techniques of today, upcoming techniques that can be available within approximately
five years and techniques that are on research stage or suggestions of future
techniques.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Today</th>
<th>Upcoming</th>
<th>Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security Level</td>
<td>Rule-based Access</td>
<td></td>
<td>New tools for rule-based access; GPS</td>
</tr>
<tr>
<td>2. New Places and Situations</td>
<td></td>
<td>Antivirus software, firewalls, fingerprint reader authentication, etc</td>
<td>Writing recognition, eye scanning authentication</td>
</tr>
<tr>
<td>3. Device Security</td>
<td>Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Hidden Affordances</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Responsibility</td>
<td>Policy</td>
<td></td>
<td>Contract</td>
</tr>
<tr>
<td>6. User Integrity</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The three techniques focused in this thesis, rule-based access, authentication and
policy are very useful today, but they can also be used in the future. Their form can
change and they can be more adjusted to the time, since new authentication methods
for example, are continuously emerging. They can also with advantage be used
together with other techniques or in combination with each other.

For the first and the second problem rule-based access can be used and suggestions
for the future are that new tools like positioning are used for the rule-based access.
For the third and the fourth problem authentication can be used. Also other methods to increase the security on the mobile device and prevent hidden affordances have been discussed. Upcoming techniques are for example antivirus software and firewalls, which can be downloaded to the device. New techniques for authentication, like fingerprint readers are coming as well. Suggestions for the future are to be able to use built-in cameras for eye scanning or touch-screens for writing recognition.

For the last two problems policies exists and can be used today. Another form of solution, namely contracts, is suggested to be used in the future instead of policies between the company and its employees.

7.3 Conclusions

To conclude this work I am going to answer the main question of how and when secure nomadic computing can be offered.

As known, the security in the area of nomadic computing is not high enough today. The fact, that nomadic computing is increasing, makes the security even more important. The question is if nomadic computing ever can be secure and what level of security that decides if nomadic computing is secure or not. This question can not easily be answered, however some suggestions can be made of what can be said to be basic requirements.

For the first, we must be able to seamlessly roam between different kinds of networks and still keep a high level of security, for example with an end-to-end encrypted tunnel, we must be able to use biometrical authentication on the device, and there has to be a strong access control on the remote side.

Second, I think that for nomadic computing and remote access to be secure, the users themselves have to see to their devices and protect them in the best possible way, as well as the companies must put their effort on doing everything in their power to provide the highest possible protection. Everything in between are out of their hands and instead it is up to the cellular telephone providers and the owners of the networks to protect.

User awareness and education are a great step on the way. Even if efforts are made to simplify and decrease the interaction of the users, awareness and education are always important.

I also think that the three techniques, rule-based access, authentication and policy/contract, will continually be an important part of trying to make nomadic computing and remote access secure.

Security is always important, today as well as in the future. A certain amount of threats will always exist, no matter how many security mechanisms that are used. New improved mechanisms comes all the time, however also the attacks are more sophisticated and the attackers are likely to get smarter every day.

As seen in the model of technology uptake, different parts are affecting the evolution of nomadic computing. Security is part of the concurrent forces in the evolution that is needed to create trust, which is decisive to the employment of nomadic computing in the future. The user must have confidence in the technique, but as seen in chapter 5 the user must also have confidence in the organisation in order for the technique to evolve and be adopted.

Today nomadic computing is only in its initial phase, but in the future I think nomadic computing will be as normal and frequently used as the cellular phones are today, as long as an effort is made to keep a high level of security.
8 REFERENCES

8.1 Literature


8.2 Proceedings and Articles


### 8.3 White Papers and Reports


# Glossary

Own explanations have been used in this glossary. There are many definitions of the different terms, but these explanations are defining how the terms should be understood in accordance to the context of this thesis.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACL</strong></td>
<td>Access Control List. Contains sets of data with access rights for e.g. users or processes, to different objects like systems, resources, services.</td>
</tr>
<tr>
<td><strong>GPRS</strong></td>
<td>General Packet Radio Service. An extension of <strong>GSM</strong>, a packet switched standard used in the same network for communication from mobile devices.</td>
</tr>
<tr>
<td><strong>GSM</strong></td>
<td>Global Standard for Mobile communication. A public network for telephone communication.</td>
</tr>
<tr>
<td><strong>HTTPS</strong></td>
<td>Secure Hyper Text Transfer Protocol. A protocol used to transmit individual messages securely over the Internet.</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>Internet Protocol. A network layer protocol, which moves data in packages. IP is not connection oriented.</td>
</tr>
<tr>
<td><strong>OSI</strong></td>
<td>Open System Interconnection. A reference model for computer networking containing seven protocol layers, from the first physical layer to the last application layer on the top of the communication.</td>
</tr>
<tr>
<td><strong>SSL</strong></td>
<td>Secure Socket Layer. A protocol used to transmit private documents over the Internet between a client and a server.</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>There can be both natural and technical threats to the security. In this work threats have the meaning of being technical.</td>
</tr>
<tr>
<td><strong>TLS</strong></td>
<td>Transport Layer Security. A protocol used to guarantee privacy and data integrity over the Internet between a client and a server.</td>
</tr>
<tr>
<td><strong>UMTS</strong></td>
<td>Universal Mobile Telecommunications System. A packet switched standard with higher speed than <strong>GPRS</strong>. Often seen as a 3G standard.</td>
</tr>
<tr>
<td><strong>Virus</strong></td>
<td>A file containing code that can be loaded and run on a computer or a mobile device without being detected. Can cause damage for example by using all memory that is needed for a system to function.</td>
</tr>
<tr>
<td><strong>WAP</strong></td>
<td>Wireless Application Protocol. A protocol used in the <strong>GSM</strong> network for communication from mobile devices.</td>
</tr>
<tr>
<td><strong>WEP</strong></td>
<td>Wired Equivalent Privacy. A security protocol for WLANs with the purpose of encrypting data over radio waves.</td>
</tr>
</tbody>
</table>
APPENDIX A

Pentagon Area Common Information Technology (IT) Wireless Security Policy

September 2002
EXECUTIVE SUMMARY

This Pentagon Area Common Information Technology (IT) Wireless Security Policy provides guidelines for implementing wireless technologies in the Pentagon and swing spaces. The guidelines present a balanced approach for mitigating the vulnerabilities and security risks while supporting the responsible introduction of new technologies into the workplace.

Highlights of the Pentagon Area Common IT Wireless Security Policy are as follows:

- Recognizes the pace of technological change and, therefore, requires an annual review to keep pace with the rapidity of technological advances
- Does not apply to Sensitive Compartmented Information Facilities (SCIFs) which are governed by Director of Central Intelligence Directive (DCID) rules
- Excludes Land Mobile, Emergency, and Tactical Radios and one-way receive-only devices (e.g., devices with a wireless receiver and no transmitter)
- Prohibits:
  - Connectivity to a classified network or computer
  - Synchronization with IT devices that are not approved by a Designated Approving Authority
- Allows use of wireless devices (e.g., cellular telephones and Personal Digital Assistants):
  - For unclassified data only
  - In areas where unclassified information is electronically stored, processed, or transmitted
  - In areas where classified information is electronically stored, processed, or transmitted unencrypted when there is a documented operational need; the device’s infrared, radio frequency and microphone/audio capabilities are disabled; and DCID rules are followed.
- Requires punitive action for repeated violations of this policy that jeopardize the security of the Pentagon Area common IT Enterprise
PENTAGON AREA COMMON IT
WIRELESS SECURITY POLICY

1.0 INTRODUCTION

The commercial sector has introduced many wireless technologies that support increased productivity and connectivity. Wireless devices are rapidly being deployed in the Department of Defense (DoD) to support mission operations. Although wireless computing devices and infrastructure support systems can provide an increase in connectivity, they also provide an increase in security vulnerabilities and risks to DoD information and operations. While we proceed to assimilate these technologies in the DoD workplace, we also need to ensure a balanced approach is taken regarding the associated vulnerabilities and security risks. Thus, an integrated protection approach must be implemented when deploying wireless technology to support DoD business and mission operations.

This document establishes policy, definitions, and responsibilities necessary to mitigate the vulnerabilities and security risks introduced by wireless technologies and the infrastructure installed to support them. This policy will be reviewed annually and updated, if required, to address technology improvements which may provide practical application for the Pentagon community without introducing additional security risks and vulnerabilities.

1.1 Policy Goals

Information Assurance (IA) is defined as (DoD) information operations that protect and defend information and information systems by ensuring their confidentiality, authentication, availability, integrity, and nonrepudiation (Reference Section 6, Item 7). These IA axioms are described as follows:

- **Confidentiality**: Verify that information is private and therefore seen and accessed only by intended recipients. Confidentiality is created primarily through the use of protocols that use encryption.

- **Integrity**: Verify that information received is the same information transmitted by the originator, unchanged.

- **Authentication**: Identify an individual or computer to ensure access to information is authorized. Authentication goes hand-in-hand with identification and confidentiality.

- **Nonrepudiation**: Ensure that an individual cannot deny sending or receiving information.
Availability - Ensure that information (voice, video, and data) and supporting service resources (e.g., server, local networking infrastructures, and transport medium) are up and running when needed.

Based on the five IA axioms, the goals of this policy are to:

1. Protect DoD information, users, and wireless devices from unauthorized disclosure
2. Ensure that DoD information is protected against an intrusion that could alter, disable, or circumvent the transmission
3. Require centralized oversight, configuration management, and control of wireless information systems
4. Ensure protection against physical compromise (e.g., immediate notification of misplaced or missing DoD wireless devices to the appropriate authority)
5. Ensure user authentication of DoD information transferred via wireless computing devices
6. Ensure there will be no adverse impact to DoD critical operations if wireless computing devices and the supporting infrastructure are rendered inoperable

1.2 Applicability and Scope

This policy applies to:

1. Pentagon Area (defined as Pentagon and swing space) tenants (and their on-site contractors) which include Office of the Secretary of Defense (OSD), Joint Staff (JS), Washington Headquarters Services (WHS), the Military Departments, the Defense Agencies, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the Pentagon Area DoD Components/Agencies)

2. Wireless-Information Systems (W-IS) defined as wireless telecommunication or computer-related equipment or interconnected system or subsystem of equipment (includes software, firmware, and hardware) that is used in the Pentagon Area to support DoD business, operations, and missions in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data. W-IS excludes Land Mobile, Emergency, Tactical Radios, and one-way receive-only devices

2.0 POLICY

2.1 All Pentagon Area W-IS shall be:

1. used for Unclassified and Sensitive But Unclassified (SBU)/ For Official Use Only (FOUO) data, only
2. approved, certified, and accredited by the Pentagon Designated Approving Authority (DAA) for Common IT (CIT) or the Component/Agency's DAA based on the supported business or mission operations and in accordance with the DoD Information Technology System Certification and Accreditation Program (DITSCAP) or successor directives
3. compliant with DoD TEMPEST policies and guidelines (NSTISSAM TEMPEST/2-95)
4. compliant with applicable National Telecommunications and Information Administration (NTIA) and Federal Communication Commission (FCC) requirements
5. compliant with most recent DoD policy for authentication
6. configured with preferences and settings for services approved by the Cognizant DAA (i.e., Pentagon DAA for CIT or the Component/Agency's DAA)
7. configuration managed and controlled

2.2 All Pentagon Area W-IS shall not be:

1. connected to a classified network or computer
2. used where classified information is electronically stored, processed, or transmitted un-encrypted unless all of the following are met:
   a. there is an operational need and the mission cannot be accomplished without the use of the W-IS
   b. the device's Infra Red (IR), Radio Frequency (RF) and microphone/audio capabilities are disabled
   c. Director of Central Intelligence Directive (DCID) rules are followed
3. used as a mission critical system; there shall be no impact to mission operations if the Pentagon Area W-IS fails to sustain medium level outages lasting from seconds to hours
4. used as a primary means of communications for mission operations
5. used to download or load any freeware or shareware enhancements or any extraneous software
6. used to synchronize with a non-Pentagon or non-Component/Agency DAA approved and accredited system or network (including personally-owned home computers or contractor-owned computers or networks)

2.3 Pentagon Area Defense network-capable, wireless computing devices shall employ the following security mechanisms:

1. password protection or strong identification and authentication using techniques such as CAC, PKI and Biometrics for those W-IS that store, process, and transmit
DoD information. Passwords shall not include words found in the dictionary and shall be at least eight (8) characters in length using 3 of the following attributes: upper case alphabet characters, lower case alphabet characters, numeric characters and special characters. The password system will render the device inoperable without the proper authentication

2. features and capabilities to disable IR, RF, and microphone/audio (see definitions)

2.4 Acquisitions of Pentagon Area W-IS that store, process, and transmit DoD information shall require the following features:

1. compliant with most recent DoD policy for authentication
2. intrusion detection, auditing, and monitoring mechanisms
3. encryption via NIST FIPS-approved or NSA-approved encryption mechanisms while in the wireless environment
4. virus protection software or equivalent protections to prevent action of malicious logic
5. digital transmitter/receiver

2.5 The Pentagon Area W-IS common IT transport infrastructure deployed within the Pentagon shall:

1. support Pentagon DAA for CIT and Component/Agency DAA approved, certified, and accredited W-IS
2. support security for voice, data and control channel information via NIST FIPS-approved encryption mechanisms for all modes of operation
3. be under the direct control of the Federal Government
4. be able to monitor and detect the exfiltration of signals from areas where classified information is being electronically stored, processed, or transmitted un-encrypted (e.g., passive RF detector)
5. provide the capability to restrict user options to minimize the amount of traffic related information transmitted
6. provide security mechanisms that are scaleable, manageable, flexible, and standards-based
7. employ security mechanisms that are compatible and inter-operative with those mechanisms used on wired voice and data telecommunications networks and computing devices
8. support strong identification, authentication and auditing if remote administration is employed

3.0 RESPONSIBILITIES
3.1 Pentagon DAA for CIT shall:

1. provide oversight for Pentagon Area wireless policies and implementations
2. provide guidance to Component/Agency DAAs on wireless vulnerabilities, threats, and risks consistent with applicable DoD policies, directives, instructions, and DoD authorized security assessments.
3. provide accreditation procedures to Component/Agency DAAs and have final connection approval authority over W-ISs in the Pentagon Area
4. provide security awareness training guidance to Component/Agency DAAs for Pentagon Area W-ISs
5. recommend to the DoD CIO that a Component/Agency be disconnected from the Pentagon common IT transport infrastructure for repeated violations (i.e., greater than three) of a nature that jeopardizes the security of the Pentagon Area common IT enterprise

3.2 The Component/Agency DAA shall:

1. approve, certify, and accredit all Component/Agency W-IS used in the Pentagon Area (Operational Security and Force Protection concerns must be evaluated)
2. approve, certify, and accredit W-IS systems in accordance with the DITSCAP. The accreditation documentation shall be in accordance with the Pentagon DAA for CIT accreditation procedures
3. conduct an audit at least annually to detect unauthorized W-ISs used within the Pentagon
4. incorporate wireless technology into the Information Assurance training (to reflect changes in technology, and Operational Security and Force Protection concerns) for all affected personnel (i.e., administrators and users)
5. establish disciplinary actions for failure to adhere to W-IS policies and directives
6. report security related events (e.g., the loss or misuse of the W-IS) to the Pentagon DAA for CIT
7. develop recovery and restoration guidance for compromised W-ISs
8. require affirmed acknowledgment that the user shall comply with all DoD applicable policies and directives

3.3 The Pentagon Area W-IS User shall:

1. be trained on the responsible use of accredited Pentagon Area W-IS
2. provide affirmed acknowledgment that they will comply with all DoD applicable policies and directives
3. report lost or stolen Pentagon Area W-IS within 24 hours through the user’s chain of command to the Component/Agency DAA
4. report violations to this policy through the user’s chain of command to the responsible DAA
5. immediately disable any RF, IR, and microphone/audio features and return any W-IS to the Component/Agency’s DAA if the device receives or is used to transmit any classified data

3.4 The Pentagon Area W-IS common IT transport infrastructure Service Provider shall:

1. support Pentagon DAA for CIT and Component/Agency DAA approved and accredited W-IS
2. support security for voice, data and control channel information via NIST FIPS-approved encryption mechanisms
3. be under the direct control of the Federal Government
4. be able to monitor and detect the exfiltration of signals from areas where classified information is being electronically stored, processed, or transmitted unencrypted and at critical points in the Pentagon (e.g., E-Ring)
5. provide the capability to restrict user options to minimize the amount of traffic related information transmitted
6. provide security mechanisms that are scalable, manageable, flexible, and standards-based
7. employ security mechanisms that are compatible and inter-operable with those mechanisms used on wired voice and data telecommunications networks and computing devices

4.0 EFFECTIVE DATE

This policy is effective immediately.

5.0 POC

The point of contact for this policy is the DoD CIO.

6.0 REFERENCES

1. DoDD Number O-8530.1, dated January 8, 2001, Subject: Computer Network Defense (CND)

4. Deputy Secretary of Defense Memorandum, dated May 6, 1999, Subject: Department of Defense (DoD) Public Key Infrastructure (PKI)


6. Policy for Land Mobile Radio Systems (August 1, 2001)


10. DODD 5200.2 Department of Defense Personnel Security Program (DoDPSP), 9 April 1999

11. DODD 5200.2-R DoD Personnel Security Program, January 1987