DSV Report Series No. 09-001

Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks
Securing Information Assets:
Understanding, Measuring and Protecting against Social Engineering Attacks

Marcus Nohlberg
Abstract

Social engineering denotes, within the realm of security, a type of attack against the human element during which the assailant induces the victim to release information or perform actions they should not. Our research on social engineering is divided into three areas: understanding, measuring and protecting. Understanding deals with finding out more about what social engineering is, and how it works. This is achieved through the study of previous work in information security as well as other relevant research areas. The measuring area is about trying to find methods and approaches that put numbers on an organization’s vulnerability to social engineering attacks. Protecting covers the ways an organization can use to try to prevent attacks. A common approach is to educate the users on typical attacks, assailants, and their manipulative techniques. In many cases there are no preventive techniques, dealing with the human element of security, in place.

The results show that social engineering is a technique with a high probability of success. Furthermore, defense strategies against it are complicated, and susceptibility to it is difficult to measure. Important contributions are a model describing social engineering attacks and defenses, referred to as the Cycle of Deception, together with a thorough discussion on why and how social engineering works. We also propose new ways of conducting social engineering penetration testing and outline a set of recommendations for protection. It is crucial to involve managers more, but also to train the users with practical exercises instead of theoretical education, for example, by combining measuring exercises and penetration testing with training. We also discuss the future threat of Automated Social Engineering, in which software with a simple form of artificial intelligence can be used to act as humans using social engineering techniques online, making it quite hard for Internet users to trust anyone they communicate with online.
There are four persons who were absolutely crucial in this research process, mentioned in chronological order. The first is my former boss, now friend, Kenneth Alfelt. He set the wheels in motion, and got the process started. My supervisor Benkt Wangler made it all possible through constant support and, well, supervision. It has been an honor working with you. My co-supervisor Stewart Kowalski supplied a never-ending wealth of inspiration and brilliance. Thomas Ekström and The Logic Planet AB, gave me invaluable support.

I have also had the blessing of highly supportive friends and colleagues. I would especially like to mention Rose-Mharie Åhlfeldt who not only wrote a paper together with me, but also helped me out during the processes with so many things, as did my dear friend Carl-Johan Åkerberg and Alexander Backlund. Most of the papers were written in collaboration with others: Johannes Bäckström, Kerstin Karlsson, Markus Huber and Martin Boldt. It has been a blast writing papers with you, and I would love to do it again. Vera Lindros did a fantastic job helping me with the language of the thesis.

This thesis is dedicated to my family. This is not something I just write to keep the peace (since they will all be reading this) but because I mean it. You have helped me, inspired me, fed me and put up with me when I turned massively self-occupied during the final process of this thesis (and perhaps long before that). More concretely, this is dedicated to: My parents, Arne and Ingrid Nohlberg, for their undying support and love. Carina and Julius Mikszáth, my sister in blood and my brother in spirit. My dear sister Maria Almqvist and her husband, Erik. Then we have the next generation: My niece (Sara) and my nephews (Sebastian, Olof, Oskar, Victor and Elias).

The list of names here could be very long. So for anyone who does not find his or her name in the list above, this is for you: Thank you.

Yes, this turned out to be quite sentimental. But it is sentimental to write an Acknowledgement-section after a long research project such as this thesis. Try it yourself. You should! Research rocks!
Phishing ..................................................................................................................................... 58
  What Phishing is .................................................................................................................... 59
  Spear Phishing ...................................................................................................................... 60
  Spy-Phishing ........................................................................................................................ 60
  Examples of Phishing Attacks............................................................................................... 60
  Defense against Phishing ........................................................................................................ 64
  Impact of Phishing and New Threats ..................................................................................... 65
  Why Social Engineering and Phishing Works ........................................................................ 65

Research Results ..................................................................................................................... 67
  Understanding ......................................................................................................................... 67
  Measuring ............................................................................................................................... 68
  Protecting ............................................................................................................................... 70

Concluding Discussion ............................................................................................................ 73
  Method .................................................................................................................................. 75
  Results ................................................................................................................................. 75
  Contributions ......................................................................................................................... 76
  Scientific Quality ................................................................................................................... 78
    Credibility ........................................................................................................................... 78
    Conformability ................................................................................................................. 78
    Dependability ............................................................................................................... 78
    Transferability ................................................................................................................. 79
    Relevance ....................................................................................................................... 79
  Future Work ........................................................................................................................... 80

References ............................................................................................................................... 83

Part II: Publications ................................................................................................................. 89
Part I: The Research Frame and Research Results

Part I of this thesis consists of six chapters and presents the background and structure of the research. It also contains a description of the results of the research, the discussion and suggestions for future research.

Chapter 1 presents the research problem, aim and objectives together with a brief overview of the research approach, delimitations, results and contributions. Related research and the thesis structure are also described.

Chapter 2 presents the research background by describing fundamental concepts in information security.

Chapter 3 presents the research design; how it was planned and executed.

Chapter 4 presents social engineering and Phishing.

Chapter 5 presents the research results.

Chapter 6 presents the concluding discussion as well as suggestions for further research.
“I am a lot like you. We have the same interests, are of the same age and, yes, we even think strangely alike. It is weird that we never met before! I am the kind of person you can really trust. We share so much! We even dislike the same things! If I want a small favor from you, that is really nothing to talk about, now is it? That is what friends do, is it not?”

Social engineering\textsuperscript{1} is about creating deceptive pretexts; examples of which can be seen in the fictional text above. In social engineering the goal is to trick the victim into sharing protected information, or to make them perform certain actions. It is a part of security sometimes omitted from the big picture, even though most information security professionals seem to agree that it is of great importance. The area of this thesis is information security, which is a broader approach to security than computer security in that it does not care about the form of the data it wants to protect – thereby including humans in the big picture.

Regarding security as a broad concept has flourished in recent years. We see some interesting numbers in the Global statistics from “the Global State of Information Security in 2007” (PWC, 2007). More and more companies now employ a CSO or a CISO (60 % in 2007, 43 % in 2006). There has also been a steep increase in having an overall information security strategy (37 % in 2006 and 57 % in 2007). Technical safeguards are all the rage, 88 % of the organizations now employ firewalls, 82 % use backups and 80 % have protection against spyware (PWC, 2007). What is notable, however, is that 63 % of the organizations do not use audits or monitoring to ensure that the employees actually follow the security policy. In fact, less than half (48 %) actually try to measure and review the efficiency rate of their security policies and procedures (PWC, 2007). Among major Swedish companies it is widely thought, historically, that security is of the utmost importance, no matter the cost (Brandon, 2003). With the continued increase in the focus on information security, it is notable that much of the attention is put on increasing technical security such as firewalls, anti-virus and so on. However,

\textsuperscript{1} The term "social engineering" is not only used within security but also in sociology where it describes the practical use of sociological knowledge, and in political science when talking about the large-scale influence on attitudes and social behavior in society by governments or private groups.
an increasing number of organizations do not know about the number and nature of security incidents (PWC, 2007). This is probably not because they do not get data from their protective systems, but because security specialists have started to realize that information security is much more than what is easily measured with the conventional solutions and that focus has to be put on the human element of information security (PWC, 2007).

In this thesis we focus on the human element of security. We do this by addressing the attack technique called “social engineering”, a major concern in information security. Social engineering was made infamous by Kevin Mitnick, partly through his actions as a hacker, and partly because of his writings and speeches on this hacking technique. It is notable that Mitnick did in no way invent the technique, since it is basically frauds used in an information security context. Mitnick managed to get access to several high security government systems, not by using high tech password crackers or obscure bugs in the systems, but by using a con man’s approach to obtaining information. By piecing information together he managed to get the access he wanted. His most frequently used tools were the telephone and a well planned out ruse. Some of these deceptive tactics are used in Phishing, where they can be combined with technological means to provide a devastatingly efficient attack. The difference between Phishing and social engineering principally lies within the high degree of personal contact within social engineering, and the very limited amount of personal contact in Phishing. Therefore the scales differ; social engineering tends to be used against a limited number of targets (that has been selected with greater care), while Phishing uses data mining, making it similar to spam, in order to attack more marks.

Social engineering attacks are quite different from many of the primarily technical attacks, due to them also having a clear, specific aim. The vast majority of attacks and threats to security have been “script kiddies”, viruses, trojans and other broad attacks without specific aims (Mitnick & Simon, 2002). Recently there are indications that organized crime is behind more and more of the attacks, and the focus has moved away from creating viruses and attacks that are mostly a nuisance to creating attacks that can generate an income (Jackson Higgins, 2008).

Since many users do not believe that anyone would ever attack them, because they are not “rich and famous”, and that hackers cannot do much damage anyway (Brostoff, Sasse & Weirich, 2002), social engineering attacks can be highly successful. This attitude is also influenced by the fact that most users do not understand how security works and therefore construct their own, often incorrect, models (Adams & Sasse, 1999). The “old” way of managing information security has led to two specific problems, according to Adams and Sasse (1999 p. 45):

4
(a) users’ lack of security awareness, and

(b) security departments’ lack of knowledge about users, producing security mechanisms and systems that are not usable. These two factors lower users’ motivation to produce secure work practices. This in turn reinforces security departments’ belief that users are “inherently insecure” and leads to the introduction of stricter mechanisms, which require more effort from users.

The setting is thus; we are in a world in which security spending has increased but so have security incidents. In addition, the users lack security awareness and the protective measures are not well liked, among the users, or usable. At the same time, there are attacks, based on social engineering, which are easy to learn and hard to protect against, that can be quite efficient.

The Problem

It seems that stricter technical controls may not be a viable solution to the problems associated with humans and security. In fact, many users know their behavior is not compliant with the current security policies of the organization and instead find solace in the behavior of fellow employees, and the belief that the regulations are unrealistic (Brostoff, et al. 2002).

In a study carried out by Treasury Department inspectors, one third of Internal Revenue Service (IRS) employees divulged their logins and passwords to auditors who called pretending to be computer technicians (Dalrymple, 2005). There have been other studies on the “gullibility” of users, and the extent to which they submit information while under attack from perpetrators using Phishing and social engineering techniques. The results generally indicate that users are quite susceptible to these kinds of attacks, but due to a high degree of uncertainty about the studies’ results, it is hard to determine the extent of their vulnerability. Nevertheless, some studies do provide a certain shock value. For instance, when revisiting the highly publicized “Chocolate for passwords” study three years later, it was shown that 64 % would submit their office computer password in exchange for a piece of chocolate (Kelly, 2007).

Perhaps it is as in a comment from one of the interviews conducted by Björck (2005, p. 186): “It doesn’t matter what technology you have - there is no technology that can protect you against human beings - forget it.”

The following quote is Gartner’s (2002a) comments about the risks:

"Malicious individuals have always known that the best way around any security system is to manipulate a human target into giving them what
they want – what we call social engineering. It remains the single greatest security threat to enterprises.”

It is apparent that there are great risks associated with humans and security, and especially with regard to attacks aimed at human weaknesses. We, in the information security world, often know little about what it is that makes these attacks succeed, how we can measure them and, perhaps more importantly, how we can prevent them. If we do not know the extent of the risks, we can hardly realistically judge whether any protective measures applied are actually increasing security or if they are just for show. From a cybernetics perspective, this amounts to Ashby’s “Law of Requisite Variety” (Heylighen & Joslyn, 2000). If we want to secure a system, we need to know what to secure it against. Furthermore, if we ignore attacks aimed at humans, we almost ensure that those attacks are the ones to which we will be vulnerable. Security must be holistic.

Early in the research process, in attempting to identify what social engineering consists of, we created a mind-map inspired by Näckros (2005), which included different, and possible, influencing factors. This mind-map, Figure 1, which is in no way a complete description of the topic, provides an understanding of the complex issues that in some way can be argued to be connected to or influence social engineering and the human element of security. This mind-map was created as a tool with which to visualize the research area and is based on the findings from the literature study. The purpose of the mind-map is to illustrate the broad selection of research areas associated with the human element of security and should not be regarded as a complete analysis of the interconnecting areas.
Figure 1. An illustration of research areas and subjects connected to the human element of security/social engineering.

In order to organize the research work, as well as its presentation, this thesis is structured like a temple, because as Sun Tzu states in “The Art of War” (Sun Tzu, translation from 1910): “Now the general who wins a battle makes many calculations in his temple ere the battle is fought.”
The temple, as illustrated in Figure 2, consists of a sturdy foundation, the research approach, on which the aim and the research question described in this section have been added. Additional sections of the thesis build the structure that culminates in the flag of contributions; the final part of the calculations made in the temple that comprises this research project.

The Aim

The aim of this work is to increase overall information security readiness by addressing some of the most efficient attacks that exist – attacks against the human element. This is achieved by gaining a working knowledge of the threat named social engineering, an often neglected, but, by many considered, crucial area of information security. In extending the knowledge of what makes humans susceptible to attacks, as well as learning about current attacks, their countermeasures and methods of testing organizations and individuals’ vulnerability to them, we can make new and important research contributions to academia, and provide results that are useful for professionals working within information security.

The Research Question and Objectives

To put it succinctly, the research question of this work is: “What is social engineering and how can we best protect ourselves against attackers who use it?”
With regard to the research question, we believe there are three aspects of the area that are the most important ones to study. The selection of these three areas is based on previous work, experience, ongoing literature studies, as well as informal discussions with a number of information security professionals. In addition, each area represents an objective.

- **Objective 1:** To learn more about what constitutes social engineering. Also, what the underlying mechanisms are, how humans are influenced, and what techniques are being used by attackers? Furthermore, to create a model that better describes the concept, in order to understand the term. To improve knowledge of the area it is important to review the literature on the subject, and learn from other areas of research. This objective covers the area of understanding.

- **Objective 2:** In order to even begin protecting ourselves against social engineering attacks, we need a means of measuring the current level of readiness to see if the protective measures used have any effect. We cannot control what we cannot measure. Thus, it is necessary to study the methods of measuring an organization’s vulnerability to social engineering. Although a few methods of penetration testing are in use today, many of these have ethical or practical problems. An effort to assess the efficiency of preventive approaches in this area is necessary. By testing several ways of measuring, a set of recommendations is created. This objective covers the area of measuring.

- **Objective 3:** To study how social engineering attacks can be prevented. In order to ensure security, protection against nefarious attacks is of the utmost importance. The current means of protection are studied, and novel defense approaches based on knowledge from other areas are tested. This objective covers the area of protecting.

The research approach aims to gain as much knowledge as possible from literature studies, mostly to obtain background knowledge on the subject. In order to acquire a deeper understanding and to achieve novel results from the organizations examined, both qualitative and quantitative studies are used.

### The Research Approach

The research began with an early phase, which developed from an idea of examining the human element while interviews with systems administrators were being conducted in a study on overall security readiness in health care (Åhlfeldt & Nohlberg, 2005), in combination with an ongoing literature study. As this literature study and the interviews with systems administrators indicated a need to examine social engineering further, the subject was divided into three sub-areas, as discussed in 1.3. The subsections below discuss these three areas in more detail.
In order to address the research question and the objectives, a research plan was designed. The goal was to work in each of the three objective areas, and to try to maintain an industrial focus with some practical applicability of the results. During the research process, literature was continuously studied in order to obtain the necessary background information, as well as updates on new related research. The plan is illustrated in Figure 3, and described further in Chapter 3. Protecting is covered in most of the papers, but Paper 2 specifically focuses on that area.

![Figure 3. The research plan concerning aim, research questions and objectives.](image)

The published results from the studies are found in Part II, and summaries of the results and contributions are presented in “Concluding Discussions” on page 73.

**Understanding**

In order to learn more about social engineering in general, we studied the materials that could be found in the literature, written and online. A broad range of subjects were studied, ranging from sociology, psychology, and criminology, as well as information security and more obscure literature, both academic and popular. One of the conclusions we could draw was that noticeable amounts of texts are derived from a small selection of imperative works that we then chose to focus on. The most relevant parts of the knowledge about social engineering and manipulative techniques were summarized in a book chapter (Book Chapter 1, Part II). As we found some flaws in the common description of what constitutes social engineering, as well as the attack cycle in general, we developed a new model describing social engineering. The cycle of deception was created using the results from the literature study, as well as those gained from semi-structured interviews, as sug-
gested by May (2001), conducted with the lead criminal investigator in a relevant case. This cycle was subsequently further validated by discussing its usefulness (1) with security experts and (2) with a group of social workers who are often subject to deception.

Measuring
In the attempt to devise how to best measure susceptibility to social engineering attacks, a selection of methods was used. In the first study, a quantitative approach was used, in which hundreds of subjects were deceived into believing that they were answering questions related to “micro efficiency”. This false concept was used rather than openly informing that the questions related to information security (Paper 1, Part II). The same quantitative approach was used in a highly sophisticated spear-phishing attack against students in a study to determine whether security education actually made students behave with more security awareness. It did not, apparently (Paper 6, Part II). In a much softer approach, and in an attempt to find novel aspects of security, qualitative research was used in the next study. The subjects of this study were interviewed about security in general and social engineering in particular. They were asked to think about possible flaws after being given short introductions to the area. This approach exposed a selection of weaknesses and perhaps also increased the subjects’ interest in security afterwards. The study thereby bordered on action research, although this was not a primary goal. With regard to readiness at management level, we used qualitative interviews structured on the deception cycle as developed in Paper 3, Part II. By interviewing managers and senior employees at large corporations, we did obtain an overall image of the readiness for a highly probable kind of future attack, which is automated social engineering.

Protecting
One of the methods useful for preventing successful attacks is to carry out the measuring as discussed above. During those tests, a number of suggestions for protection also emerged and were discussed. We did realize that one of the crucial aspects of preventing these kinds of attacks was to make it possible for managers to understand the security risks in general and social engineering in particular. One way this was done was to study how senior security professionals inform managers about security (Nohlberg & Bäckström, 2007). We also realized that in order to facilitate ongoing information and awareness at a higher management level, a software solution was necessary. To address the problems associated with informing managers, who often have little interest in security nor time to learn a new piece of software, we developed a prototype management information system for information security (Paper 2, Part II). This was created using a user-
centered approach to security and software development. The interface was tested by the target audience and regarded as good. It was considered crucial by the studied organization that the interface design had a high degree of usability. If human weaknesses are to be addressed in a software solution such as the one proposed in Paper II, it is important to design a solution that is easy to use and adapted to the needs of the target audience. Usability is, in fact, a crucial part of security in general, and human related security in particular. If the users do not understand how to use the products correctly, there is a risk that they will find another way of using it, as unsafe as that might be. We need to pay attention to ensuring that the users understand the programs and emphasizing the importance of secure behavior when using computers and computer networks (Whitten & Tygar, 1998; Flechais & Sasse in Cranor & Garfinkel 2005; Dourish & Redmiles, 2002).

Research Delimitations

The human element of security can cover both unintentional human mistakes, as well as deliberate attacks by perpetrators. In this research, the focus lies on intended attacks that may exploit unintentional mistakes, such as divulging information to a stranger that asks for it, but not unintentional accidents such as pouring coffee on a laptop. This is because controls against mistakes are not useful in preventing intentional attacks, but controls against intentional acts can provide protection against both intentional and unintentional attacks.

There is a distinction between what is technical, and what we consider human related security in general and social engineering in particular. For example, it could be claimed that a virus exploiting bad code in an operating system is exploiting a human weakness; poor programming. However, in this thesis, social engineering is considered from an aspect of attackers intentionally using manipulative techniques as the main method of attack. Consequently, phishing is included to some degree, and regarded as a subset of social engineering, but we do not consider that viruses exploiting human weaknesses as a means of spreading, such as the well known e-mail viruses, belong to social engineering in this context, even if they use some of its techniques.

There is a distinct possibility that gender issues can play a part in social engineering, but they have not been a focus of this study. While the statistics are collected in some of the studies, we draw no specific conclusions based on gender, although this an interesting area of study in the future.

Furthermore, although the legal implications of social engineering are an interesting area, they are beyond the scope of this thesis.
Results and Contributions

This research has used a rather broad approach which has resulted in useful and new knowledge, suitable for a wide audience in both academia and among security professionals. The approach can also be used by future researchers, who can initiate further research based on this thesis. The results, in the form of papers, have all been published or presented in peer-reviewed academic conferences, journals or books.

Our work contributes with a merger of the aspects that enable social engineering, both from a social psychological, and a descriptive perspective that uses a model to describe the actions of the victim, the attacker and the defender. We also recommend how to carry out social engineering penetration testing, as well as suggest methods of protection against social engineering attacks. In addition, a novel future threat, in the form of Automated Social Engineering is described. The contributions are described further on page 76.

Related Research

This section presents related work in the area of information security.

There are a number of specific problems associated with humans and security in general and social engineering especially. In this chapter, the three main areas of interest for this research are discussed. The research has been divided into these areas on the basis of previous work, experience, ongoing literature studies, as well as informal discussions with a number of information security professionals.

One of the problems associated with this area of research is that there has been little interest in the area in the past. Björck and Yngström’s (2001) study, for example, attempted to classify research in information security.

In their study, they classified the papers accepted by the “IFIP World Computer Congress” (SEC 2000) and placed their contribution and research area in a matrix. The Y-axis deals with whether or not the contribution is primarily focused on being empirical, or theoretical, and the X-axis consists of three areas. The technical area, for example, deals with computer hardware and software, communication protocols, as well as cryptographic algorithms and technical evaluation methodologies. In the formal area, they place research dealing with procedures to formalize human behavior in the information system. Examples include information security policy, the legal system, and so on. In the informal area, there is research about informal human behavior, for example, social relations, ethics, and security implications of intrapersonal communication. The results are illustrated in Figure 4. The dots within the dotted line represent research aiming to move from one level of abstraction to another, for instance, implementing a theory in the empirical world.
The research conducted in this thesis has mainly dealt with the informal area, what Björck and Yngström (2001) call “security implications of intrapersonal communication”. A large part of our research deals with the empirical world, as we believe there is a need for a practical understanding of the risks and procedures, but at the same time there is also a need for models that can explain them. Our intended research position is indicated by the large red dot in the model above.

This research position is further motivated by the conclusions of Björck and Yngström (2001), in which they argue that the human element of security is one of the most important. They maintain that while 80 % of all information security research is currently being carried out in the technical domain, resources are perhaps better spent in the formal and informal domains where critical problems can be found.

In recent years there has been an increased interest in this research area, with books written on the subject and special conferences that focus on the human element, exemplified by the International Symposium on Human Aspects of Information Security & Assurance (HAISA).

The three research areas, understanding, measuring and protecting are presented below. They are discussed and compared to some of the state of the art research today, together with a conclusion of each area.

Understanding
The research framework of this thesis describes social engineering and Phishing, two of the major areas of what is often attributed to be the human element of security. They are examples of attacks aimed with deliberation at primarily humans and human weaknesses. There are, of course, security
flaws related to humans that are without deliberation, for example, those not
carried out by attackers, but instead by unconcerned and unwitting users.
Examples of such flaws can be a user that mistakenly destroys the wrong
back-up CD, deletes the wrong file, and so on. In this research the focus is,
however, on the deliberate attacks against humans, not the unintentional
mistakes users can make.

**Previous Work in the Research Field**

Much of the material presented in this thesis describes parts of what consti-
tutes the human element of security, the major impact on social engineering.
There is ample material to be found regarding Phishing and social engineer-
ing; the problem is that most of the material is not of adequate academic
standard. Most articles, and so on, are from contemporary magazines, web
pages, and other such sources. Those of an academic standard tend to use
the same references as the more contemporary ones, meaning that the factual
basis on which the field is grounded is quite narrow. It is difficult to over-
look the tremendous impact that Mitnick and Simon (2002) have had on the
field, and little is written that is not to some extent covered or mentioned in
their book, even though the field nowadays spans several hundreds, perhaps
thousands, of information sources. This small set of foundational references
does not automatically mean that the quality is low, but it can potentially be
a problem since the research area is narrow and few researchers are working
in it. It is important to continuously remember to check sources and to be
critical when reading, especially since a lot of the sources are highly anec-
dotal web pages.

The typical perpetrators of social engineering attacks are described in this
thesis on page 32. In the field of criminology, much work has been carried
out to determine the types of individuals that become criminals. Within the
study of deviance, there are ample theories explaining why people turn to
crime. Most relevant to this area of research is perhaps the Differential As-
association theory developed by Edwin H. Sunderland (DeMelo, 2007). In
Sutherland’s differential association theory, the view is that criminal beha-
vior, both techniques and values, is learned from social interaction with oth-
ers. Once a potential perpetrator has learned the techniques, be they simple
or complex, the values supporting the crime can be learned from just about
anyone (DeMelo, 2007).

It is unavoidable that a research area such as this one describes the tech-
niques actually used for social engineering attacks, which can then be used
by the aspiring criminal, in cooperation with a social network supporting
criminal actions, to become a criminal. This is, however, not anything un-
usual for this particular field, but a dilemma shared with much of informa-
tion security research. It is better that we all know and understand the flaws, rather than only the attackers.

A description about what makes humans susceptible to influence from others is given in the Book Chapter of part II below. There is a wealth of information on these subjects, although most often not from an information security perspective, but on marketing or other areas instead. Prominent authors in the field are Cialdini (2001) and Levine (2003). These authors, and many others, write about social psychological aspects of deception and the ways we influence each other. From the literature on deception in general, we learn of several ways deception can occur. In the Book Chapter of part II, we use that knowledge in an information security and social engineering setting, by describing the deceptive methods used in typical social engineering attacks. Finding research in the area with an information security setting is rare, but in one paper (Jordan & Goudey, 2005), an interesting taxonomy of twelve categories of social psychological vulnerabilities is revealed. This taxonomy is used to describe a selection of current attacks by malicious code and the social engineering areas they exploit. With regard to more contemporary sources, we discover Harl’s (1997) influential presentation that describes how social engineering can be used by an attacker.

With regard to deception, and techniques that educate about deception, there is a surprisingly large amount of literature that seems to be unknown to most researchers in the field of social engineering. Grazioli (2004) writes about different theories that describe deception, and focuses on the “Theory of Deception”, ToD.

“the Theory of Deception describes the information processing involved in both deceiving and detecting deception, [...] the Theory of Deception states that individuals detect deception by noticing and interpreting anomalies in their environment in light of the goals and capability for action that they ascribe to others with whom they interact. The interpretation process is triggered when individuals notice inconsistencies between their experience and their expectations about their experience.” (Grazioli, 2004, p. 151).

This theory is interesting, as are other, conflicting theories of deception, such as the Interpersonal Deception Theory, IDT. The difference between the two theories, according to Grazioli (2004), is that ToD would be more suitable to use in a context with more personal contact (therefore social engineering), while IDT is more aimed at communication with little personal contact (therefore Phishing).
Conclusion on Understanding

We have found notably little research carried out on the human elements of information security. There is, however, interesting and relevant research in other fields than information security. Furthermore, there is also much potential for learning from psychology, social psychology and sociology.

Measuring

Growing up, this author was raised with his father’s favorite quote from Lord Kelvin: “To measure is to know”. Perhaps it can be argued that it is the only way to fully understand the impact, and the relevance, of the research area. It is rather easy to measure, and thus to understand, the impact, for example, that the deployment of an anti-virus software has on an organization. One of the most obvious effects is, hopefully, the disappearance of viruses, and logs that probably display significant numbers of thwarted attacks, and updates, as well as successful recoveries carried out by the software. Something concrete has a value that is easy to grasp, and easier to market. With regard to humans, it is harder to measure, both the inefficiency and efficiency of security measures. Another fact that can be troubling is that while technical attacks tend to be on a large scale, for example, viruses or attacks against firewalls, the attacks aimed at humans are often on a smaller scale, with a greater focus on individuals. This makes collecting relevant statistics difficult, thus making it hard to fully grasp the scale of the problem.

Previous Work in the Research Field

One approach to measuring is sending out fake Spear Phishing e-mails to the organizations’ own users. This has been done by both the State of New York (Bank, 2005), and the US military school, West Point (Dodge & Ferguson, 2006). In the West Point case, students were sent an e-mail from a person claiming to be a Colonel, ordering them to click on an attached link to verify their grades. This approach received 80 % compliance among the students. In the case of the State of New York, 15 % of the employees tried to enter their passwords into a special online “password checker” after receiving an e-mail from the “Office of Cyber Security and Critical Infrastructure Coordination”, urging them to do so. This was after they had received educational materials on security. A follow-up study several months later, using a similar approach, received a lower compliance rate (8 %).

This approach is interesting, but it creates a new set of problems, both ethical and practical. There is a possibility that the trust between the organization and the employees can be affected, and there are also other ethical questions. Still, it may be a very efficient method, not only for diagnosing a level of insecurity, but also for educating the users. If they do submit information,
and are criticized for it, they may become inoculated against further, real attacks.

There have, of course, also been other academic studies on Phishing reviews. A highly publicized and interesting study was done by Jagatic, Johnson, Jakobsson and Menczer (2007) in which a highly specialized and targeted Phishing attack was attempted against university students. The experiment was a stunning success, if seen from the perspective of a potential attacker. The test using a classic Phishing attack was 16% successful, but the more advanced attack was 72% successful.

While the Phishing study by Jagatic, et al. (2007) in itself is highly interesting, the debate that followed with its highly vocal complaints and articles in the media criticizing the study after its publication, as well as the ethical and emotional dilemmas, are also interesting. This once again demonstrates the necessity of a strictly ethical approach while conducting these kinds of studies, as there is an inherent problem that with large scale deceiving of users they may feel violated by the test. Judging from the reactions in many of the cases where users have been deceived, there are often strong opinions against using these kinds of tests, based on the feelings of the individual subjects. The strong interest in conducting Phishing research in that particular study, and the experiences that were gained, led to the publication of an excellent paper on how to perform fraud experiments (Jakobsson, Finn, & Johnson 2008). However, the article was published late in our research process.

While large scale attacks using Phishing techniques to measure a level of insecurity are quite manageable because it does not take much longer to send 10,000 e-mails than it does to send 10, with social engineering attacks it is different. It is, obviously, not feasible to carry out a social engineering review on every single employee. One reason is that employees would probably notice if they all suddenly started to get friends who wanted them to reveal information. Another reason is the fact that it would take a tremendous amount of time for the penetration tester to properly social engineer a large number of people individually. The ethical complications would be even greater than with those for Phishing attacks, as a social engineer should try to develop a relationship with the mark, preferably over a long period of time. Therefore, large-scale social engineering reviews are probably unfeasible for most, if not all, organizations.

The ethical problems connected to social engineering reviews are also discussed at length in Hasle, Kristiansen, Kintel and Snekkenes (2005), and especially in Jakobsson, et al. (2008). It is important to consider that the subjects in these tests are humans and not machines. The impact of a review on the individual must be considered and minimized, and anonymity ensured. A novel proposal to avoid the dilemmas associated with reviewing individuals,
that are also discussed in length, is suggested by Vroom and von Solms (2004). They actually propose focusing on reviewing the organizational culture rather than the individuals. While this is an interesting approach in theory, we find it hard to develop a practical deployment using that approach for reviewing. Nevertheless, the discussion and arguments against individual reviewing are relevant and interesting.

In our early research, (Paper 1, Part II), we tried a slightly different approach to this problem. That study tried to test users’ awareness and degree of susceptibility to common social engineering attacks, and if a quantitative approach to penetration testing of social engineering could be used. By conducting a quantitative study using the false cover of studying “micro efficiency”, an organization with above average skilled users was surveyed on three classic social engineering cons. The results indicate that the approach could be useful as a part of, or a separate reviewing technique. The human element was not merely vulnerable, but vulnerable to the extent that it shades most other security areas.

By using a web based study and false pretences, the people assessed (highly qualified IT-consultants) were asked a set of questions in a different context than security. The results can perhaps be significant with regard to which extent the organization is vulnerable to social engineering. This approach shares some of the dilemmas discussed with Bank (2005) above, but it is at least a practically feasible method of conducting social engineering reviews on a large scale in organizations.

The dilemmas associated with penetration testing and social engineering are also discussed by Barrett (2003), who concludes that it is preferable to use a review style which has results and objectives that are clear and can be accepted by both subjects and company. Furthermore, while Barret (2003) argues that reviews should not lead to discipline or dismissal for the individuals, nothing more concrete than that is discussed.

Another academic approach to social engineering review was taken by Hasle, et al. (2005), whose approach to social engineering penetration tried to test a larger population. They performed two tests. The first was a survey where the users were asked to submit their login information to authenticate if they had won a prize; the second test was an e-mail which triggered a login box. According to their findings, approximately one quarter of the users could be tricked into submitting their passwords. A more recent study (Bakhshi, Papadaki & Furnell, 2008) produced similar results; about one quarter of the users were easily deceived by a Phishing attack.

A traditional approach to social engineering reviewing is argued by Jones (2003), who advises the reviewer to actually conduct social engineering attacks on the users. A similar approach is used by Orgill, Romney, Bailey, Orgill
who actually have a person trying to manipulate his way to gaining information from the employees of the tested organization. This is done in two parts. The first is to let the person wander around submitting employees to a written questionnaire with questions on security, logins, and so on, and in the second part the person tries to gain physical access to the perimeters. Both approaches are disturbingly efficient; 81 % of the subjects asked gave their login names, and 59 % also revealed their passwords. Very few employees asked for identification or questioned the reviewer. The auditor also managed to obtain unrestricted, physical access to the building.

Dalrymple (2005) describes the highly successful internal review on social engineering conducted by the IRS, where a select number of users were called, under some pretext, and asked to reveal their passwords, which 35 % of the employees complied with.

The classic approach, as used by Ogrill, et al. (2004), definitely has its uses, but the flaws are that it is costly (since it takes a lot of time to perform), and the employees can perceive it as being more ethically questionable than a more indirect form of deceptive study. It is also possible that the subset of users who are tricked will not tell their colleagues about it. If everyone in the organization is told about the study, it is possible that the users who were not reviewed will then keep to the “lie detection” bias (Marett, Biros, Knode, 2004), feeling that they, themselves, would not fall for “tricks like that”.

Information Systems Audit and Control Association, ISACA (2004) provides a list of areas that should be tested when doing a social engineering audit. They suggest the four areas to test are:

- Test of Controls – a general overview of the organization, can give basic knowledge usable in further tests.
- Telephone Access – to use a set of well known attacks to test the organizations’ resistance to attacks over the telephone.
- Garbage Viewing – to see if there is any sensitive information being thrown away (dumpster diving).
- Desktop Review – Check the user’s workplace. Merge the data from the social engineering audits with other audits.

The guidelines given by ISACA (2004) present a basis for testing that could be perceived as ethical, at least by the organization, but the attacks suggested and the general set-up seems, in our opinion, to provide little data that can actually be useful, and the approach, while nicely structured, is slightly shallow and incomplete.

A related study was done by Grazioli (2004) who studied the impact of deception on MBA students trying to evaluate whether to trust a web-site or
not. This study was mostly centered on deception, but proposed testing against deception cues in order to discover to what extent it was possible to influence the students by deceptive tactics. The findings were that as a group, the students were unable to discriminate between deceptive web pages and genuine ones. This approach could probably be adapted for testing if users are able to discriminate between genuine requests for help or assistance and malignant ones.

**Conclusion on Measuring**

One of the reasons for the focus on technical solutions to the security problem is perhaps that it is easy to see the benefits of using a product against a measurable threat. We believe that there is a need for similar methods of presenting the risks associated with humans. There are a couple of different approaches that can be used. The first is to select what one wants to test. If the test should be a broad approach covering a large number of subjects, a Phishing attack would be the most suitable. If fewer subjects should be tested somewhat more thoroughly, then social engineering would be better. Phishing is, in our opinion, basically using social engineering techniques against a wider audience, by using technical means, with less precision, but greater coverage. It is hard to choose the preferred number of the subject group. While a study on a smaller subset may give useful statistics, the fact is that it is still enough with just a single vulnerable employee for the organization to be vulnerable. Furthermore, the ethical implications of conducting extensive tests that attempt to deceive the employees can also be difficult to handle.

**Protecting**

Learning about, and measuring, a problem is interesting, but it is important to also try to find possible solutions to the problem. While the extent of the vulnerability of social engineering is not precisely known, and may never be conclusively proven, there are few arguments against its existence. Consequently, there is a need for protection against attacks on the human element of information security. Currently, the typical recommendation for protection is education, which, for example, Mitnick and Simon (2002) argue for.

**Previous Work in the Research Field**

While conducting a more general case study on the status of information security in the healthcare domain by interviewing persons responsible for information security, it was obvious that education in the field was lacking in most of the subjects’ organizations. One organization had not provided any
security education in the last 10 years, and in none of them was there now an active education program for the users (Åhlfeldt & Nohlberg, 2005).

While education is an important tool to use, it is important not to lose focus on the psychological aspects of the field. A defense against social engineering attacks must take psychology and persuasion into account, and develop that in order to understand, and counter, the persuasive attack (Gragg, 2002).

In the Background Chapter of this thesis, the current state of the art techniques of social engineering are presented, including a thorough description of the interesting “A multi-layered defense against social engineering” by Gragg (2002). The chapter includes a description of the specific educational needs, as well as general guidelines from other sources. In addition, the chapter includes a presentation of protection against Phishing, which describes practical end user measures as well as somewhat more organizational aspects.

There is also an interesting Masters Thesis aimed at the area of education for protection against social engineering attacks, “Fighting Social Engineering - Increasing information security in organizations by combining scenario based learning and psychological factors of persuasion”, by Hermansson and Ravne (2005). In their thesis, the authors test, with some success, scenario based learning on psychological factors of persuasion, and create a software prototype for this. Subsequently, this scenario method was assessed as being more efficient than using ordinary lectures.

While their approach is interesting, we believe there is a risk in focusing too closely on certain methods of manipulation, since the typical characteristic of the social engineer is the adaptability and the flexibility of the attack. Therefore, it is hard to know whether such a strict and controlled model for education would be successful in real life, even though it is successful in the evaluation done by Hermansson and Ravne (2005). Many measures have been used in attempts to prevent Phishing attacks, both novel ones, such as using cartons (Srikwan & Jakobsson, 2008), and variants on Phishing attacks followed by targeted education of the users who “fell” for them, referred to as embedded training (Kumaraguru, Rhee, Sheng, Hasan, Acquisti, Cranor, & Hong, 2007).

Thomson and von Solms (1998) present a novel set of guidelines for information security awareness training that could easily be used for education on social engineering. They actually apply the same manipulative techniques on their students that a social engineer uses on a target in order to educate more efficiently. In this way they gently try to persuade the students into changing their security behavior.

Once again, turning to the field of deception, a couple of interesting studies have been done on educating users in detecting deception. These studies
dealt with an interesting piece of software named Agent99, developed to train military personnel in detecting deception. This software uses a multimedia approach, and is, according to the studies, an efficient way of training users in detecting deception (Cao, Lin, Deokar, Burgoon, Crews, & Adkins (2004), Biros (2005)). Marett, et al. (2004) also evaluate deception training in a military context, and suggest the field should be studied further, as it is promising.

**General Aspects of Security and Education**

Lee and Harley (2002) provide insights into the problems associated with security education, and express some views that education is hopeless, because users do not want to be educated. With this in mind, security education must be “maintained as strongly and vigorously as the technological aspects of the wider policy” in order to be useful (Lee & Harley, 2002, p. 81). However, they do argue that while security education does work if done well enough, it cannot be relied on as a complete solution to the problem. In the experience of Lee and Harley (2002), education works best on lower-grade staff, such as secretaries and administrators, but often fails with engineers and managers.

In an article about education regarding security, Adams and Sasse (1999) provide a set of guidelines for how efficient security education should be performed. Their general idea is to inform and empower the users by guiding them into the right actions.

Conti, Ahamad and Stasko (2005) give another view on how to educate users, which is more aimed at security awareness. Their idea is to train users to:

- Be alert for manipulation.
- Be aware of their own personal weaknesses.
- Take maximum advantage of the abilities in the system to counter these weaknesses.

It is believed that this approach makes the users more protected and resistant to attacks.

Björck (2005) also has some suggestions on the optimal way to educate the users. One of the recommendations is to use examples of previous security breaches. However, it is important that the users understand the rationale behind the security rules, and that top managers act in accordance to the same rules as ordinary employees. One of the conclusions made by Björck (2005, p. 238) is that more focus should be put on information security education, as well as other informal areas of research, such as ethics, awareness and policies.
One novel approach to protecting against social engineering attacks is to educate the users in transactional analysis, and how it can be used to identify "attacker" and “victim” communication patterns. Transactional analysis is based on the works of Eric Berne, and can be used to analyze communication. It is based on every person having three “ego states”, Parent, Adult and Child. In any communication and at any time, one of these is dominant. In any kinds of communications with others, the ego state the communicators are performing in influences the outcome of the communication and reflects on the individuals (Berne, 1996). There is a set of common counterproductive social interactions, from which the most interesting one in this area is the third degree interaction, in which one, or both, of the communicators can get hurt. This can be used to analyze the language patterns of social engineering attacks, and perhaps to train employees to be more resilient to them.

**Conclusion on Protection**

In the area of security education, there is a lot of material, both with regard to traditional education, which requires more time and resources from the end user, and security awareness, something that is quite useful in this context. With regard to assessing what the best approach would be, it would probably be necessary to actually test the efficiency of the approaches, and in order to do that, a metric is needed, leading back to problems discussed in the Measuring section above.

The other methods of protection could also be tested once a metric is in place, but since some of them, like Graggs (2002) “A multi-layered defense against social engineering”, are costly and perhaps overly complicated, only a dedicated organization would be able to employ it.

The smaller, organizational changes that can be made to increase protection are perhaps best employed when educating the responsible personnel, making education the natural first step in building defenses.

**Thesis Structure**

This thesis consists of two parts. Part I is an introduction to the research area and the research questions, how the research has been conducted, as well as a summary of contributions and discussion of the work. The second part contains the published materials; one book chapter and six papers. These are in Part II. A description is found in Table 1.
Table 1. Structure of the thesis.

<table>
<thead>
<tr>
<th>Part I</th>
<th>Chapter 1 Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chapter 2 Background</td>
</tr>
<tr>
<td></td>
<td>Chapter 3 The Research Design</td>
</tr>
<tr>
<td></td>
<td>Chapter 4 Social Engineering and Phishing</td>
</tr>
<tr>
<td></td>
<td>Chapter 5 Research Results</td>
</tr>
<tr>
<td></td>
<td>Chapter 6 Concluding Discussion</td>
</tr>
</tbody>
</table>

Background

This chapter presents an overview of fundamental information security concepts significant to this thesis. This is useful knowledge, especially for the reader not well versed in security.

Information Security

In order to provide a basic framework for security in computing, a presentation of basic terminology and concepts follows, dealing with the classic views on what constitutes information security compared to other security views. There is also a brief presentation of typical groups of perpetrators.

Basic Terminology and Concepts

While the field of information security is a rapidly evolving field of research, the basic concepts do not tend to change as quickly. This section is useful for the reader with limited insight into security, since it describes some of the classic models of what constitutes security. It also provides an argument for our selection of security model for this thesis.

Every part of a system needs well-balanced security. It is only after all the parts of the system have reasonable protection that it can be said to be secure. Historically there have been several terms for security, such as computer security, network security and IT security. Nowadays, the most common term when discussing security in a broader context is information security, as the focus is on the information, which has the higher value, rather than the technology. There are three fundamental terms used when talking about information security (SIS, 2003):

- **Confidentiality.** Only those individuals who are entitled to access a resource can access it. Access may also include printing, and knowing that an object exists.

- **Integrity.** Only authorized individuals should have the possibility to modify the asset. This also includes writing, changing, status changing, deleting, and creating.
• **Availability.** Assets should be available to those who need them when they need them. If someone has access rights to a resource, that individual should be able to access it.

These three terms are often referred to as the “CIA-triad” which is the basis of all security modeling. There have been additions to these terms over the years, of which one of the most common is accountability. Organizations want to be able to audit what decisions a user has made, in such a way that the user cannot deny having made a decision (SIS, 2003).

A different perspective on the CIA-triad and its extensions is the Parkerian Hexad, as proposed by Parker (1998). It adds three new attributes to the CIA-triad:

• **Possession or Control,** which is for situations when the data might be encrypted, but the confidentiality has not been broken. An example of this is the loss of an encrypted USB-memory.

• **Authenticity,** which concerns the correct labeling of information and who is attributed to it.

• **Utility** deals with usefulness; for instance, if all the files are encrypted but the encryption key is lost, the data would not breach any of the other traits in the Parkerian Hexad, but the files would not be useful.

It is important that a secure system incorporates all these aspects, and that the aspects often, but not always, overlap.

![Image of information security hierarchy](image.png)

**Figure 5. The SIS illustration of information security (SIS, 2003).**

Another model for describing information security is the one used by the Swedish Standardization of Information Technology (SIS, 2003). This authority maintains that information security is the protection of information assets, which is achieved by maintaining secrecy, integrity, availability and accountability of information. SIS (2003) illustrates these terms in a hierarchical figure, where the terms are also classified in a ranking order, as illustrated in Figure 5. We argue that this model is suboptimal, especially in the
areas concerning “Administrative security”, which is poorly described. Considering the SIS model of security, our social engineering research would probably primarily belong to “Administrative security”, but would also need to address most other parts of the model. The boundaries are fuzzy as it is apparent that this model was not created with an intention to cover social engineering. The SIS model generally seems to be one more concerned with the hierarchical structure of an information security organization, rather than a useful description of the term information security. In fact, the efficiency of social engineering attacks against an organization that has closely modeled its security according to the SIS-model would probably be high, due the attacks falling “between the cracks” in the structure. One way of addressing this would be to introduce a new section in the model named “Cultural security”, which could include cultural, psychological and social aspects of security. This is, however, outside of the scope of this thesis.

A further problem with the SIS-model is the absence of the attacker in the model. One of the existing models of security that includes the role of the attacker is the ISO/IEC 15408-1:1999(E) Common Criteria model, as seen in Figure 6. Another positive aspect of the Common Criteria model is the inclusion of ownership. The model also includes such fundamental areas as risk, assets, threats and vulnerabilities. It is a very good model to describe information security as a whole, and also has the added benefit of being more useful, in our opinion, than the SIS-model described above.

![Diagram of ISO/IEC 15408-1:1999(E) Common Criteria model]

The problem with using the Common Criteria model in this research is that it has a different focus than what we need. It provides a good general description of attacks and information security, but it is not well adapted to describ-
ing social engineering attacks due to the models broad scope. One example is that owners, in fact, are a risk themselves from a social engineering perspective, which is not described in the model, where they are reduced to simply trying to impose countermeasures. Nevertheless, the Common Criteria model was successfully used as a foundation during the creation of the conceptual models describing key concepts of social engineering that can be seen in this chapter below.

A security model that has a more holistic approach and is thus more useful in this research context is the SBC model proposed by Kowalski (1994), which provides a description of security that focuses on the perspective of the organization and assets, as seen in Figure 7.

![SBC Model](image_url)

Figure 7. SBC Model, from Kowalski (1994, p. 19).

In the SBC (Security By Consensus) model a greater emphasis is put on a holistic approach, thus including the social aspects completely lacking in the SIS model above, as well as in the common criteria model. In the SBC model the owner or user of a system is perceived to create opportunities to become a victim by not protecting the systems they use or own. It is notable here that the perpetrators are not included in the model, due to the fact that collecting enough data on the perpetrators to enable a crime prevention program for IT crime is regarded as almost impossible (Kowalski, 1994).

The Systemic-Holistic Model (Yngström, 1996) was developed in order to address the problem of how to structure and present security knowledge at
an academic level, but to also have a use as a general description of security in security informatics. The Systemic-Holistic Model builds on the same framework as the SBC-model, but has a different scope. It is based on General Systems Theory, Cybernetics and General Living Systems Theory (Yngström, 1996). The idea is to be able to view a system both from small details and from a larger whole aspect with the same model; the overview can be seen in Figure 8. The framework is organized into level of abstraction (physical constructions, theories/models and designs and architecture), the context organization (geographical, space and time bound) and the content subject areas (technical and non-technical areas) (Yngström, 1996). The systemic module is the epistemological part of the model, the methodology of how to understand and use the framework.

Looking at the details of the framework in Figure 9, we see the similarity to the SBC-model above.

One of the differences between the SBC-model and the Systemic-Holistic Model is within the three levels of abstractions visible in the latter model. Each knowledge/subject area is supported by reality or a physical construc-
tion. The second dimension deals with the level of abstraction, that is, how detailed the view of the knowledge/subject area is. The third dimension, context, brings meaning to that particular subject area (Yngström, 1996).

The SBC-model and the Systemic-Holistic Model both not only illustrate that there is a need for a holistic and multidisciplinary approach to security, but also the importance of focusing on more than technical aspects of security.

Perpetrators

Most people have a very specific idea of who the computer criminals are. Accordingly, they are pale, socially awkward teenagers with high IQ’s, low EQ’s and a desire for destruction. They are extremely skilled at what they do, and their competence often surpasses even the most experienced professional. At least that is the way they are perceived in the movies, and, perhaps, how they were at the beginning of the computer era. However, the world has moved on. The motives for the early hackers were to gain access to computer resources, something that had a high value in those days. The goal of the next phase was the gathering of information, and the goal of the current phase is financial gain. This change of goals has also meant a change of perpetrators. Rogers (2000), updated in Wilson (2007), describes eight categories of hackers:

1. The Novice: Often referred to as script kiddies. Limited skills and often uses software developed by someone else.
2. The cyber punk: Young, often male, with higher skills. Often attacks high profile targets. No stranger to vandalism.
3. The Internal: Insiders who use their access either for financial gain or for revenge if they are disgruntled.
4. The Petty Thief: Perpetrators who start as regular thieves, but learn to use technology to increase their earning potential and lower the risks. Often not highly skilled in the beginning, but can acquire skills in the long run.
5. The Old Guard: Regards hacking as a challenge for the mind, and are quite curious. Often very skilled and often also lacking criminal intent. Will share their findings.
6. The Virus Writer: Mostly young males, often motivated by revenge or curiosity, but this is a group Rogers has yet to define.
7. The Professional Criminal: Highly trained, perhaps ex-intelligence operatives, use their skills for financial gain. Seldom caught, and work for organized, criminal groups.
8. The Information Warrior: Motivated by patriotism, they use their skills to disrupt an enemy country.

There are subgroups being developed, but these are the basic types of hackers.

In order to further explain the concept of the perpetrator in a social engineering context, we created the model in Figure 10. This conceptual model, as well as those in further sections of the thesis, was created as a single, large model that provides a conceptual overview of social engineering. The models were verified to the best knowledge of security experts to be valid. From this large model, sections have been used to illustrate key concepts in this thesis. These conceptual models are related in spirit to the ISO/IEC 15408-model that is illustrated in Figure 6, however, they have been adapted to the field of social engineering, as that model’s scope of security is too broad. One example of change is that our term “mark”, could be seen as a subclass of “owners”, specifically the humans, who are affected in an attack. Correspondingly, we use the term “perpetrator” to refer to the “threat agents” that actually conduct the attack. In the same manner “threats” are referred to as “attacks” in our model, as our scope is far less general and instead specifically focused on social engineering attacks. The term “Assets” is the same in our conceptual models and in the ISO/IEC 15408-model. We chose to use the terminology common in social engineering rather than the more general terminology used within the ISO/IEC 15408-model.

One further difference is the level of detail. As our conceptual models are created specifically for social engineering, they cover far more details than those offered in the ISO/IEC 15408-model. For instance, the model in Figure 10 covers the Perpetrator in great detail, and also includes such aspects as the criminal organization and classic criminological traits. Our conceptual models do, however, chiefly match the flow of the ISO/IEC 15408-model, even if specific social engineering terms and concepts are used.

![Figure 10. Conceptual model of the perpetrator.](image-url)
An aspiring computer criminal must possess three qualities (Pfleeger & Pfleeger, 2003):

- **Method.** He or she must have the skills and tools and other necessary resources to perpetrate an attack.

- **Opportunity.** A perpetrator must have the time and the access to perform and succeed with an attack.

- **Motive.** There must be a reason for a perpetrator to perform an attack on the system.

If any one of these factors is not available to the criminal, the attack will never occur. The problem is that knowledge about systems and methods of attacks are easily obtainable, and since most systems today have Internet access, attackers often have an opportunity. Motives are diverse. Some carry out attacks to steal money, or specific data, while others do it for the challenge and the fun. There are also those that do it because of revenge (Pfleeger & Pfleeger, 2003).

The criminal culture, as discussed by Ferrell (1995), can be seen as the major factor determining crime. In fact, one of the flaws of traditional criminological reasoning is that the contemporary culture is sometimes neglected in the consideration of criminological analysis. The criminal subculture spans more than simply proximity, something that is available almost anywhere in a connected world, it also concerns motives, drives, rationalizations and attitudes, as well as certain appearances, group specific language and self presentation, and style (Ferrell, 1995).

In order to be able to perform attacks, the perpetrator must have knowledge about what kinds of attacks are possible, the method. Some attacks are obvious, and require no great cunning or planning, while others require certain skills or knowledge as well. There are three basic ways of acquiring this knowledge. The method may be known in advance, one can search for it with the specific intention of using it for attacks, or it may be found by chance. The perpetrator can discover an attack method that works well, on the first try, or a book or text describing attacks without having any prior intention of carrying out an attack. It is notable here that Sunderland’s Differential Association Theory (DeMelo, 2007) states that once a potential Perpetrator learns the methods required, he or she can easily get the required motive from just about anyone. Thus, by learning the necessary methods, it is probable that the perpetrator will also pick up the motives needed.

While the potential motives for attacks are many, the majority of them seem to fit into certain categories. They are either carried out for financial gain, or information, or for revenge against someone or something. They may also be done just for the fun of it, entertainment, or for sabotage purposes. An in-
creasing trend in recent years is attacks that support certain values, a kind of political hacking.

When the perpetrator knows both how and why something should be attacked, an opportunity is needed. We have made the following distinctions among these:

Opening: An opening can either be known or assumed. This is a weakness or a specific opportunity that the perpetrator knows about. For instance, the fact that it can be assumed a credit card company knows about credit card numbers. However, the perpetrator can also have prior knowledge, either from his/her own experience or from others, about certain weaknesses. An example would be a perpetrator who in his/her previous career has learned about a certain weakness.

Random: A perpetrator can choose to carry out random attacks systematically, "trial & error", for instance, by calling a set of phone numbers while searching for a specific person. A perpetrator can also just conduct an attack based on a (mostly) sudden random impulse.

If a perpetrator has prior knowledge about an organization, perhaps from a previous attack (or knows someone who has), it is easier to use a "step n+1" attack, where prior knowledge is used. An organization may, for example, have a reputation of being easy to attack, or having things of great value.

When the perpetrator has all of the above, the only thing missing is the means. The first of these needed is the skill to carry out the attack. Skills can comprise influence techniques, programming knowledge, or simply the desired language. No matter how skilled the perpetrator is, if he/she does not know the language of the target, an attack is very difficult. Purely technical means are the communication channel used for the attack. The basic set includes the telephone, e-mail, www or other network communication, such as instant messaging. Uniforms that are used by the perpetrator also constitute means. In addition, time to perform and prepare is also necessary. All of these means can, however, be bought using the means of funding.

There is increased suspicion that many of the perpetrators have ties to organized crime, thereby making it easier for them to acquire means, method and opportunity (Hansell, 2004).
The Research Design

This chapter describes how the research was planned, conducted and which methods were used.

The Research Strategy

The aim of this research, as well as the previous work, is to try to cover the research area as completely as possible, while still maintaining a focus on information systems. It is easy to become lost in details not quite relevant to the research area. In order to maintain a focus during the process, certain delimitations must be made.

The intention with this research was not to base it on certain case studies or a single organization, but to try to achieve general knowledge, and to cover as wide an assortment of organizations as possible. This gives a broader understanding but also exposes the research to the vulnerability of being too broad to actually offer useful results, due to the variance of the studied organizations. This was addressed by a careful selection of the organizations that were studied, as well as contrasting research where possible.

The focus was on small to medium sized organizations. This focus is due to the different situations facing smaller organizations compared to major ones. It is also a delimitation which was made because of the problems associated with getting major organizations involved in these kinds of studies. This delimitation mainly affected the areas dealing with prevention and measuring, as the area about knowing remains basically the same regardless of the size of the organizations that are studied. We also tried to study major organizations to provide information and a broader understanding of the field.

There was little possibility of covering the whole field of the human element of information security, since this includes several research disciplines. It is unavoidable that there is a need to learn from other fields of research, such as sociology, psychology, and so on, while still maintaining the focus on information systems.

One problem is when can the area be said to be sufficiently studied to be able to draw any final conclusions. The easy answer is probably never, due to the complexity of the field, but by conducting studies that are sufficiently broad from several viewpoints, a valid contribution can be made.
Data Collection Techniques

In order to gather data from the real world, a selection of techniques was used. We mostly conducted interviews and surveys, but also observations and prototype testing. The interviews were all semi-structured (May, 2001) with a predetermined set of questions, but we also asked follow-up questions where and when needed. This is a common approach in qualitative studies. In most cases, the interviews were recorded digitally and then transcribed, but in some cases notes were taken during the interviews instead. There are advantages to both approaches. When taking notes during the interview, there is the risk of missing pieces of information for the coding process. In addition, it is hard for one interviewer to both ask questions and take notes at the same time. However, taking notes during the interview does reduce the workload associated with transcribing recorded interviews.

The surveys used in this study were both traditional ones, in which we asked people their opinions, and some that were conducted using false pretexts. This caused some ethical concerns, but in all the studies and tests the anonymity of the subjects has been a major consideration. The surveys were all done digitally over the Internet in order to create cost and time efficient studies that reached as many recipients as possible. The digital surveys conducted in this thesis have worked satisfactorily.

The observations were carried out during the development of the management information system. In this case we actually watched, and recorded, the subjects trying to use the interface in its various stages. Notes were taken in a task log and then used to improve the interface in the next step.

The penetration tests were mostly carried out either with interviews or surveys, but one test consisted of an actual penetration test using Phishing. When this test was created, the highest possible levels of anonymity were assured for the subjects, and any data they were tricked into submitting was guaranteed not to fall into the wrong hands. This is described with great detail in Paper 6, Part II.

Research Process

In Figure 11, a broad plan can be seen, mostly focused on the order in which the material was completed. The plan also provides an historical view of the order of completion of the previous material. The work has mainly been conducted in parallel, and knowledge has been collected in all areas throughout the project.
This research was conducted in parallel with working at an information security company, The Logic Planet AB. The research process started with a number of mandatory courses required for the PhD, as well as several optional courses. These were within risk management, information security, law, ethics and criminology, and so on. All in all they provided a good background and understanding of the field of research. Together with input and considerations acquired at conferences, symposiums, workshops, and so on, as well as the early papers, this constitutes the background of the thesis.

A literature analysis not only consists of reviewing the literature, but also an evaluation of the knowledge gained from seminars, conferences, and so on, as well as the daily work as a security specialist. This has been carried out in parallel to the writing of papers.

Using the classification presented in Chapter 1.4, the planned and the completed papers have been added in accordance to the position we considered appropriate. Some minor position changes have been made in order to make them legible. Most of the research has been done in, or near, the informal research area with an empirical focus, as shown in Figure 12.
When the contributions are matched against the three research objectives, we obtain an image showing the coverage of each, as can be seen in Figure 13.

While some of the contributions are positioned in one single area, most of them actually cover two, or in one case, three areas. Exactly how the division has been made can be argued; the focus here has been on which area the main contribution is in.
As the cycle of deception is one of the major contributions of this work, some effort has been made to validate this further than what is presented in the included papers (Papers 3 and 5, Part II). Two different approaches were used. The first was interviews with three security experts, one of whom has a PhD in security, another is a researcher with twenty years experience in military information security, and the third is a researcher and teacher of information security. The subjects were selected due to their interest in the human aspects of information security. The interviews were conducted on the telephone, after the subjects had been given a document describing the cycle of deception. They were then asked to answer questions about the model: did they consider it to be useful, could they see any other uses for it, was the model complete, should some aspect not be included in the model, and could it be used to improve security in general. The complaints the three experts raised mostly concerned issues related to the presentation of the model (it was unclear where it started) as well as on how it was connected to the “big picture” of security. There were different views on the extent of the generality of the model; two of the subjects found it to be useful for a far broader set of crimes, while one found it useful specifically for social engineering due to the wording in it. The subjects all felt that it could be useful for teaching about social engineering, but also to prepare defenses and to investigate attacks. In general, the subjects found the model to be useful, relevant and that it contributed to the overall knowledge in security.

As the model was created with information security in mind and mainly security professionals have discussed it, we wanted a group of professionals with a good understanding of deception, but with little knowledge of information security to examine it. There are some professional groups that work extensively with other people in relationships where one part can benefit from deceiving the other. Examples of this include the police force, lawyers, medical doctors and social workers. We chose to study social workers since they work with both adults and younger persons, in different kinds of situations, and they have a good knowledge of psychology, criminology as well as social psychology from their education. The social workers that took part in the seminar are specialists in questions related to younger children and are regarded as some of the best in their field. The model was presented verbally for the group, consisting of four experienced and trained social workers. The model was presented to them and they were asked whether they felt it was useful and reasonable according to their experience. The general consensus was that the model did explain what happened when someone was trying to deceive them, but also that it gave a reasonable description according to their experience. They did note, however, that, in a short presentation, it was somewhat difficult to understand the model and that many of the deceptive attempts they are exposed to are of such a low degree of complexity that the attackers in those cases, mostly persons with substance abuse problems,
hardly spent time developing any kind of relationship but went directly to
the attack. In some cases, involved parents may try to deceive a social work-
er in a manner in accordance to this model, for example, in custody conflicts.
They also mentioned that this model could be the basis for education on how
children can become victims to deceptions online.

Research Documentation
As an important part of the research process, papers were written and pub-
lished in peer-reviewed conferences, journals or as book chapters. How each
paper relates to the individual research areas is described in the research
process above. The papers included in this thesis have all undergone minor
changes and updates, mostly in order to conform to the thesis template.

The following six papers and one book chapter are included in the thesis.
The papers are presented chronologically in the order that they were written.

Paper 1  Social Engineering Audits Using Anonymous Surveys –
Conning the Users in Order to Know if They Can Be
Conned
Marcus Nohlberg
In Proceedings of the 4th Security Conference, Las Vegas,

Paper 2  User-centered security applied to the development of a
management information system.
Marcus Nohlberg and Johannes Bäckström
In Information Management and Computer Security vol. 15,
issue 5. ISBN: 978-1-84663-696-7

Book Chapter 1: Why Humans are the Weakest Link
Marcus Nohlberg
In Gupta, M. and Sharman, R. Social and Human Elements in
Information Security: Emerging Trends and Countermea-
sures, IGI Global, Hershey, PA, USA. ISBN: 978-1-60566-
036-3.

Paper 3  The cycle of deception - a model of social engineering
attacks, defenses and victims
Marcus Nohlberg and Stewart Kowalski
In Proceedings of the Second International Symposium on
Human Aspects of Information Security and Assurance (HAI-
Paper 4  **Non-Invasive Social Engineering Penetration Testing in a Medical Environment.**
Marcus Nohlberg, Stewart Kowalski and Kerstin Karlsson

Paper 5  **Measuring Readiness for Automated Social Engineering**
Marcus Nohlberg, Stewart Kowalski and Markus Huber

Paper 6  **Phishing with Gifts as Bait: Measurement and Analysis of Phishing Attacks within a University Environment**
Martin Boldt and Marcus Nohlberg
Submitted to the *International Journal of Information Security*. 
Social Engineering and Phishing

This chapter contain detailed descriptions of “social engineering”, as well as Phishing, which is an important type of social engineering attack. The section on social psychology in Book Chapter 1 in Part II, is a recommended read, as it explains many of the reasons why we are susceptible to social engineering.

Social engineering is a technique in which an unauthorized person manages to pose as an insider or an authority to successfully obtain access to information or resources (Kajava & Siponen, 1997). A hacker can use social engineering to access other valuable data to benefit the hacker in further attacks (Hasle, et al. 2005). Mitnick provided our favorite definition in an interview by Tanneeru (2005):

“Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a Web site, which exploits a technical flaw and allows the hacker to take over the computer.”

A social engineering attack focuses primarily on people’s vulnerability, and is based almost entirely on using “the principle of easiest penetration” (Pfleeger & Pfleeger, 2003). The greatest threat is that no matter how secure the system is in itself, it is never more secure than its users (Granger, 2001; Mitnick & Simon, 2002 etc.). Social engineering can be used instead of, or in combination with, threats and bribes. The classic social engineer aims at not leaving any traces, and generally leaving as little of an impression as possible, and thus threats and bribes are not favorite weapons of choice (Mitnick & Simon, 2002). However, foreign intelligence officers, for example, can still use them (Syrén & Malmström 2001).

Social engineering is used because it is often much easier to simply ask someone, a mark (the person being targeted by the perpetrator), for information, than to prepare and conduct a complicated software or hardware attack (Granger, 2001; Mitnick & Simon, 2002).
Models Describing Social Engineering

In the literature, most of the attacks are described using the typical attack cycle as presented in Figure 14.

![Figure 14. The Social Engineering Attack Cycle (Mitnick & Simon, 2002).](image)

The description of this cycle is derived from Gartner (2002a). The first step is to gather information, for example, from public sources, such as phone books, web pages, and so on, or from other, previous social engineering attacks. This information will be used to develop a relationship with the target.

The second step is to develop a relationship by trying to create rapport and using the natural tendency of humans to be somewhat trusting and helpful.

The third step is to exploit the relationship by getting the target to reveal information, such as credit card numbers, passwords, secret information, and so on. This information can be the ultimate goal of the attack, or the starting point of the next stage.

The fourth step is the execution in which the attacker tries to achieve the end goal, or iterates into further cycles. It is possible that attacks consist of several cycles.

A Conceptual Model of the Social Engineering Attack

Another perspective is to look at a conceptual model of the typical attack as in Figure 15.

![Figure 15. A Conceptual model of the social engineering attack.](image)
The attack is performed by a perpetrator using a certain method and a specific type of attack against a mark. The aim is to acquire something of value possessed by the mark. Every attack has one or more time points, based on whether or not the attack can be carried out again, or if the deception is a long con with several points of contact. The different kinds of attacks are described in more detail on page 53.

The Cycle of Deception

One of the contributions of this thesis is an improved set of models, describing social engineering, named “the Cycle of Deception”. Although this model and its origins are described in greater detail in Paper 3, Part II, a description of the model follows. Its aim is to improve the “social engineering attack cycle”, as described above, making it a more useful model, both for professionals and those interested in learning more about social engineering. It consists of three different cycles; the attack, the victim, and the defender cycles, which are then merged into a model describing the complete cycle of deception.

The Attack Cycle

The attack cycle concerns the behavior of the attacker, and the actions he or she will take in an attack. In Figure 16, the stages of the attack cycle are described.

An attack must have a purpose, a goal, and a plan how to reach it. This is where traditional criminological knowledge becomes relevant. The four classic traits that an attacker must possess are method, motive, opportunity, and means (Pfleeger & Pfleeger, 2003). In order to be able to carry out an attack, the perpetrator must know what kinds of attacks and which methods are possible. Some methods are obvious and require no great cunning or planning, while others require certain skills or knowledge. There are three basic
ways to acquire this knowledge. A perpetrator might have prior knowledge about a method, it could be searched for specifically to use in an attack, or it might be found by chance. A perpetrator could discover an attack method that works well, on the first try, or he/she could chance on a book or text describing attacks without any prior intention of using such information. It is notable here that Sunderland’s Differential Association Theory (DeMelo, 2007) states that once a potential perpetrator learns the methods required, he or she can easily pick up the required motive from just about anyone. Therefore, by learning the methods required it is probable that the perpetrator will also find the motives needed. The criminal culture, as discussed by Ferrell (1995), can be seen as the major factor determining crime. In fact, one of the flaws of traditional criminological reasoning is that the contemporary culture is sometimes neglected in the consideration of criminological analysis. The criminal subculture spans more than simply proximity, something that is ubiquitous in a connected world. It also concerns motives, drives, rationalizations and attitudes, as well as certain appearances, group specific language and self presentation, and style (Ferrell, 1995). Map & Bond: The stage in which the attacker tries to obtain information needed for the attack. This can be done by using traditional social engineering techniques, such as dumpster diving or desktop hacking, or by searching the web for data and studying other open sources of information. However, this information can also be obtained when the attacker befriends the victim or someone with usable knowledge, and uses manipulative techniques to get this person to divulge the information needed, or to “prepare” the victim for the next step. In order to create a deceptive relationship, the attacker uses influence techniques, for example, authority, scarcity, liking and similarity, reciprocation, commitment and consistency, social proof, and involvement (Cialdini, 1993). The influence techniques then exploit certain social psychological weaknesses, as suggested in the taxonomy put forth by Jordan and Goudey (2005). In other words, the victim is manipulated into trusting the attacker. Execute: During the execute-step, the attacker does something clearly illegal, or not allowed, for example, asks the target to submit his or her login information, or sends the nefarious e-mails. Recruit & Cloak: The term, cloak, refers to the actions performed to conceal the illegal activities used in the execution of the attack. Such actions can be to continue with the “friendship” to normalize the illegal activities, some kind of move that makes the victim seem untrustworthy, or more advanced techniques to conceal the crime. In some cases, the victim can be recruited to either work for the attacker or act as the perpetrator’s ambassador/reference. Evolve/Regress: This is when the attacker learns from the process and creates an internal justification for his/her actions. At this stage, there are basically two choices for the attacker. If the process has been successful thus far, the attack evolves, moving into another phase, or, if the results have been unsuccessful thus far, the attack regresses, which means to
either stop the attack or return it to a more basic level in order to try again for success.

The Defense Cycle

The defense cycle describes the general options available to the defender, who could, in some cases, be the same person as the victim, or security professionals, or similar, in an organization. This section is based on the work of Kowalski (2002), which has provided the terms and definitions and identified the flow.

![Figure 17. The Defense Cycle (adapted from Kowalski, 2002), which starts with Deter.](image)

The description of defenses, given by Kowalski (2002), has been adapted to a circle to match the model in Figure 17. Several examples of implementations, which can, of course, consist of many other measures, are given below. The description is based on what the defender must do to successfully provide defenses. For example, having a good, public defense policy, or a reputation of reporting illegal incidents to the police, can deter an attacker. In addition, keeping the availability of sensitive data to a minimum, educating employees about the risks and methods of attackers who try to bond with them, as well as providing a strong policy on how to act, are measures that protect the organization. Furthermore, running a surveillance of the network communication can reveal when sensitive data are being sent or accessed, and having well-educated employees who know when they are being asked illicit questions, helps to detect an attack. Furthermore, making it easy to report social engineering incidents and not attaching any social or professional stigma to such an act, as well as making the employees aware of how they can be manipulated by an attacker, enables a defender to respond to an ongoing attack. Also, knowing the value of your data, reporting attacks and having a well-designed policy, means that a victim can recover from the attack and learn from it. Hopefully the attacker can be found and prevented from evolving and attacking you, or others, in the future.
The Victim Cycle

The victim cycle is focused on the behavior of the targeted person, the individual victim of the attack. A common mistake when analyzing crime is that too much focus is on the attacker, and not enough is on the victim. In fact, many crimes could be more readily prevented by focusing more on the victim than the attacker. The flow is described in Figure 18.

![Figure 18. The Victim Cycle, which starts with Advertise.](image)

By having something of value and making it known, either knowingly or unknowingly, the victim *advertises* its suitability as a target. Furthermore, by *socializing* with the criminal, the victim sets him/herself up for deception, and *exposing* valuables makes them accessible to the attacker. When the actual crime is being executed, the victim *submits* to it, for instance, by revealing the secret information. After the crime has been executed, the victim can choose to *accept* it, for example, through believing that it was not so “serious”, or simply by *ignoring* it, either knowingly, or by actually being unaware of it. The victim can learn from the crime and *evolve* into someone who will be harder to victimize in the future. However, it is also possible that the victim can *regress*, becoming someone who accepts the role of victim and thus easier prey in the future.

The Cycle of a Social Engineering Attack

When the three different cycles are merged and a target in the center is added, a more holistic view of the prerequisites of a social engineering attack appears, as illustrated in Figure 19. One of our theories is that in order to achieve a “successful” social engineering attack, all the steps in all the cycles have to fall into place. The attacker must succeed with the first three steps for the attack to be successful, and with the fourth and fifth to be able to continue attacking in the future. This is based on the reasoning that if the attacker is unable to provide a plan and a method for the attack, it will most
likely fail. Furthermore, if the attacker cannot learn about the potential victim, or perform the attack, it will fail. In addition, if the attacker is unable to conceal the attack, he/she will most likely be caught, and, if the attacker, through internal rationalization, judges that the attack was not a “good” experience, he/she will most likely not continue.

![Diagram of The Cycle of Deception](image)

Figure 19. The Cycle of Deception, which starts with Advertise/Deter/Plan.

The same reasoning applies to the defender. If any one of the steps in the defense cycle is adequate enough to stop the attacker, then the attack will obviously fail or lead to the capture of the attacker. In contrast, if no single part of the cycle can stop the attacker, then the attack will not fail due to the activities of the defender. With regard to the victim cycle, we assume that the victim must submit in each of the sections of the model for the attack to succeed.

Potential Targets

Mitnick and Simon (2002) provide a list of typical targets (in social engineering often referred to as “marks”) for social engineering attacks. They are:

- People who are unaware of the value of information, such as administrative assistants, receptionists, security guards, etc.
- People with special privileges, such as technical support, system administrators, etc.
- Manufacturer/vendor: Organizations that manufacture hardware, software, etc., which could be of interest for hackers.
• Specific departments. This could be accounting, human resources or other departments with potentially valuable information.

In general, typical marks are those who lack a certain insight into security, who work with helping others, have high access rights or specific knowledge, or who have access to something valuable, either information or economic value. This basically means that almost everyone with access to any part of the system is a potential target (Harl, 1997). The marks can also be organizations, but it is notable that in the actual attack, the target is always a human as social engineering is an exchange between humans.

![Figure 20. Conceptual model of the mark.](image)

In our conceptual model of the mark, as seen in Figure 20, the mark has some kinds of knowledge that is used to counter the attack, gained either from personal interest, required education or previous experience. This knowledge can be sorted into two separate categories:

**Every person has a certain security awareness.** Within this awareness, we do not place specific security knowledge, but rather a level of suspicion, gullibility, caution, and an inherent paranoia we find, to some degree, in most people. The factors affecting awareness are discussed in greater detail by other researchers.

**An understanding of the current security policy:** Not every person is affected by a security policy. Some organizations do not have one, some individuals
are unaware of any policy, and others are simply not affected by any kind of policy. However, those individuals actually controlled by policies have some knowledge about them, and also follow them to an extent. While people cannot be expected to rigidly follow security polices, simply understanding them possibly provides a certain level of protection if the policy is well written. One of our preferred methods of describing organizational security work, and thus by extension the policy, and indeed the effects of security in general, from both an organizational, and an individual perspective, is the SBC-model used by Kowalski (1994). The areas covered in the SBC-model are those that should also be included in a security policy, and the aspects that should regulate the education of employees. Any such education should cover both general security and security awareness training.

To build further on security awareness, a person has a certain kind of knowledge of attacks based on human weaknesses. While such knowledge alone does not provide sufficient protection, it can be assumed that knowing about attacks and how they are performed leads to better protection than ignorance. The other kind of knowledge is centered on security information with regard to technical attacks, and includes traditional computer security areas such as firewalls, anti-virus programs, and so on.

Social Engineering Attacks

There is a vast selection of social engineering attacks and some of the classic examples are presented below. In addition, the whole picture is described using a conceptual model of a social engineering attack, as illustrated in Figure 21. In general, an attack can either be a short con or a long con. While a short con is an attack with a single contact between perpetrator and mark, a long con is an attack with several contacts between mark and perpetrator.

![Conceptual model of the attacks that can be used in social engineering.](image)

Each attack can belong to one of three different categories:

*The physical attack* is primarily carried out in the real world. Its intent is often essentially to gather information that cannot be found in other sources.
such as online searches. This kind of attack is sometimes done in order to facilitate another, more advanced, attack. The favored methods of physical attacks are:

- **Dumpster Diving**: In which the perpetrator goes through the mark’s garbage to find information (Granger (2002) and Gupta (2002)).

- **Theft**: The perpetrator can steal physical information, or computers containing the information. This is often not considered information theft, but computer theft instead.

- **Extortion**: This is carried out either by threats or actual violence against the victim or his/her loved ones.

- **Desktop Hacking** (Gupta, 2002): By looking at the office environment, valuable information can often be found. For example, passwords, and so on, might be written on post-it notes and cunningly hidden under the keyboard perhaps. Often the attacker can also see the password by “shoulder surfing”, which is watching while the mark types the password.

*The Social Attack* primarily utilizes social techniques, but can also employ technical means. The main characteristic, however, is that the social attack uses deceptive relationships of some kind to be successful. In order to create a deceptive relationship, a perpetrator uses influence techniques, described in greater detail in Part II, Book Chapter.

The classic example of a social attack is to simply call the mark on the phone, explain that there is a problem with the network and ask the mark for some assistance in a series of complicated, technical corrective measures. When the mark finds that the process is too complicated, the perpetrator offers to help if the mark simply shares his or her login information. This is an example of a direct attack (Mitnick & Simon, 2002).

A social attack can also be based on a pretext relationship developed on deceptive terms between perpetrator and mark. Such a relationship can be based on, for example, romance, business or friendship. Furthermore, quite a lot of research is available on how to easily develop a strong relationship that can be exploited, which is described further in Part II, Book Chapter 1.

A more indirect approach involves the perpetrator getting the mark to ask the perpetrator for help. This is known as a reverse social engineering attack and consists of three phases (Granger, 2002 and Mitnick & Simon, 2002). The first is to sabotage the system and actually create some kind of disturbance. This can be of the simplest kind, for instance, unplugging a network cable, or more advanced, such as creating network interference through technical attacks. The next phase involves advertising, in which the perpetrator lets the mark know that the perpetrator can solve that kind of problem. This can be done by sending out e-mails, handing out business cards, using posters or
similar. Lastly, the solve-phase is when the perpetrator solves the problem, but not without attending to his/her own interests. For instance, the problem might be "solved" if the mark submits login information, or installs a specific piece of software, and so on.

Social attacks can also be carried out using technical means, such as e-mail or instant messaging. In such an attack, the perpetrator would, for example, aim to get the mark to click on a certain link, or install a piece of malicious software (Gulati, 2003).

*A combination of technical and social attack methods* is used, for example, when creating a Road Apple. This is when an attacker leaves a USB memory stick, or a CD with a tempting text (such as “Salaries 2008” or “my nude pictures”), outside a building, to entice a mark’s curiosity into using the item in his/her computer (Stasiukonis, 2006).

We consider that Phishing is a social rather than a technical attack as the most important part of the eventual success of a Phishing attack is the social aspect of it, the message and the context.

**Protection against Social Engineering**

The literature seems to agree on one thing: there is no “silver bullet” protection against social engineering. Education is the most commonly recommended means of protection, particularly if combined with a decent security policy (Hancock 1996; Mitnick & Simon, 2002; Gupta, 2002; Granger, 2002 etc.). Mitnick and Simon (2002) also provide several guidelines about what should be taught to the users regarding social engineering. These include what kinds of attacks can occur, how to detect them, and where to report them. There is also a lesson on not to trust everyone.

Hiner (2002) presents some clear guidelines with regard to education in protection against social engineering attacks, as illustrated in Figure 22:

![Figure 22. Education leads to defense (Hiner, 2002).](image-url)
One should begin by thinking about how the employees in the organization would act “if an unfamiliar person who looked out of place sat down in a cubicle and started working on a computer.” (Hiner, 2002). Then one should consider these three questions:

- Would any of your employees become suspicious about this event?
- Would any employee choose to report it?
- Would any employee know how, and who it should be reported to?

If the answer to any question is no, then further education is needed using the organization’s security policy as a foundation. Figure 22 illustrates the different areas of the policy that should cover each of the questions above.

Other examples of important aspects that should be considered when building a defense against social engineering are (Hiner, 2002):

- Conduct background checks when hiring employees.
- Screen temporary and ancillary workers.
- Establish a clear reporting process for security problems.
- Open the lines of communication between physical security and the IT department.
- Monitor employee behavior patterns for abnormal activities and access violations.
- Lock out terminated employees immediately.
- Create a positive work environment, which will reduce the number of disgruntled employees.
- Publish a formally written, company security policy stating that the IT department will never ask for a user’s password.
- Require ID badges for employees and mandate that an employee with a badge always accompanies visitors.

In Gartner (2002b), there is a collection of suggested protective approaches:

- Have clear, consistent, comprehensive and enforceable security policies.
- The single strongest defense against social engineering attacks is educated employees.
- Establish procedures that eliminate any exchange of passwords.
- Avoid using passwords or authentication questions that an attacker can easily discern with a little research.
- Security plans must be coordinated with physical/organizational security.
Gragg (2002) has a different approach to protection, and proposes “A multi-layered defense against social engineering”. Gragg argues the need for Social Engineering Land Mines, SELM, used together with a defense in several layers:

**Foundational Level: Security Policy Addressing Social Engineering**

The foundation of any security is a thorough security policy (Gragg, 2002). Such a clear policy strengthens the users’ resistance to social engineering, and, if the policy is strict enough, leaves users without any other option than to deny the Social Engineers’ requests. Another interesting point made by Gragg (2002) is that a strict security policy increases the users’ resistance to persuasion because they feel supported by the guidelines.

**Parameter Level: Security Awareness Training for all Users**

Gragg (2002) recommends training for all employees, using the security policy as a basis. The specific issues for protection against social engineering are:

- Know what has value
- Friends are not always friends
- Passwords are personal
- Uniforms are cheap

**Fortress Level: Resistance Training for Key Personnel**

Key personnel (those who work with helping others, especially external parts) should have more resistance training than other users. The two main points for key personnel are that they must be able to realize when someone is trying to manipulate them and that they are vulnerable to such manipulation (Gragg, 2002).

**Persistence Level: Ongoing Reminders**

Results from education and training do not last forever. Gragg (2002) recommends constant and creative reminders of the risks.

**Gotcha Level: Social Engineering Land Mines (SELM)**

A SELM is setup in the system to detect and stop social engineering attacks. These SELMs can be implemented to be used in several ways. Some examples by Gragg (2002) include:
• *The Justified Know It All.* This is an employee who has been given the task of questioning every person he or she does not know why they are on the floor. Besides questioning everyone, this employee should also have a decent knowledge of the security risks.

• *Call Backs by Policy.* Whenever any questionable request is made by phone, personnel should call back and check that the number they are calling belongs to someone with suitable authorization. If, for any reason, a call back is not possible, they should make a security log and be authorized to decline the demand.

• *Please Hold by Policy.* As a social engineer tends to use pressure, surprise or overloading to persuade the target. Therefore, users should be instructed to put any doubtful person on hold for a while, to give the user time to think, and perhaps to discuss the request with a manager or colleague.

• *Key Questions.* Gragg (2002) argues the need for a *three-question rule* (three questions that only the real employees could know, such as the name of certain pets) to use as a means of identification. These should be easy to remember, and available in a database for the personnel. Another means of control is the *bogus question* that implies false knowledge, which the real employee can correct, but the social engineer cannot.

**Offensive Level: Incident Response**

There must be a well-defined protocol to use as soon as a social engineering attack is discovered. This should be part of an incident response unit, which immediately informs the employees that an attack is in progress and what to expect. The unit also starts investigative work to identify the social engineer, and the target (Gragg, 2002).

While Gragg’s (2002) “Multi-layered defense against Social Engineering” in theory provides quite extensive protection against social engineering, it is also a rather extensive commitment for the organization, especially considering the fact that many organizations do not provide any information at all about the risks of social engineering. In fact, the approach may be too expensive and complicated to be feasible.

**Phishing**

Before explaining Phishing further, it is important to examine the difference between Phishing and social engineering. In our opinion, the difference lies within the scope of the attacks, and the delivery. A social engineering attack targets a single, often specifically selected person (or organization), whereas a traditional Phishing attack employs techniques used by spam in order to
target thousands, or even millions, of users. Thereby, one could say that Phishing is social engineering using data-mining. The difference is, however, not always clear. In addition, more sophisticated and precise Phishing attacks, in general, and Automated Social Engineering, in particular, both serve to obscure the differences. In fact, one can argue that social engineering is an important part of most Phishing attacks, as they often, to some extent, focus on deceiving humans (Ollmann, 2004). A simple way to distinguish between them is that Phishing is simply social engineering in combination with the techniques from spam.

In this thesis Phishing is regarded as Jakobsson (2005, p. 3) regards it: “Phishing can be described as the marriage of technology and social engineering”. We consider Phishing to be an attack mainly against the human element, and therefore a subset of social engineering.

What Phishing is

One of the organizations working against Phishing, the Anti-Phishing Working Group, defines Phishing as:

“Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords.” (Anti-Phishing Working Group, 2008).

Phishing typically uses less personal means than a telephone for message delivery, for example, e-mail or instant messages. Phishing is basically deceiving people into believing that someone of authority, and with legitimate reasons, needs their personal information, or that they must install a piece of software. The two primary goals are (Post- och telestyrelsen, 2007a):

- Acquire personal information.
- Get the user to install programs.

Phishing should not be confused with Pharming, which is a technique for misdirecting users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning (Anti-Phishing Working Group, 2008). As this is primarily a technical attack, it is not covered further in this thesis. Spear Phishing
Spear Phishing

Spear Phishing is a relatively new technique that does not use the wide attack patterns of Phishing, but instead sends highly targeted e-mails. The trick is to make the sender seem like someone the mark actually knows, or is associated with. A good method of gathering this data is data mining. While the goal of Phishing is to steal information from an individual, the goal of Spear Phishing is not only to steal an individual’s data, but may also be to gain access to a specific organization’s computer system (Microsoft, 2006).

This specific targeting makes Spear Phishing much more dangerous than ordinary Phishing, and professional attackers probably prefer to use it in order to get financial gains, trade secrets or even military information (O’Brien, 2005).

Spear Phishing could be regarded the “perfect” mix of social engineering and Phishing, and it also seems a lot more efficient and dangerous, than ordinary Phishing (O’Brien, 2005). It uses a higher degree of authority and the technique of the attackers pretending to be someone the mark is associated with. In order to strengthen spear Phishing even further, another context element can be added; that the victim anticipates receiving the message. This is described by Jakobsson (2005). The idea is to send a message that is not only from a person who can be expected to send such a message, but also in a context and time in which the recipient would anticipate receiving such a message. For example, sending a false e-mail from eBay directly after the user has placed a realistically winning bid on an auction site. This can be a devastatingly efficient attack. Similar attacks have been tried using data from social networks to create attacks emulating they are from people the victims know, something referred to as Social Phishing (Jagatic, et al. 2007).

Spy-Phishing

A “Spy-Phishing” attack consists of the attacker sending an e-mail, or a link, where the mark can download or execute a piece of software, which the installs itself on the marks computer, monitoring traffic until the mark visits a specific web-site. When the mark visits this site the software becomes active, and sends the login info etc. to the attacker. It is thus a combination of Spyware and Phishing that Trend Micro (2006) believes will be very common in the future.

Examples of Phishing Attacks

While it has always been a goal of computer criminals to acquire data and access to other resources, the name Phishing does not have a long history. The word is derived from the analogy of fishing for information by using e-mails as lures, and combined with the “classic” hacks “phreaking”, using a
child’s toy to get free access to telephone systems (Trend Micro, 2005). The term was first mentioned online in 1996, and in the media in 1997 (Oßmann, 2004). In the early days, the primary goal of the attacks was America Online accounts, which were then used to trade for other services, such as pirated software (Oßmann, 2004).

Most of the communication channels used over the Internet can be used for Phishing attacks, but the most common examples of Phishing attacks are those conducted by e-mail.

Dear eBay User,
During our regular update and verification of the accounts,
we couldn't verify your current information.
Either your information has changed or it is incomplete.
If the account information is not updated to current information
within 5 days then, your access to bid or buy on eBay will be suspended.
go to the link below,
and re-enter your account information.

[Click here to update your account.]

***Please Do Not Reply To This E-Mail As You Will Not Receive A Response***
Thank you
Accounts Management

Copyright©1995-2005 eBay Inc.

Figure 23. Phishing example – e-mail text (Anti-Phishing Working Group, 2005).
An example of a Phishing e-mail sent to thousands of eBay customers (as well as other Internet users) can be seen in Figure 23. The attackers’ goal is to get the receiver to click on the attached link, which will lead to an official looking but fake webpage (as seen in Figure 24). The mark can try to login using his/her login information, and thus, unknowingly, submit the login information to the attackers.

This example uses several of the techniques often employed within Phishing e-mails, a full list is (Ollmann, 2004, p.6):

- Emails that appear and sound official
- Copies of legitimate corporate emails with minor URL changes
- HTML based emails used to obscure target URL information
- Standard virus/worm attachments to emails
• A plethora of anti-spam detection inclusions
• Crafting of “personalized” or unique email messages
• Fake postings to popular message boards and mailing lists
• Use of fake “Mail From:” addresses and open mail relays to disguise the source of the email

**Web-based Delivery**

By using malicious web-site content, an attacker can perform a Phishing attack against an unknowing mark. This can be carried out either on a web-site run by the attacker, or by embedding code on a third-party site (Ollmann, 2004). The techniques for this described by Ollmann (2004, p. 7) are:

- The inclusion of HTML disguised links within popular web-sites, message boards.
- The use of third-party supplied, or fake, banner advertising graphics to lure customers to the Phishers’ web-site.
- The use of web-bugs (hidden items within the page – such as a zero-sized graphic) to track a potential customer in preparation for a Phishing attack.
- The use of pop-up or frameless windows to disguise the true source of the Phishers’ message.
- Embedding malicious content within the viewable web page that exploits a known vulnerability within the customer’s web browser software and installs software of the Phishers’ choice (e.g. key-loggers, screen-grabbers, back-doors and other Trojan horse programs).
- Abuse of trust relationships within the customer’s web-browser configuration to make use of site-authorized scriptable components or data storage areas.

Other examples of attacks using web pages include using fake banner advertising and obscuring the mark’s destination after clicking on the banners (Ollmann, 2004).

**Instant Messaging and IRC**

As many new clients for Instant Messaging, IM, and IRC, allow for dynamic content, they are likely to be used in much the same way as e-mail is today (Ollmann, 2004). The trend is that IM will be attacked more frequently in the future (Symantec, 2006).
Defense against Phishing

One of the most important tools for strengthening the defenses against Phishing is education (Ollmann, 2004).

There is a lot of focus on informing the users on the proper behavior to avoid being tricked by Phishing techniques. In general, the advice can be summarized into five separate points to remember (derived from Microsoft (2005a), Post- och telestyrelsen (2006b), FraudWatch International (2006), Ollmann (2004) etc.):

- Never reveal sensitive information in an e-mail or Instant Message.
- Be wary of clicking on links in messages.
- Check whether the webpage is genuine or not, and that the information you submit is protected.
- Keep an eye on your account balance.
- Keep your computer updated and use a firewall and anti-virus software.

Even if these tips seem simple, it is apparent that security education has been less successful with regard to providing protection against Phishing. We see examples of problems with traditional education methods (Kumaraguru, et al. 2007) that recommend simulated attacks carried out in combination with targeted education afterwards, aimed at those who need it. This might be complicated by suggestions that if users are trained to look for certain indicators of secure communications, they may more easily fall for attacks spoofing such indicators (Downs, Holbrook, & Cranor, 2006). There are indications that better general knowledge about how the Internet and web works can be efficient in providing resistance to Phishing attacks (Downs, Holbrook, & Cranor, 2007). Other novel examples of Phishing education include the use of comics, as described by Srikwan and Jakobsson (2008). There are also more technical approaches for protection against Phishing attacks. The most obvious approach is using anti-Phishing software, which somehow informs the user whether he/she is at risk or not. Some of the newer web browsers have this built in, and there are software programs that can be downloaded for protection against Phishing.

At an organizational level, as well as a systems administrative level, there are a lot of strategic decisions that can be made to improve protection against Phishing, as discussed by Ollmann (2004). In general, they deal with building an infrastructure that does not lend itself to being vulnerable to Phishing attacks, for example, by employing encryption, digitally signed e-mails, using strong, token-based authentication, monitoring the system, as well as strict host and linking conventions.
As these are mostly technical solutions, they are not covered further in this thesis.

Impact of Phishing and New Threats

Stolen data can have many uses. Credit card information can be used to pur-
chase goods and services, ATM card information can be used to duplicate
ATM cards for the withdrawal of cash. Account information can be used to
steal information or for acting as another user online (Trend Micro, 2006).

Actually making reliable estimates on the extent of the success of Phishing is
complicated, because many of the victims do not know they have been
fleeced (Hansell, 2004). Calculating the real costs is also complicated, as it is
not well known how successful the attacks are. Reasonably reliable sources
mention costs in the area of $1.2 Billion a year in the US alone, and that 57
million Americans had received these fraudulent e-mails in 2003 (Gartner,
2004).

Historic findings indicate a continued increase in Phishing activity. Syman-
tec (2006) reports a rise from 5.70 million daily Phishing attempts in the first
half of 2005 to 7.92 million daily attempts in the last half of 2005. The Anti-
Phishing Working Group (2008) reports an increase from 8829 unique sub-
mitted Phishing reports in December 2004, to 15244 reports in December
2005, and in January 2008 there were 29284 reports.

Symantec (2006) also expects a future increase in Phishing attacks, as well
as an increase in Instant Messaging Phishing attacks. Trend Micro (2006)
warns for the future increase in ever more sophisticated and targeted Phish-
ing attacks. The general trend seems to be that for computer criminals the
motivation for the attacks is no longer fun, or bragging rights, but instead,
economic criminals are carrying out attacks for financial gain (Trend Micro,
2006). There are also suggestions that organized crime is behind Phishing

Why Social Engineering and Phishing Works

There are a number of psychological issues that can be used to create the
perfect pretext for an attack. These are described in more detail in Part II,
Book Chapter 1. In that chapter, sufficient examples are given on manipula-
tive techniques in general, and also on how those techniques can be used by
attackers in a social engineering context.
Research Results

This section describes and elaborates on the results gathered during the research process. In it we combine what has been gained from the individual papers into a greater picture. The results are ordered into the three pillars as illustrated above, but the big picture is also described by synthesized results.

Understanding

Early on in the research process it was not certain that the human element of security in general and social engineering in particular was such a major problem. In the first paper, (Åhlfelt & Nohlberg, 2005) we conducted a case study on systems administrators in health care and it was apparent that the human element was a major problem. After studying the area further, it was apparent that humans share a lot of common weaknesses. These weaknesses have been rather well known in other areas of research, mostly in those dealing with social psychology and in marketing. Our results in this area are the concrete description of how these common weaknesses can be, and are, used in a social engineering context. This is described in depth in the Book Chapter in Part II. We have also used several of these techniques when planning, and indeed when realizing attacks in other research projects, for example, the highly successful attack described in Paper 6, Part II. For the design of that attack we used the findings from the Book Chapter, Part II, in order to create a successful attack.

In order to more fully describe how a social engineering attack works, the cycle of deception was created, as described in Paper 3, Part II and shown in Figure 25. It describes the actions, or inactions, of the victim, the defender and the attacker in a social engineering attack. The cycle of deception can be, and has been, used as a teaching tool to help explain the somewhat complex iterative nature of the social engineering attack, and to give a more thorough view of those involved in the deception.
Measuring

The first problem associated with measuring susceptibility to social engineering attacks is defining what constitutes a good way of assessing social engineering. We have tried several approaches, some traditional and others more novel, each of which has its own advantages and disadvantages. In order to highlight their relative strengths, we have created comparison matrices that are illustrated in Tables 2 and 3.

While there will probably never be a silver bullet approach to measuring social engineering that fits all scenarios, these matrices serve as a starting point when choosing a method of measuring that suits the needs of the organization best.

The matrices have been kept as simple as possible, and the methods are ranked from 1 – 5, of which 5 is the most suitable approach for addressing a particular problem area. The rankings have been chosen from our own experiences as users of the methods and what we have learned from reading about others using similar methods.

The first matrix, Table 2, concerns the results gained from an organizational perspective, using the classic values of Behavior, Attitude, and Knowledge, used by many security researchers, for instance, Kruger and Kearney (2006). The results are ranked on the basis of the information obtained about the organization as a whole. The focus on the whole organization is the reason why “Phishing Users”, for example, is given a higher grade than “Actual
S.E.”, which is simply because it covers far more users than it could feasibly cover with “Actual S.E.” This can be seen in Table 2.

<table>
<thead>
<tr>
<th>Measure using</th>
<th>Read more</th>
<th>Areas measured</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Behavior</td>
<td>Attitude</td>
<td>Knowledge</td>
<td></td>
</tr>
<tr>
<td>Phishing Users</td>
<td>Paper 6</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Deceptive Surveying</td>
<td>Paper 1</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Asking users</td>
<td>Paper 4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Asking managers</td>
<td>Paper 5</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Actual S.E.</td>
<td>Jones (2003) etc.</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

It may be difficult to learn about the attitude of the users when deceiving them, but learning about it is easier when asking them questions. As the “Deceptive Surveying” covers more employees, it is given a higher score than “Asking Users”, even if the interviews used in “Asking Users” result in more qualitative knowledge. The problem associated with both “Phishing Users” and “Actual S.E.” is that they do not provide much information about the attitude; instead they give excellent information about the behavior of the users. The same is true with regard to the knowledge area, where the same constraints apply as with the attitude area.

The second matrix in Table 3 deals with what we consider to be other important areas when selecting a testing method. “User Coverage” concerns the number of users typically included in a test. “Individual Coverage” deals with how well each tested individual’s knowledge is covered. “Expense” concerns the actual cost of conducting a test based on the method chosen. This is certainly a field in which there can, and will, be huge variances depending on the complexity of the measurement, number of people involved, and on how the count is done. For example, should the cost of lost productivity, while a survey is being answered, be included? Should it also include the loss of trust among employees? In this latter example, the focus should be on the credible cost associated with employing some external part to perform the study, based on the man-hours needed to devise and carry it out. This is simply due to the fact that other costs are too individual to calculate in a meaningful way.

The “Ethical Impact” aspect is considered to be the potential trust/distrust problems that can arise from an organization’s own employees after the study. For instance, a highly deceptive study may infuriate the employees, making them distrustful of the organization in the future, while interviews may create a more positive and trusting environment. The “Learning Impact”
aspect concerns how much positive learning the study can generate in an organization. More learning is generated if more users are involved and affected by the study. However, other factors also influence the process, such as the wake-up call that a simulated attack can evoke in the employees. This can happen whether they are attacked themselves, or a trusted colleague is deceived and they are later informed about it.

Table 3. Other important aspects of measuring.

<table>
<thead>
<tr>
<th>Measure using</th>
<th>User Coverage</th>
<th>Individual Coverage</th>
<th>Expense</th>
<th>Ethical Impact</th>
<th>Learning Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Users</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Deceptive Surveying</td>
<td>5</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Asking users</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Asking managers</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Actual S.E.</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

These studies indicate that trying to find the “best” method of measuring susceptibility to social engineering is not meaningful. However, the tables above can be of some guidance. The best method is the one that provides the information needed according to the constraints of the organization. For example, if the budget is a major constraint, a deceptive survey can be devised for quite a low cost. If an actual test on as many users as possible is important, then Phishing is a good choice. However, if only a small group can be tested, or if security is highly crucial and the budget is of no major concern, actual social engineering testing is a good choice.

We believe there are good reasons for those active in penetration testing to try other methods than the small-scale actual social engineering tests that are quite common today. Trying alternative methods is easy and cheap, and the learning process among the users can be activated in novel ways.

Protecting

For many, the single most interesting part of this thesis is the section on protection, as there is always great interest in a silver bullet solution to any problem. At the beginning of this research process, the goal and hope was to find an efficient and simple solution to the problem of social engineering. As the research has progressed, it has become apparent that such a solution is unlikely. The human mind is a fragile and fickle thing. There are some weaknesses, that have been exploited for hundreds of years, which still work well today. While there are certain efficient and simple solutions to specific
kinds of social engineering, such as letting the suspected perpetrator of a telephone deception know that the call is being recorded, the risk associated with these specific preventive measures is that they are limited to a certain kind of attack. This is one of the fundamental problems with most of the protection advice other researchers have given. A summary of protective tips and tricks can be found on page 55 and page 64. An extensive method for regulating an organization in order to protect it against social engineering attacks is the “Multi-layered defense against social engineering” by Gragg (2002). It would probably provide increased protection for those organizations that have the commitment to introduce and enforce it. However, all of these tricks and tips share a common problem. If the preventive measures are generally known, the attackers can circumvent them. An example of this is teaching users to always enter the wrong user-ID and password at the first try if they suspect the site is a Phishing site. This would work very well for a short time, until the attackers became aware of it and started to ask everyone to enter their information twice. It would also provide the victims with a false sense of security; that by following a set of heuristics the attackers will not be able to trick them. This false sense of security may be one explanation for the high rate of susceptibility among the security experts presented in Paper 6, Part II. Thus, teaching the easy tricks may be dangerous. Consequently, we are not able to present a simple solution to all the problems of social engineering, but we can submit some generally good ways of improving protection against social engineering, as well as a set of future possibilities.

The first step towards protection against social engineering attacks is knowing what constitutes them, and we argue that the thesis provides a good starting point for this knowledge. Accordingly, it is probably more efficient to train users than simply to educate them. In order to train them, users must be exposed to attacks and make choices, good and bad, on their own, rather than passively take part in educational programs. One way of achieving this is constantly conducting various penetration tests, such as those discussed above. These will keep the users alert, unless they done to an excessive degree, in which case the users will grow weary of the tests.

One of the most important steps in protecting against social engineering attacks is involving the managers in general and upper level management in particular. This can be facilitated by talking to managers about security in the ways discussed in Nohlberg and Bäckström (2007). It is important to involve them, and a good way of doing this is to adapt a language suitable for that particular audience. An even better way is to use a management information system that provides up-to-date information on all aspects concerning information security adapted to the demands of the management users. Our trials with the prototype of such a system, presented in Paper 2, Part II, indicated great interest in that system. It is notable that many of the
components needed for a management information system are available as open resources, which means that development costs can be kept low.

Involving the managers and trying to test the users are the foundation of protection. Since the attackers are flexible and can adapt easily, it is dangerous to be set in fixed patterns. In addition, there is need for a more holistic approach, which can be found in using the cycle of deception as a starting point for preparing the defenses and understanding the readiness of the organization. This was tested in a study, presented in Paper 5, Part II, with good results. By understanding the consequences of the cycle of deception, non-standard defenses can be devised by each organization. In attempting to address the first three steps of the cycle, attacks can be avoided, and by working on the last two, it is possible to bring the attackers to justice and strengthen the organization in the future. It is also important to remember that security is, at best, regarded as a nuisance among the employees, and, at worst, they loathe it. It is a good idea to find ways to motivate the stakeholders, be they users or management. Examples of good motivation could be financial rewards, public acknowledgement, or, perhaps even, privileges. Users and managers will probably not suddenly be motivated to adhere to security guidelines unless they are given incentives.

Since there are almost always financial constraints to all security work, the cycle of deception can also be used to rank and prioritize security work, and as a tool with which to follow up improvements and measurements.

To summarize the concrete advice on protecting, the following is a set of crucial areas that should be covered:

- Learn about what social engineering is and what general risks you may face.
- Remember that attacks will constantly change and adapt, so there is a risk in training users on methods for spotting deception that are too specific.
- Involve managers and get their support and cooperation. Unless managers care about security and behave securely themselves, it is hard to get the ordinary users involved.
- Train the users and let them experience attack-like scenarios.
- Consider, in a holistic way, the organization’s readiness to face social engineering threats.
- Acquire an overview of the organizational readiness in order to be able to address weak areas.
Concluding Discussion

This chapter contains the discussion part of the thesis, together with some ideas that might be good starting points for further research. Early in the research process, a mind-map was created containing the possible areas associated with the human element of security, as illustrated in Figure 1. That model has been updated with the areas covered in this thesis, as can be seen in Figure 26. The areas we covered are presented in bold text and rounded rectangles.

![Human element of security mind-map revisited](image)

Figure 26. The human element of security mind-map revisited.

Many areas were not examined in depth in this thesis, but covering all aspects was never the aim. Instead, the intention was to use a broad approach to the area, which, we argue, has been achieved in this research. Although
other research areas have been visited, the foundation has been in information security. One of the obvious reasons for not covering all the areas was time constraints, but also that we had insufficient background information to include all aspects in an adequate way. For instance, legal aspects of social engineering are complex and require a deep understanding of legal research. We have attempted to confine ourselves to the areas in which our previous knowledge would be most beneficial.

In revisiting the section of security models, the SBC-model is used to describe which areas have been examined in this thesis, as Figure 27 illustrates.

![Figure 27. The SBC-model (Kowalski, 1994). The white areas have been studied in this thesis.](image)

Most of our work in the thesis has been based in the social area, except for the Legal/Contractual aspect, which has been outside the scope of this thesis. Some technical areas, mainly “Communications”, have also been influenced because of the impact of Phishing attacks and the suggested future threat of Automated Social Engineering. The Applications area has been examined to some extent in our design of a management information system for information security.
Method

The three different areas studied in this thesis cover a broad and relevant section of the field referred to as social engineering. The study of these areas also necessitated the use of a selection of methods, ranging from qualitative to quantitative, as well as from surveys and actual penetration tests to interviews and observations. The decision to use these methods was made consciously because the studied area had not been previously examined to any great extent. It was therefore appropriate to try to study it from as many aspects as were relevant for this thesis. We do argue that using several methods gave good results, probably better than we would have obtained using only a single method. We have worked hard to ensure an acceptable level of ethics in our research, even though the research area itself deals with attackers not concerned with ethics. This has led to some constraints in the research, mostly on the kinds of studies that have been possible, but it has been manageable and not influenced the results in any major way. In a world without research ethics, it is possible that the knowledge levels in areas related to social engineering would be further advanced, but it would be a sad and dangerous world.

Results

The results gained from this research are, in some cases, not surprising, but it is good to have them confirmed. Other results indicate aspects that were quite unexpected. Early on, our hope was to be able to present a set of easy, rule of thumb guidelines that could prevent social engineering attacks. It seems that this was not only a naïve hope, but also something unfeasible. Instead, our results are spread over three different areas, as discussed above.

The first step to improve protection against social engineering is to find a structure for the work. The cycle of deception is an excellent starting point, as most parties can quickly understand it. The second step is to involve both managers and users. Managers can be involved by being informed in a way that suits their interests and needs, preferably by using a management information system. While education is often heralded as the best solution to the social engineering threat, one of the included papers indicates that even highly trained users can fall victim to social engineering, which in that case involved the Phishing technique. If users with several years security training and a personal interest in security can fall for an attack, it is unfeasible to assume that conventional education, which often spans a couple of hours or a day at most, would work. We argue that users should instead be trained by using simulated real attacks, such as Phishing, but they also need to be heard. It is wasteful, and perhaps even risky, not to listen to users. A good way of listening to them is having anonymous incident reporting. An even better way is also carrying out regular interviews with a selection of users,
where they are both heard and informed. This was done in a study presented in Paper 4, Part II, and the results indicate that such a soft approach has its benefits.

It is important to focus on the underlying mechanics of the potential attacks, and address those using the suggestions above. It would be easy for us to provide simple solutions for particular attacks, such as trying false logins and passwords on potential Phishing sites, since being able to login with a fake ID means that the site is a fake. While this is an excellent suggestion for a very specific attack, the perpetrators would certainly adapt their strategy by informing all users that the first login attempt was wrong and they should try again. Suddenly the highly successful defensive technique becomes a dangerous aid for the attacker. Furthermore, it would not be feasible to continue the arms race of “trying faulty logins”, as it would be unlikely that users would attempt more than one false login. In the very nature of security work lies the problem of being a step behind the attackers. Consequently, in this research process, we have attempted to strengthen the knowledge base regarding social engineering that we rely on as security professionals and researchers. More specific examples of defenses can, and hopefully will, be devised from the framework suggested in this thesis.

Contributions

The results in this thesis are an improvement of the general knowledge of social engineering, in both the academic world and among practitioners. We have achieved this by merging knowledge from other disciplines, and by attempting novel approaches to both protection and social engineering reviewing.

The concrete contributions from this research are:

- A description of the socio-psychological factors that make humans susceptible to attacks, see Book Chapter in Part II. This chapter explains how humans can be, and are, manipulated in information security attacks. This chapter is especially useful for those with limited previous knowledge in either social psychology or information security.

- A model describing the cyclical patterns of attacks, defenses, as well as the victims’ actions and inactions. This model can have several concrete uses. For example, it has been used as a teaching aid for educating in social engineering. It has also been used to obtain an overall understanding of defenses and preventive measures for conducting readiness studies. Furthermore, the model can be used to create automated social engineering AI-bots. There is also a possibility that it could be used to model and describe other crimes committed with intent, even if this is outside the scope of the thesis. The model is further described in Paper 3, Part II.
• A set of conceptual models describing certain key concepts of social engineering: the perpetrator, the mark, a general view of the attack, as well as the different types of social engineering attack. These are described in Chapter 2, Part I.

• Recommendations of the different approaches for conducting social engineering penetration testing. These were derived from several methods that were attempted in the real world during this thesis work. The methods used are presented in Papers 1, 4, 5 and 6 in Part II. This is further merged into a comparison on page 68, where recommendations for penetration tests based on different prerequisites can be found. These matrices should be useful for professionals working with audits and penetration tests, as well as for other academics in the field.

• Recommendations for protective measures, including aspects for protecting end users, as well as those concerning management information systems for information security, and details on how to inform managers about security issues. Papers 1, 3, 4, 5 and 6 in Part II concern user level protection. The papers concerning management information systems on security information, and the art of involving managers in information security are Paper 2 in Part II and Nohlberg and Bäckström (2007). These recommendations are useful for organizations that want to improve their protection, and for other academics studying penetration testing. The paper on the design of a management information system for information security contains several relevant and useful design heuristics that can be used for designing information systems in general, and those related to security in particular. If a software solution can be used, to some extent, to protect against social engineering, it would be ironic if it did not consider the humans using it. In order to achieve good usability for our interface, we developed a user-centered security concept that mainly focuses on usability, which is, in fact, an often overlooked but key security concept. If, for instance, the technical products that are employed in an organization are hard to use, new ways of attacking the users trying to understand the products will be created. It was therefore very relevant to present design heuristics that can help to design not only a security management information system, but perhaps more secure software in general.

• The concept of automated social engineering, ASE, has been coined and described within the context of this thesis work. Automated social engineering is one of the possible epic threats to global Internet use in general, and Web 2.0 in particular. It combines the massive numbers of attacks used, for instance, in common spam and the sophistication and targeting of social engineering. As current readiness for this appears to be low even in security conscious organizations, as described in Paper 5, Part II, it is
quite possible that ASE may be astonishingly successful and cause major problems if we do not create better awareness and readiness for this threat.

Scientific Quality

We use the criteria for qualitative research, suggested by Lincoln and Guba (1985), in the discussions of the scientific quality in this section. It is notable that some of the criteria are interwoven, so in certain cases the same arguments may apply.

Credibility

Credibility refers to the trustworthiness of the research, the information sources used, and that sources or references for the findings and conclusions drawn from the material used can be found (Lincoln & Guba, 1985). Our means of addressing this have been to allow the interviewees to read the interview transcriptions and make corrections and changes to any misinterpretations, thereby ensuring that we understood them correctly. The surveys have been studied with reasonable statistical tools. Where there are problems with the studies that may have influenced the results, this has been clearly indicated and discussed in the respective papers. Other related work has been identified, and where material from other sources has been used, it has been clearly referenced. The research process has also been described in detail, making it possible to see how the research has been conducted. Furthermore, the contributions of the papers and the book chapter have been published and subjected to a peer-review process. This means that the research conducted, its conclusions and findings have been exposed to critical reviews. The contributions have also been discussed with colleagues, both within academia and those working as practitioners in the security field. A further means of validating credibility is the actual, real world use of some of the findings, most notably the management system interface.

Conformability

Conformability concerns the extent to which the results cohere with and are supported by the data, that is, the objectivity of the report (Lincoln & Guba, 1985). We address this by documenting how all data have been collected and which techniques were used. In addition, we have documented our reasoning behind the conclusions drawn from the data gathered. As our studies examined different areas and used different approaches, we describe the complete picture and the conclusions that can be drawn when all the results of this thesis are combined. The received submissions to conferences, journals and books entail that our results have been examined and accepted.
Dependability

It is important that the findings are consistent and could be repeated in a similar setting, with similar subjects, or that the same conclusions could be drawn by other researchers using the same data (Lincoln & Guba, 1985). In order to provide dependability, we have documented our findings so that the data can be studied further. We have also described the methodological considerations, which questions were asked and how the studies have been conducted. This makes it possible to conduct the same studies in similar settings, and it is our belief the results would be comparable. By publishing our results, other researchers have had the possibility to examine our conclusions based on the data gathered, and in that manner the conclusions have been discussed. We thus claim to have achieved dependability.

Transferability

Transferability concerns the degree of applicability in other contexts of our research results (Lincoln & Guba, 1985). The research focus has been on human weaknesses in a security setting. These weaknesses are fundamentally the same no matter which organization a person is connected to; be they educational, health care, high-tech, medical or other. This is due to the fact that human weaknesses, as discussed in Book Chapter 1, Part II, are common traits among all humans, to some extent, even if certain cultural (both societal and organizational) aspects might influence which of the weaknesses is most easily exploited in a particular person. This creates a great deal of transferability among organizations. We have also used literature from other areas than information security, in order to strengthen our research and hopefully provide results that can be useful in other domains. We argue that our results possibly could also be transferred into other research areas, although they primarily relate to information security. The deception cycle could, for instance, perhaps be helpful in criminology, where it may be used, in a general way, as a basis for describing other kinds of frauds and crime with intent. We have tried to make it easier for others to decide whether or not this research suits their goals by describing our findings and data in a thorough manner that is even accessible to the reader without a background in information security.

Relevance

Relevance deals with having solved problems, current references, clear premises and a description of the thesis context (Lincoln & Guba, 1985). This is perhaps the most important aspect. Is this research relevant? We do believe that we advance the research in the field by employing a broader approach to security and contributing to a sometimes overlooked field of research within it. We also provide models that explain phenomena in the research field. The
contributions are described on page 76, but in general, the positive reception both in academia and among professionals indicates that this research is relevant and extends the body of knowledge.

Future Work

In this work several different perspectives on social engineering have been tried and studied. This has been beneficial, since academics have not studied the field to a great extent previously. The three different pillars of this research; Understanding, Measuring and Protecting, all served their purposes in providing the broad understanding that was the goal of this thesis. However, each area could alone be studied further by an aspiring researcher. There are some concrete examples of areas of study that we consider especially relevant.

• The cycle of deception is a tool that can be useful in many other areas of crime, and could be studied in relation to different crimes. For example, the deceptions carried out by prisoners to get compliance from their wardens, the manipulative techniques parents use against social workers in custody conflicts, and many other issues not related to information security. The model could also be used to create specific, social engineering training programs, and serve as a tool for creating social engineering artificial intelligence bots, as described below.

• The psychological and social-psychological aspects of security are still research areas in their infancy, and they have a wide selection of research opportunities with a great deal of potential. For instance, there are indications that certain people are more susceptible to deception than others. This is indicated in many studies on deception which reveal that about 30% of the subjects are deceived. If we could identify those in an easy way and tailor specific training for them, the overall security would benefit tremendously. It is possible these people could be identified by traditional psychometric methods, such as personality types, and so on.

• The penetration testing methods described in the measuring section of this work could be studied further and applied in more, and different, organizations. They could also be used as benchmarks against other methodologies, both manual and more automated, to enable more precise recommendations. The methods could also be complemented with other means of penetration testing. There ought to be many other ways of trying to measure susceptibility.

• The cultural aspects, such as the values of the society in which the attacker and the victim live, tend to be somewhat overlooked in security. This may be due to the proverbial “hot potato” that cultural studies can become if not carried out correctly. In an increasingly globalized society it would
be improper for security specialists not to consider the area. Attackers would be more than happy to exploit it – something they are possibly doing already. There are several studies that may be useful as a starting point for this, most notably the “The World Value Survey”, in which a large number of nations were surveyed on a large selection of areas; religion and values, sociodemographics, natural identity, religion and morale, politics and society, family, work, environment and perceptions of life. Each of the eight areas examined in this survey influences the social engineering attack, most importantly, how the attack should be performed to be successful. A would-be perpetrator planning to attack a specific country would be well advised to spend some time reading through the data collected in “The World Value Survey” to prepare which kind of attack should be selected and how it should be deployed. Culture can also include organizational culture. While this is an area we know more about, it is still well worth studying further.

- AI-bots are rather simple pieces of software that are easy to program and develop, and, at the same time, can emulate basic human interaction (Walentowicz & Mozuraite Araby, 2008). They mainly work by pattern recognition, and are available both as free software and as more advanced commercial software. We have seen great potential in the use of AI-bots in research projects related to this. For instance, they have been successfully used as a training tool in teaching employees about security in general (Walentowicz & Mozuraite Araby, 2008), but we have also seen their potential in other areas. We believe they can be used to train people in experiencing social engineering attacks and how an attacker would work, while being educated at the same time. This would have the benefit of providing a much richer experience for the user, while at the same time keeping down costs and avoiding ethical dilemmas. The same bots could also be used for social engineering penetration testing, for example, when using social networks or online chats, a technique attackers will most likely be using in the future. If the bots were sufficiently developed, they could be used as a communication firewall, scanning messages and chats to detect and warn when deceitful communication is at hand. This, however, is a goal that lies sometime in the future, but the other suggested uses, mentioned above, can reasonably be developed and used within a short time. That carrying out successful social engineering without using much technology is simple does not mean that doing even more successful social engineering while using technology is not possible. We need to prepare the defenses and our organizations. This should be achieved partly by adapting to the threats of today, but also by realizing that the threats of tomorrow are going to be far more sophisticated. If we do not prepare for them today, we may be swept away by the oncoming torrent of attacks.
References


Part II: Publications

Part II includes six papers and one book chapter each representing different parts and stages of the research. They are presented in chronological order. The Book Chapter and Paper 3 present the result from the aspect of Understanding. Papers 1, 4 – 6 are mostly focused on Measuring. Paper 2 is mostly focused on Protecting, even if this area is also covered, to some extent, in the Measuring section. The publications are not included in this digital version due to copyright constraints.

<table>
<thead>
<tr>
<th>Paper 1</th>
<th>Measuring</th>
<th>Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Marcus Nohlberg</td>
</tr>
<tr>
<td>Paper 2</td>
<td>Protecting</td>
<td>User-centered security applied to the development of a management information system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marcus Nohlberg and Johannes Bäckström</td>
</tr>
<tr>
<td>Book Chapter 1</td>
<td>Understanding</td>
<td>Why Humans are the Weakest Link</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marcus Nohlberg</td>
</tr>
<tr>
<td>Paper 3</td>
<td>Understanding</td>
<td>The cycle of deception - a model of social engineering attacks, defenses and victims.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marcus Nohlberg and Stewart Kowalski</td>
</tr>
<tr>
<td>Paper 4</td>
<td>Measuring</td>
<td>Non-Invasive Social Engineering Penetration Testing in a Medical Environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marcus Nohlberg, Stewart Kowalski and Kerstin Karlsson</td>
</tr>
<tr>
<td>Paper 5</td>
<td>Measuring</td>
<td>Measuring Readiness for Automated Social Engineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marcus Nohlberg, Stewart Kowalski and Markus Huber</td>
</tr>
<tr>
<td>Paper 6</td>
<td>Measuring</td>
<td>Phishing with Gifts as Bait: Measurement and Analysis of Phishing Attacks within a University Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Martin Boldt and Marcus Nohlberg</td>
</tr>
</tbody>
</table>
No 91-004 Olsson, Jan
An Architecture for Diagnostic Reasoning Based on Causal Models

No 93-008 Orci, Terttu
Temporal Reasoning and Data Bases

No 93-009 Eriksson, Lars-Henrik
Finitary Partial Definitions and General Logic

No 93-010 Johannesson, Paul
Schema Integration Schema Translation, and Interoperability in Federated Information Systems

No 93-018 Wangler, Benkt
Contributions to Functional Requirements Modelling

No 93-019 Boman, Magnus
A Logical Specification for Federated Information Systems

No 93-024 Rayner, Manny
Abductive Equivalential Translation and its Application to Natural-Language Database Interfacing

No 93-025 Idestam-Almquist, Peter
Generalization of Clauses

No 93-026 Aronsson, Martin
GCLA: The Design, Use, and Implementation of a Program Development

No 93-029 Boström, Henrik
Explanation-Based Transformation of Logic programs

No 94-001 Samuelsson, Christer
Fast Natural Language Parsing Using Explanation-Based Learning

No 94-003 Ekenberg, Love
Decision Support in Numerically Imprecise Domains

No 94-004 Kowalski, Stewart
IT Insecurity: A Multi-disciplinary Inquiry

No 94-007 Asker, Lars
Partial Explanations as a Basis for Learning

No 94-009 Kjellin, Harald
A Method for Acquiring and Refining Knowledge in Weak Theory Domains

No 94-011 Britts, Stefan
Object Database Design

No 94-014 Kilander, Fredrik
Incremental Conceptual Clustering in an On-Line Application

No 95-019 Song, Wei
Schema Integration: - Principles, Methods and Applications
No 95-050 Johansson, Anna-Lena
Logic Program Synthesis Using Schema Instantiation in an Interactive Environment

No 95-054 Stensmo, Magnus
Adaptive Automated Diagnosis

No 96-004 Wærn, Annika
Recognising Human Plans: Issues for Plan Recognition in Human - Computer Interaction

No 96-006 Orsvärn, Klas
Knowledge Modelling with Libraries of Task Decomposition Methods

No 96-008 Dalianis, Hercules
Concise Natural Language Generation from Formal Specifications

No 96-009 Holm, Peter
On the Design and Usage of Information Technology and the Structuring of Communication and Work

No 96-018 Höök, Kristina
A Glass Box Approach to Adaptive Hypermedia

No 96-021 Yngström, Louise
A Systemic-Holistic Approach to Academic Programmes in IT Security

No 97-005 Wohed, Rolf
A Language for Enterprise and Information System Modelling

No 97-008 Gambäck, Björn
Processing Swedish Sentences: A Unification-Based Grammar and Some Applications

No 97-010 Kapidzic Cicovic, Nada
Extended Certificate Management System: Design and Protocols

No 97-011 Danielson, Mats
Computational Decision Analysis

No 97-012 Wijkman, Pierre
Contributions to Evolutionary Computation

No 97-017 Zhang, Ying
Multi-Temporal Database Management with a Visual Query Interface

No 98-001 Essler, Ulf
Analyzing Groupware Adoption: A Framework and Three Case Studies in Lotus Notes Deployment

No 98-008 Koistinen, Jari
Contributions in Distributed Object Systems Engineering

No 99-009 Hakkarainen, Sari
Dynamic Aspects and Semantic Enrichment in Schema Comparison

No 99-015 Magnusson, Christer
Hedging Shareholder Value in an IT dependent Business society - the Framework BRITS

No 00-004 Verhagen, Henricus
Norm Autonomous Agents
No 00-006 **Wohed, Petia**  
Schema Quality, Schema Enrichment, and Reuse in Information Systems Analysis

No 01-001 **Hökenhammar, Peter**  
Integrerad Beställningsprocess vid Datasystemutveckling

No 01-008 **von Schéele, Fabian**  
Controlling Time and Communication in Service Economy

No 01-015 **Kajko-Mattsson, Mira**  
Corrective Maintenance Maturity Model: Problem Management

No 01-019 **Stirna, Janis**  
The Influence of Intentional and Situational Factors on Enterprise Modelling Tool Acquisition in Organisations

No 01-020 **Persson, Anne**  
Enterprise Modelling in Practice: Situational Factors and their Influence on Adopting a Participative Approach

No 02-003 **Sneiders, Eriks**  
Automated Question Answering: Template-Based Approach

No 02-005 **Eineborg, Martin**  
Inductive Logic Programming for Part-of-Speech Tagging

No 02-006 **Bider, Ilia**  
State-Oriented Business Process Modelling: Principles, Theory and Practice

No 02-007 **Malmberg, Åke**  
Notations Supporting Knowledge Acquisition from Multiple Sources

No 02-012 **Männikkö-Barbutiu, Sirkku**  
SENIOR CYBORGs- About Appropriation of Personal Computers Among Some Swedish Elderly People

No 02-028 **Brash, Danny**  
Reuse in Information Systems Development: A Qualitative Inquiry

No 03-001 **Svensson, Martin**  
Designing, Defining and Evaluating Social Navigation

No 03-002 **Espinoza, Fredrik**  
Individual Service Provisioning

No 03-004 **Eriksson-Granskog, Agneta**  
General Metarules for Interactive Modular Construction of Natural Deduction Proofs

No 03-005 **De Zoysa, T. Nandika Kasun**  
A Model of Security Architecture for Multi-Party Transactions

No 03-008 **Tholander, Jakob**  
Constructing to Learn, Learning to Construct - Studies on Computational Tools for Learning

No 03-009 **Karlgren, Klas**  
Mastering the Use of Gobbledygook - Studies on the Development of Expertise Through Exposure to Experienced Practitioners' Deliberation on Authentic Problems
No 03-014 **Kjellman, Arne**
Constructive Systems Science - The Only Remaining Alternative?

No 03-015 **Rydberg Fåhræus, Eva**
A Triple Helix of Learning Processes - How to cultivate learning, communication and collaboration among distance-education learners

No 03-016 **Zemke, Stefan**
Data Mining for Prediction - Financial Series Case

No 04-002 **Hulth, Anette**
Combining Machine Learning and Natural Language Processing for Automatic Keyword Extraction

No 04-011 **Jayaweera, Prasad M.**
A Unified Framework for e-Commerce Systems Development: *Business Process Patterns Perspective*

No 04-013 **Söderström, Eva**
B2B Standards Implementation: Issues and Solutions

No 04-014 **Backlund, Per**
Development Process Knowledge Transfer through Method Adaptation, Implementation, and Use

No 05-003 **Davies, Guy**
Mapping and Integration of Schema Representations of Component Specifications

No 05-004 **Jansson, Eva**
Working Together when Being Apart – An Analysis of Distributed Collaborative Work through ICT from an Organizational and Psychosocial Perspective

No 05-007 **Cöster, Rickard**
Algorithms and Representations for Personalised Information Access

No 05-009 **Ciobanu Morogan, Matei**
Security System for Ad-hoc Wireless Networks based on Generic Secure Objects

No 05-010 **Björck, Fredrik**
Discovering Information Security Management

No 05-012 **Brouwers, Lisa**
Microsimulation Models for Disaster Policy Making

No 05-014 **Näckros, Kjell**
Visualising Security through Computer Games
Investigating Game-Based Instruction in ICT Security: an Experimental approach

No 05-015 **Bylund, Markus**
A Design Rationale for Pervasive Computing

No 05-016 **Strand, Mattias**
External Data Incorporation into Data Warehouses

No 05-020 **Casmir, Respickius**
A Dynamic and Adaptive Information Security Awareness (DAISA) approach
No 05-021 **Svensson, Harald**
Developing Support for Agile and Plan-Driven Methods

No 05-022 **Rudström, Åsa**
Co-Construction of Hybrid Spaces

No 06-005 **Lindgren, Tony**
Methods of Solving Conflicts among Induced Rules

No 06-009 **Wrigstad, Tobias**
Owner-Based Alias Management

No 06-011 **Skoglund, Mats**
Curbing Dependencies in Software Evolution

No 06-012 **Zdravkovic, Jelena**
Process Integration for the Extended Enterprise

No 06-013 **Olsson Neve, Theresia**
Capturing and Analysing Emotions to Support Organisational Learning: The Affect Based Learning Matrix

No 06-016 **Chaula, Job Asheri**
A Socio-Technical Analysis of Information Systems Security Assurance A Case Study for Effective Assurance

No 06-017 **Tarimo, Charles N.**
ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach

No 06-020 **Kifle Gelan, Mengistu**
A Theoretical Model for Telemedicine - Social and Value Outcomes in Sub-Saharan Africa

No 07-001 **Fernaeus, Ylva**
Let’s Make a Digital Patchwork
Designing for Children’s Creative Play with Programming Materials

No 07-003 **Bakari, Jabiri Kuwe**
A Holistic Approach for Managing ICT Security in Non-Commercial Organisations
A Case Study in a Developing Country

No 07-004 **Sundholm, Hillevi**
Spaces within Spaces: The Construction of a Collaborative Reality

No 07-005 **Hansson, Karin**
A Framework for Evaluation of Flood Management Strategies

No 07-007 **Aidemark, Jan**
Strategic Planning of Knowledge Management Systems - A Problem Exploration Approach

No 07-009 **Jonsson, Martin**
Sensing and Making Sense
Designing Middleware for Context Aware Computing

No 07-013 **Kabilan, Vandana**
Ontology for Information Systems (O4IS) Design Methodology: Conceptualizing, Designing and Representing Domain Ontologies
No 07-014 Mattsson, Johan
Pointing, Placing, Touching - Physical Manipulation and Coordination Techniques for Interactive Meeting Spaces

No 07-015 Kessler, Anna-Maria
A Systemic Approach Framework for Operational Risk - SAFOR

No 08-001 Laaksolahti, Jarmo
Plot, Spectacle and Experience: Contributions to the design and evaluation of Interactive Storytelling

No 08-002 Van Nguyen Hong
Mobile Agent Approach to Congestion Control in Heterogeneous Networks

No 08-003 Rose-Mharie Åhlfeldt
Information Security in Distributed Healthcare - Exploring the Needs for Achieving Patient Safety and Patient Privacy

No 08-004 Sara Ljungblad
Beyond users: Grounding technology in experience

No 08-005 Eva Sjöqvist
Electronic Mail and its Possible Negative Aspects in Organizational Contexts

No 08-006 Thomas Sandholm
Statistical Methods for Computational Markets – Proportional Share Market Prediction and Admission Control

No 08-007 Lena Aggestam
IT-supported Knowledge Repositories: Increasing their Usefulness by Supporting Knowledge Capture

No 08-008 Jaana Nyfjord
Towards Integrating Agile Development and Risk Management

No 08-009 Åsa Smedberg
Online Communities and Learning for Health - The Use of Online Health Communities and Online Expertise for People with Established Bad Habits

No 08-010 Martin Henkel
Service-based Processes - Design for Business and Technology

No 08-012 Jan Odelstad
Many-Sorted Implicative Conceptual Systems