Social Engineering: Understanding, Measuring and Protecting Against Attacks.

Thesis Proposal

2007-06-04

Marcus Nohlberg
marcus@nohlberg.com
School of Humanities and Informatics,
University of Skövde,
S-541 28 Skövde,
Sweden.

Supervisor: Benkt Wangler
Co-supervisor: Stewart Kowalski

Abstract

This thesis is about an attack against the human element of security called social engineering, where the assailant gets the mark to give out information that the mark should not give out. The thesis contains a background description on information security, as well as a more thorough description on the two most common attacks against humans, Phishing and social engineering. It also gives a short description on the factors that can make humans susceptible to manipulation.

The research is divided into three areas; knowing, measuring, preventing, which are described and state of the arts for each is described. A description of previous work, as well as planned future work is included as well as expected results and a conclusion that the human element is an important area of information security where contributions for both research and industry can be made.

Key words: Social Engineering, Phishing, Audits, Security Awareness, Vulnerability Testing, Information Security.

Table of contents

1 Introduction

From a history of relative obscurity to something of a general interest, the market and interest for security have flourished in recent years. The reason for the growth is increased spending among organizations. In 2003 British companies spent 2 % of their IT-budgets on security, and in 2004 they spent 3 %, large companies spent 4 % (Department of Trade and Industry's Information Security Breaches Survey, 2004). This increase is also clearly motivated by an increase in security breaches, as for instance reported in the previous study; 32 % of British companies suffered security incidents in 1998, and in 2004 74 % of the companies reported security incidents. One of the explanations for this steep increase is of course the increased connectivity, which not only is a great tool for business, but also exposes the organization to far more threats. Yet there seem to be no turning back from this connected world, as dependence of electronic information has grown from 76 % in 2002 to 87 % in 2004 (Department of Trade and Industry's Information Security Breaches Survey, 2004). Among major Swedish companies it is widely thought that security is of the utmost importance, no matter the cost (Brandon, 2003).

When talking about security it is common to think about solutions that are primarily technical in nature: firewalls, anti-virus software, etc. In this research proposal the focus is slightly different in that I will try to look at security from another angle; the human element of security. This is something made infamous by Kevin Mitnick, partly through his actions as a hacker, and partly because of his writings and speeches on a hacking technique called social engineering. 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 this information together he managed to get the access he wanted. His most frequently used tool was the telephone and a well planned out ruse. These techniques are in use today, for instance in the highly publicized "Paris Hilton Hack" (Krebs, 2005) where the hackers tricked employees to divulge secret information.

Social engineering attacks are quite different from the majority of the technical attacks in that they have a clear, specific, aim. The vast majority of attacks and threats to security are "script kiddies", viruses, Trojans and other broad attacks and thus done without a clear aim (Mitnick, 2002). Social engineering attacks, however, always have a clear purpose. It can be to acquire information, or even a login. Those doing it can be hackers, such as Mitnick, doing it just for the curiosity, or high tech information brokers, doing it to steal information. It can even be foreign intelligence, doing it to prepare for war (H SÄK IT Hot, 2001). But it is almost always done with intent (Mitnick, 2002).

Social engineering is a term used for techniques to trick, or con, users into giving out information, or login information, to someone that should not receive it. Techniques used in social engineering are also, to some extent, used in Phishing. The difference between Phishing and social engineering principally lies within the scales of the attack. Social engineering tends to be used against a limited amount of targets (that has been selected with greater

care), while Phishing borrows heavily from techniques used by spam to attack large amounts of marks.

Since many users does not believe that anyone would ever attack them, because they are not "rich and famous", and that hackers cannot do much damage anyway (Brostoff et al, 2002), the attacks can be highly successful. This 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 (Adams & Sasse, 1999 p. 45):

> *(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.*

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

In a study done by Treasury Department inspectors, one third of the Internal Revenue Service (IRS) employees gave away their login and password to auditors calling pretending to be computer technicians (Dalrymple, 2005). There have been other studies on the "gullibility" of users, and to what extent they submit information when being attacked by perpetrators using Phishing and social engineering attacks, and the results have generally indicated that users are quite susceptible to these kinds of attacks, but due to a high degree of insecurity about the results in the studies, it is hard to be precise about to what extent. Even so, some studies do provide a certain shock value. For instance the highly publicized "Chocolate for passwords", where more than 70 % of the subjects would reveal their password in exchange for a piece of chocolate, and where 79 % of users would give away information that could be used to steal their identities (Wagner, 2004).

Perhaps it is like said by one of the interviews 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."*

Gartner (2002a) writes 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."*

1.1 Aim

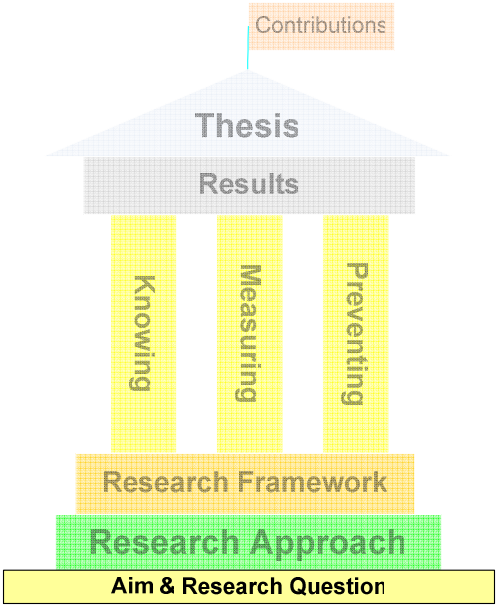

Figure 1: Aim & Research Question (author's own.)

The aim of this work is to achieve a better understanding of the threat named social engineering, nefarious attacks aimed towards the human element of the target. This is an often neglected, but by many considered crucial, area of information security. By extending the knowledge of what makes humans susceptible to attacks, as well as learning about current attacks, their countermeasures and methods for testing organizations and individuals vulnerability to these attacks, a new, and important, contribution will be made both to academia and to the professionals in the field. The contributions are expected to consist most importantly of:

- A deeper understanding of the socio-psychological factors that make people susceptible to attacks in the form of a book chapter on the subject.
- A conceptual model describing what a social engineering attack is, its stages and how it works. This is combined with a taxonomy of the different kinds of attacks that are known to be used today
- Recommendations on how to do social engineering penetration testing in organizations.
- Recommendations for protective measures, considering both traditional and often suggested education as well as novel approaches to protection against social engineering attacks.
- A novel new tool to use for education, training and penetration testing of users in the form of a social engineering AI-bot.

1.2 Delimitations

The human element of security can cover both unintentional mistakes made by humans, as well as deliberate attacks by perpetrators. In this research the focus lies on intended attacks, not the unintentional mistakes.

There is a rather strict division between what is technical, and what I consider human related security in general and social engineering in particular. This is solely to avoid this study to be almost without limits.

1.3 Research Question

To put it briefly, the research question of this work is: *"What is social engineering and how can we best protect against attackers using it?"*

1.4 Refined Set of Research Questions

Considering the research question, there are three areas to study. These three areas have been selected based on previous work, experience, ongoing literature studies as well as informal discussions with a number of information security professionals.

- What is social engineering? What mechanisms are there behind it, how are humans influenced, and what techniques are attackers using? In order to understand the term, a taxonomy of attacks and a conceptual model describing concept better will be created. In order to know more about the area it is important to cover the literature on the subject, and what can be learned from other areas of research. This objective covers the *knowing* area discussed in section 2.1.
- Which are the ways to measure an organizations vulnerability to social engineering? There is a selection of methods for penetration testing, but many of these have ethical or practical problems. An effort to judge efficiency of novel approaches in this area is necessary. By using a taxonomy of attacks, it should be possible to create a set of suggested methods for penetration testing based on the specific attack for which resilience should be tested. This objective covers the area *measuring*, as discussed in section 2.2.
- How to protect against social engineering attacks? For most of industry, it is of the utmost importance to be able to protect against nefarious attacks. In order to be able to provide increased security, the current preventive means are studied, and novel approaches to defense based on knowledge from other areas are tested. This objective covers the area *preventing*, discussed in section 2.3.

The research approach will be to gain as much knowledge as possible from literature studies, mostly in order to gain background knowledge on the subject. In order to gain deeper understanding and to get novel results from organizations studied, both qualitative and quantitative studies will be used. One clear goal is that the results and studies done should not only have excellent academic qualities, but also have a practical use, which is especially important as I am an industrial Ph.D. student. The research approach is discussed further in chapter 5 below.

1.5 Thesis Outline and Writing Conventions

The rest of the proposal is separated into three parts. Section 2 describes the research area further and is more specific about the research together with the current status on research in the respective fields.

Section 3 is an extended background, describing information about information security in general, and more specifically social engineering and Phishing. It also contains a section describing some theories about why it works, from a social psychology perspective, trying to give some insights into why the attacks are sometimes successful by describing a bit about how humans react to influence.

The final sections (4, 5 and 6) contain descriptions of earlier work, planned future work, contributions and discussion.

In order to increase legibility the genus of persons will be written as "her" in cases where gender is of no particular consequence in this work. If gender is of specific importance it will be clearly noted.

2 The PhD Problem Area

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 to me are discussed. The research has been divided into these areas based on previous work, experience, ongoing literature studies as well as informal discussions with a number of information security professionals.

One of the problems with this area of research is that in the past there has not been all that much interest in the area. Björck (2005) has done a study trying to classify research in information security.

In the study he classified the papers accepted to 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*. The X-axis consists of three areas. The *technical* area deals with for instance computer hardware and software, communication protocols and cryptographic algorithms and technical evaluation methodologies. In the *formal* area, Björck (2005) places research dealing with procedures to formalize the human behavior in the information system. Examples are information security policy, legal system, etc. In the *informal* area there is research about informal human behavior, e.g. social relations, ethics, and security implications of intrapersonal communication. The results can be seen in Figure 2 below. The dots within the dotted line are research aiming to move from one level of abstraction to another, for instance implementing a theory in the empirical world.

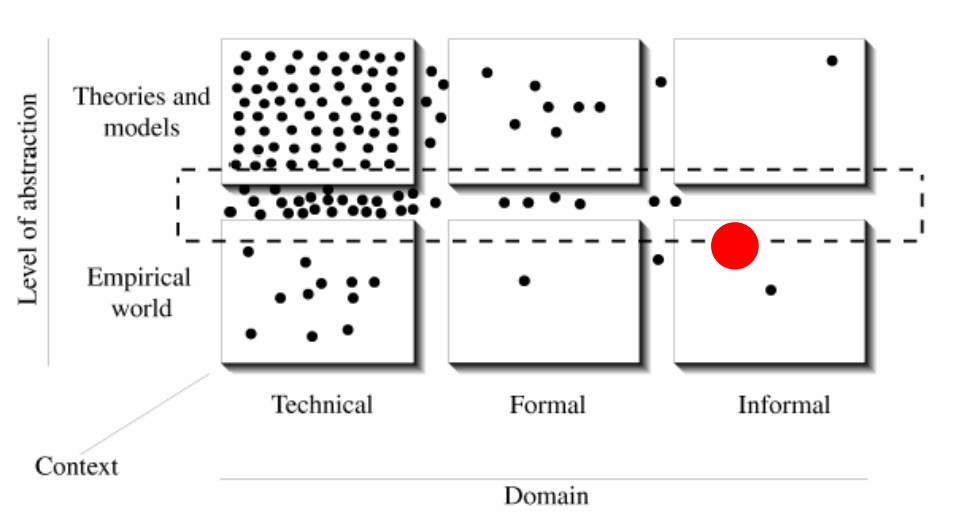

Figure 2: The classification of the 125 papers from the SEC 2000 proceedings (Björck, 2005, p. 234). The large, red, dot marks my research position.

The research proposed in this thesis would be dealing with the informal area, with what Björck (2005, p. 231) calls "security implications of intrapersonal communication". A large part of the research would deal with the empirical world, as I believe that 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. The suggested research position by me is noted by the large red dot in the model above. This is where I aim most of my work to be centered, but it is notable that the surrounding areas might also need to be studied in order to gain a deeper understanding.

This is further motivated by the conclusions by Björck (2005, p. 237) where he argues that the human element of security is one of the most important, and that while 80 % of all information security research is being done in the technical domain today, resources perhaps better spent in the formal and informal domains, where the critical problems are to be found.

In recent years there has been an increased interest in this research area, with books being written and special conferences with focus on the human element, for instance the International Conference on Human Aspects of Information Security & Assurance (HAISA 2007).

Below the three suggested research areas, knowing, measuring, preventing, are presented argued and compared to some of the state of the art today, together with a conclusion on the area.

2.1 Knowing

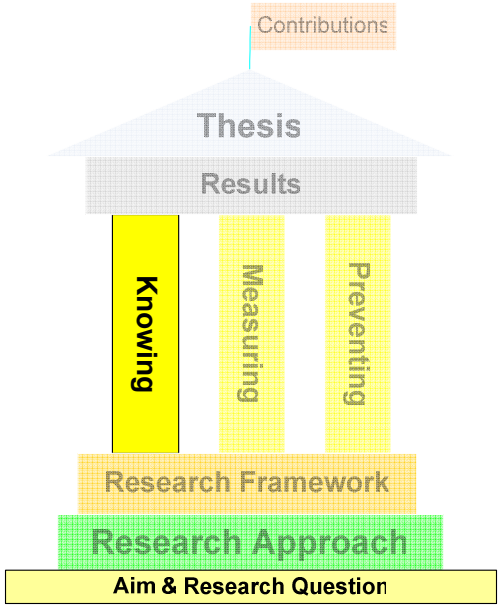

Figure 3: Knowing (author's own.)

Early in the research process, when trying to identify what social engineering consists of, I created a mind-map with different, possible, influencing factors. This mind-map, Figure 4 below, is in no way a complete (or possible even accurate) description of the topic, but it gives an understanding of the complex issues that *can* be argued to in some way be connected to or influencing social engineering.

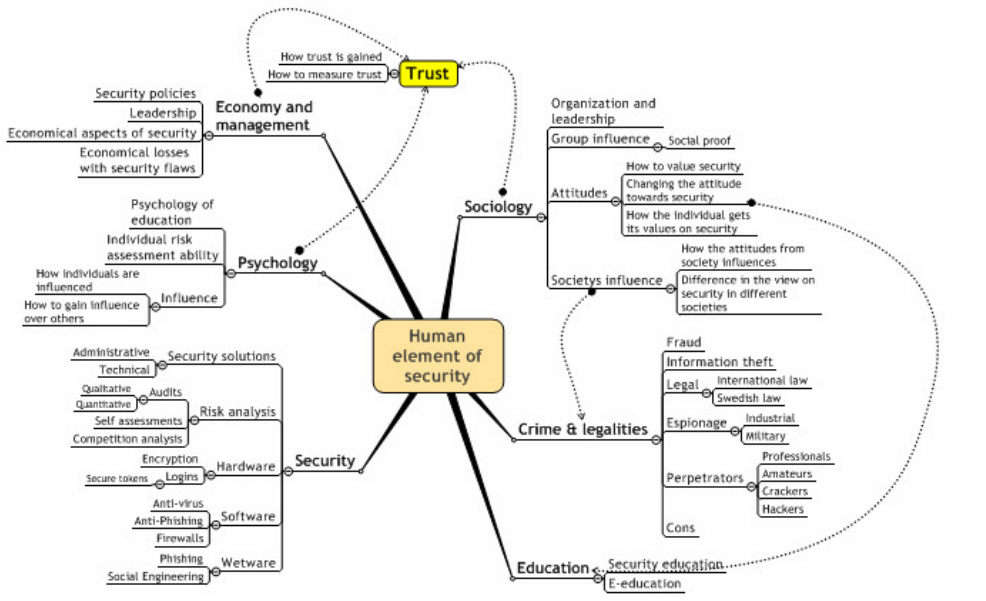

Figure 4: An example of factors influencing the human element of security/social engineering (author's own.)

It is obviously not possible to cover all areas of this complex research area in a single study such as this. Therefore a part of the process is to actually identify what can be included in the term "the human element of security".

The research framework in this thesis describes social engineering and Phishing, two of the major areas for what is often attributed to be the human element of security. They are examples of attacks aimed with deliberation towards primarily humans and human weaknesses. There are, of course, security flaws related to humans that are without deliberation, e.g. they are not done by attackers, but instead by unconcerned and unwitting users. Examples of this can be a user that mistakenly destroy the wrong back-up CD, deletes the wrong file etc. In this research the focus will however be on the deliberate attacks against humans, not the unintentional mistakes users can do.

In order to try to fully understand what the human element of security is, I will try to answer these questions:

- What is social engineering?
- What mechanisms are there behind it?
- How are humans influenced?
- What techniques are attackers using?

2.1.1 Previous Work in the Research Field

Much of the material presented in this thesis describes parts of what the human element of security, the major impact on social engineering, is. There are ample materials to be found regarding Phishing and social engineering, the problem is that the overwhelming majority of the materials are not of an academic standard. Most articles etc. are from contemporary magazines, web pages etc. Those that are of an academic standard, tend to use the same references as the more contemporary ones, meaning that the actual facts base the field stands on is rather slim. It is difficult to overlook the tremendous impact that Mitnick (2002) has had on the field, and not much is written that is not to some extent covered or mentioned in his book, even though the field nowadays span 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 small and there are not a lot of researchers working on 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 anecdotic web pages.

The typical perpetrators of social engineering attacks are described in this paper, section 3.1.2 below. This is a simplified description that should be expanded upon, perhaps by trying to actually interview and contact actual, “real life” users of social engineering, as well as performing interviews with professionals working to thwart them. One potentially interesting meeting place for real life social engineers is online discussion boards dedicated to social engineering and hacking. While it is hard to judge the quality and competency of the people contributing there (but a guess is that the competency is not all that high since it is an open forum), it is an interesting place to find possible contacts.

In criminology there has been a lot of work on who becomes a criminal. 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 Association theory developed by Edwin H. Sunderland.

In Sutherland's differential association theory, the view is that criminal behavior, both technique and values, is learned from social interaction with others. 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). With this in mind, studying a gathering place like the forum for social engineers above might be interesting, but it also puts this research into some ethical scrutiny. It is avoidable that a research area like this will describe techniques actually used for social engineering attacks, which can be used by the aspiring criminal, in cooperation with a social network supporting criminal actions, in order to become a criminal. This is, however, not something unusual for this particular field, it is shared with much of information security.

A basic description on what makes humans receptacle to influence from others are given above in section 3.4 below. This area should be further expanded, and a wider, more cross disciplinary approach can be used. It would be interesting to further study deception and influence, as described above, to gain a deeper understanding for how the techniques work, as well as studies in how lies are detected. There is a wealth of information on these subjects, and they could improve the general knowledgebase within the area. One of the papers that have an interesting new approach to the area is Jordan & Goudey (2005), who describes taxonomy of twelve categories of social psychological vulnerabilities. They use this taxonomy to describe a selection of current attacks by malicious code and the social engineering areas they exploit. This taxonomy could potentially be useful in the creation of a taxonomy of classic social engineering attacks, as well as Spear-Phishing, deception attacks or perhaps even to use in creating patterns for social engineering attacks. It is something that I would like to study further. A possible angle would be to try to use the taxonomy together with other factors that influence humans in order to create a rather complete inventory of manipulative techniques.

When focusing on deception, and techniques to educate on 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 have a focus 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 would be a highly interesting area to study further, as well as 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), and the IDT are more aimed towards communication with low degree of personal connection (therefore Phishing).

Deception is obviously a field of research that have a lot of potential for improving the knowledgebase on the human element, and I find it to be intriguing that there seems to be virtually no connection at all between the studies on deception and the studies on Phishing and social engineering.

2.1.2 Conclusion on knowing what Social Engineering is

There is a surprisingly small amount of research being done on the human elements of security, as described above. There are, however, interesting and relevant research in other fields than information security. The area of deception research shows great promise and potential, and there are probably a lot to be learned from that field, lessons that can improve knowledge about social engineering in an information security perspective. There is also great potential to learn from psychology and sociology.

I believe that it would be beneficial to the general knowledge in the field to get a deeper understanding on what influences humans, how deception works and the psychological explanations. In trying to protect against attackers using information from other domains than information security, it is important to not only look in a specific domain for explanations.

2.2 Measuring

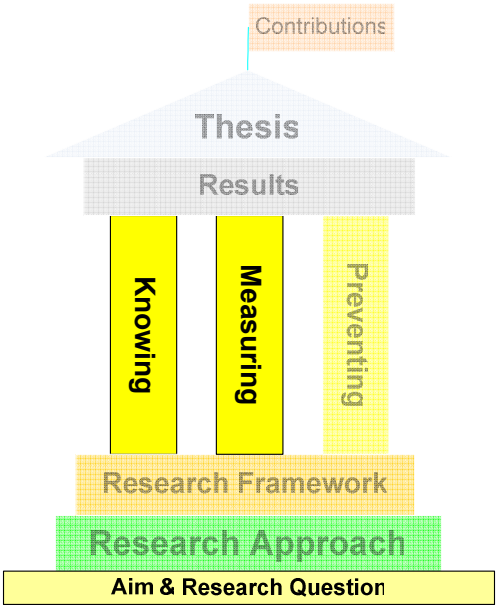

Figure 5: Measuring (author's own.)

My father has a favorite quote from Lord Kelvin: "To measure is to know". And 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 that the deployment of an anti-virus software has on an organization. One of the more obvious impacts is, hopefully, the disappearance of viruses, and the logs probably display a huge number of attacks, updates and successful recoveries done by the

software. Something that concrete has a value that is easy to grasp. When it comes to humans, it is harder to measure, both inefficiency, and efficiency. Another fact that can be troubling is that while technical attacks tend do be of a large scale, e.g. viruses or attacks against firewalls, the attacks aiming towards the humans are in a smaller scale, with a higher focus on individuals. This does not make it easy to create any kind of relevant statistics, and thus, it is hard to fully grasp the scale of the problem. In order to approach this dilemma, I will try to find answers to the following questions:

- Which are the ways to measure an organizations vulnerability to social engineering?
- Can a taxonomy of attacks be used to create a set of suggested methods for penetration testing based on the specific attack for which resilience should be tested

2.2.1 Previous Work in the Research Field

One approach on diagnosing this is to send out fake Spear Phishing e-mails to the organizations own users. This has been done by both the New York state, and the US military school West Point (Bank, 2002). 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 got 80 % compliance among the students. In the case of the New York state, 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. A follow-up to this a couple of months later, with a similar approach, got 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 influenced, and there is also other ethical question. Still, it might be a very efficient method not only to diagnose a level of insecurity, but also to educate the users. If they do submit information, and get some critique for it, the may become inoculated against further, real, attacks.

There have, of course, also been other, academic, studies on Phishing audits. A highly publicized and interesting study was done by Jagatic et. al. (2005) in which they tried a combination of Spear Phishing and context aware Phishing attacks against university students. The experiment was a stunning success, if seen from the perspective of a potential attacker. The attacks using a classic Phishing attack were successful to a lower degree (16 %), but the more advanced attack was successful in 72 % of the cases.

While the Phishing study by Jagatic et. al. (2005) in itself is highly interesting, the debate and ethical and emotional dilemmas with highly voiced complaints and critical articles in other media about the study following its publication are also interesting. This once again points out the necessity of a strictly ethical approach while doing these kinds of studies.

While large scale attacks using Phishing in order to measure a level of insecurity is quite manageable due to the fact that it does not take much longer to send 10,000 e-mails than it takes to send 10, it is not the same can with social engineering attacks. It is, obviously, not feasible to do a social engineering audit on every single employee. One reason is that employees probably would notice if they all suddenly start to get friends that want them to give out information, and another is the fact that it would take a tremendous amount of time for the auditor to properly social engineer a large amount of people individually. The ethical complications would be even greater than for the 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 audits are probably unfeasible for most, if not all, organizations.

The ethical problems connected to social engineering audits are also discussed at length in Hasle et. al (2005). A novel proposal to avoid the dilemmas with auditing individuals, that are also discussed in length, are suggested by Vroom & von Solms (2004) where they actually suggest to not audit individuals at all and instead focus on auditing the organizational culture. This is an interesting approach in theory, but I find it hard to develop a practical deployment from that approach to auditing. Nevertheless, the discussion and arguments against individual auditing are relevant and interesting.

In my previous research, a slightly different approach to this problem was tried. 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 doing a quantitative study under the false pretense 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 as a stand alone auditing technique. The human element was not merely vulnerable, but vulnerable to the extent that it shadows most other security areas (Nohlberg, 2005).

By using a web based study and false pretences, the people assessed (who were highly qualified IT-consultants) were asked a set of question in a different context than security. The results can perhaps be significant of to which extent the organization is vulnerable to social engineering. This approach shares some of the dilemmas discussed with Bank (2002) above, but it is at least a practically feasible method to do social engineering audits on a large scale in organizations.

The dilemmas with penetration testing and social engineering are discussed by Barrett (2003), where the conclusion is that it is preferable to use an audit style that has results and objectives that is clear and can be accepted by both subjects and company. They should also not lead to discipline or dismissal for the individuals. More concrete examples of this are not given by Barrett (2003), though, so it is hard to properly judge his suggestions.

Another academic approach to social engineering audit was done by Hasle et. al (2005), who used an approach to social engineering penetration that tried to test a larger population. They performed two tests, the first were a

survey where the users were asked to submit their login information in order to authenticate if they were to win a price, the second test was an e-mail sent out which triggered a login box. Their findings were that approximately one quarter of the users could be tricked into submitting their passwords.

The study by Hasle et. al (2005) is interesting, but I would argue that they really are testing resistance to Spear Phishing attacks, rather than what is considered social engineering in this study. For instance, in neither of their tests human interaction was used. Their approach is very useful, however, and could be interesting to use both as a stand alone study on other organizations, as well as a metric to which other approaches on social engineering auditing, such as the approach in Nohlberg (2005), could be compared, or the different approaches could even be combined into a more substantial methodology for auditing.

A more traditional approach to social engineering auditing is argued by Jones (2003), where the auditor is advised to actually perform social engineering attacks on the users. A similar approach is used by Orgill et. al (2004) where they actually have a person trying to manipulate his way to information from the employees of the tested organization. They do this in two parts, the first is to let the person wander around submitting employees to a written questionnaire with questions on security, logins etc. and in the second part to try to gain physical access to the perimeters. Both approaches are disturbingly efficient, 81 % of the subjects asked gave their login name, 59 % also gave away their passwords. Very few employees asked for identification or questioned the auditor. The auditor also managed to get unrestricted, physical, access to the building.

Dalrymple (2005) describes the highly successful internal audit on social engineering done by the IRS, where they called a select number of users under some pretext, requesting their passwords, which 35 % of the employees gave out.

The classic approach, as used by Ogrill et. al (2004) definitely has it uses, but the flaws are that it is costly (since it takes a lot of time to perform); it might be perceived as more ethically questionable among the employees, than a more indirect form of deceptive study. One can also question if the educational aspect of tricking a subset of all users will make those who were not audited that identify with the colleagues that actually were conned and learn from that, or would they stick to the "lie detection" bias (Marett et. al,. 2004), feeling that they, themselves, would not fall for "tricks like that".

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

- Test of Controls – the general overview of the organization, can give a basic knowledge usable in further tests.
- Telephone Access – to use a set of well know attacks to test the organizations resistance to attacks over the telephone.
- Garbage Viewing – to see if there are 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) presents 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 my opinion, to provide little data that can actually be useful, and the approach, while nicely structured, is a tad shallow and incomplete.

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

2.2.2 Conclusion on ways to measure an organizations vulnerability to social engineering

One of the reasons for the financial success of technical solutions to the security problem is perhaps that it is easy to see the benefits of using a product against a measurable threat. I 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 most suitable. If a smaller amount of subjects should be tested a bit more thoroughly social engineering would be better. Phishing is, in my opinion, basically using social engineering techniques against a broader 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 might give useful statistics, the fact is still that it is enough with just a single vulnerable employee for the organization to be vulnerable. And the ethical implications of doing extensive testing trying to deceive the employees might also be difficult to handle.

I have used an approach that is potentially useful, by deceiving the users on what is actually tested. It would be quite interesting to do a second, more extensive study, on whether this approach is suitable or not, by using more questions and several organizations that later can be compared, as well as trying to benchmark its efficiency against the other approaches suggested by other researchers.

If possible, it would be quite rewarding to actually try a large scale, classic, social engineering audit by actually trying to con the employees. This would probably take a lot of time, and it could be hard to find an organization that would allow it.

2.3 Preventing

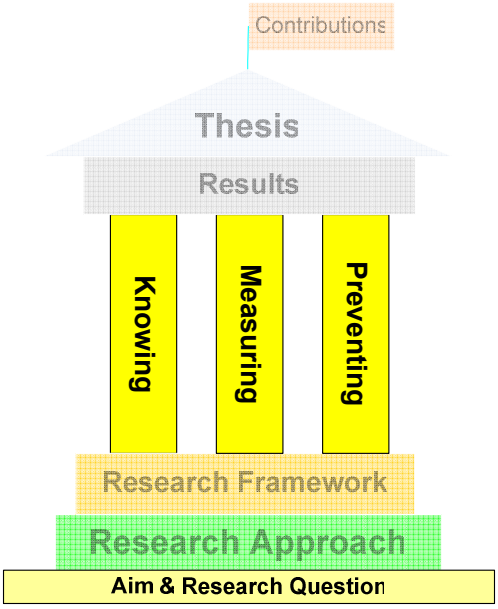

Figure 6: Preventing (author's own.)

Learning about, and measuring, a problem is interesting, but it is important to also try to find possible solutions to the problem. While the extents of the vulnerability to the human element are not precisely known, there are hardly any arguments against its existence. Therefore, there is a need for protection against attacks on the human element. The typical recommendation for protection today is education, argued by, for instance, Mitnick (2002). While it is quite possible that education is the best approach for protection, it still leaves a lot of questions to be answered.

Here I'll try to answer the following question:

- How to protect against social engineering attacks?

2.3.1 Previous Work in the Research Field

When doing a more general case study on the status of information security in the healthcare domain, interviewing persons responsible for information security, it was obvious that education was lacking among most of the subjects organizations. In one organization no education had been performed in the last 10 years, and in none were 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 must take into account psychology and persuasion and develop that in order to understand, and counter, the persuasive attack (Gragg, 2002).

In section 3.2.3 below the current state of the art is described, with a thorough description of the interesting "A multi-layered defense against social engineering" by Gragg (2002). The specific educational needs are described, as well as general guidelines from other sources. Protection against Phishing is described in 3.3.3 below, where practical; end user actions as well as somewhat more organizational aspects are described.

There is also an interesting Masters Thesis aimed on 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 & Ravne (2005). In this thesis the authors test, with some success, scenario based learning on psychological factors of persuasion, and creates a software prototype for this. This scenario method was then measured as more efficient than the use of ordinary lectures.

While their approach is interesting, I believe that there is a risk when focusing so closely towards certain methods of manipulation, as the typical characteristic of the social engineer is the adaptability and the flexibility of the attack. Therefore it is hard to know if 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 & Ravne (2005).

Thomson & von Solms (1998) presents a novel set of guidelines for information security awareness training that easily could be used for education on social engineering. They actually use the same manipulative techniques that are used by a social engineer in order to educate more efficiently. They try to gently persuade the student into changing her security behavior. I find the paper to be interesting and highly useful. The approach should be studied further in a more domain specific context, and there is a possibility to develop a novel, and efficient approach to educating using these guidelines.

Once again, turning to the field of deception, there were a couple of interesting studies being done on educating users on detecting deception. These studies dealt with an interesting piece of software called Agent99, developed to train military personnel on detecting deception. This software uses a multimedia approach, and are, according to the studies, an efficient way of training users on detecting deception (Cao et. Al (2004), Biros (2005)). The lessons learned when developing this software, as well as possible the software itself, could probably be adapted into specific education for preventing social engineering. Marett et. al. (2004) also evaluates deception training in a military context, with a suggestion to study the field further.

2.3.1.1 General Aspects of Security and Education

Lee & Harley (2002) provide insights into the problems with security education, where they present some views that education is hopeless, because users do not want to be educated. Knowing this, in order to be useful, security education must be “maintained as strongly and vigorously as the technological aspects of the wider policy” (Lee & Harley, 2002, p. 81). However, they do argue that while security education does works if done well enough, it cannot be relied on as a complete solution to the problem. In the experience of Lee & 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 & Sasse (1999, p. 46) gives a set of guidelines for how efficient education on security should be performed:

- *Inform users about existing and potential threats to the organisation's systems and sensitivity of information contained in them. Awareness of threats and potential loss to the organisation is the raison d'être for security mechanism; without it, users are likely to perceive security mechanisms as tedious motions they have to go through.*
- *Provide users with guidance as to which systems and information are sensitive, and why. The current tendency is for security departments to treat all information as equally sensitive, with as little explanation as possible. Without such indicators and guidance, users tend to make arbitrary judgements based on their – usually patchy – knowledge and experience. Explain how security levels relate to different levels of information sensitivity.*
- *Provide users with guidance as to which systems and information are sensitive, and why. The current tendency is for security departments to treat all information as equally sensitive, with as little explanation as possible. Without such indicators and guidance, users tend to make arbitrary judgements based on their – usually patchy – knowledge and experience. Explain how security levels relate to different levels of information sensitivity.*

Conti et al. (2005) gives another view on how to educate users, more aimed towards security awareness. The idea is to train users to:

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

This approach will make the users more protected and resistant to attacks.

Björck (2005) also have some suggestions on the optimal way to educate the users. One of the recommendations are to use examples of previous security breaches, but it is important that the users understand the rationale behind the security rules, as well as 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 preventing social engineering attacks is to educate the users in transactional analysis; together with the 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 communications with others, the ego state the communicators are in influences the outcome of the communication, and

reflects on the individuals (Berne, 1996). There are a set of common counterproductive social interactions, most interesting from this area is the third degree interaction, in which one, or both, of the communicators might get hurt. This can be used to analyze the language patterns of social engineering attacks, and perhaps to train employees to be more resilient towards them.

2.3.2 Conclusion on the Problems Concerning Prevention

In the area of education on security, there are a lot of materials, both on traditional education that takes more time and resources from the end user, but also on security awareness, something that could be quite useful in this context. In trying to see what would be the best approach, one would probably need to actually test the efficiency of the approaches, and in order to do that, a metric is needed, leading back to problems discussed in 2.2 above.

However, once a metric has been devised for testing, it would be very interesting to do before and after studies, testing the efficiency of different approaches to education, such as in person, online, in group and perhaps even the Agent99 software , or similar, specializing in education on deception.

The other methods for 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" is costly and perhaps overly complicated. Only a very dedicated organization would employ it.

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

3 Research Framework

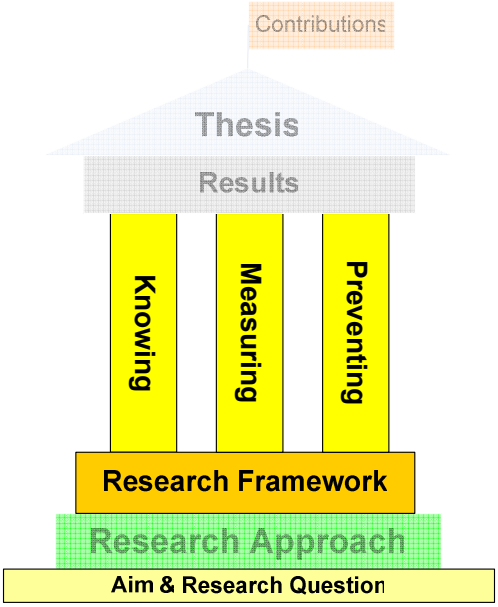

Figure 7: Research Framework (author's own.)

The first section deals with general security followed by sections about "social engineering" and Phishing that will be an introduction to the terms, as well as a presentation of some of the classic attacks that are useful to know about, especially for the reader not well versed in security. This is followed by a section on why it works is a description on psychological factors, as well as other factors, that can influence humans. The penultimate section deals with transactional analysis as well as Enneagrams to provide a short introduction to those psychological areas. The chapter is concluded with a short section on bots.

3.1 Information Security

In order to provide a basic framework for security in computing, there is first a presentation of *basic terminology*. Then a description of what kind of *vulnerabilities* information systems have, then some common *attacks* used on information systems. There is also a short presentation of a couple of typical groups of *perpetrators*. Finally there is a short overview of what kind of traditional methods for *defense* there are. This section deals with the more classic approach to security with a technical focus.

3.1.1 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 rapidly. This section is useful for the reader with limited insight into security.

Every part of a system needs a well balanced security. It is only after all the parts of the system have a reasonable protection that it can be said to be secure. (H SÄK IT, 2001).

Another important term is "Computer Security". Pfleeger (2003) and The Department of Trade and Industry (n.d.) argues that when we talk about "computer security" we mean three important aspects of the system:

- *Confidentiality.* Only those subjects who are entitled to access a resource access it. Access may also include printing, and knowing that an object exists.
- *Integrity.* The asset should only be possible to modify by those who are authorized subjects. This also includes writing, changing, and status changing, deleting and creating.
- *Availability.* Assets should be available to those who need them at the times when they need them. If someone has access rights to a resource, they should be able to access it.

A common demand from organizations is to have non-repudiation, also known as accountability, (used in a traditional legal meaning). The organizations want to be able to audit what decisions a user has made, in such a way that the user cannot deny making a decision (H SÄK IT, 2001).

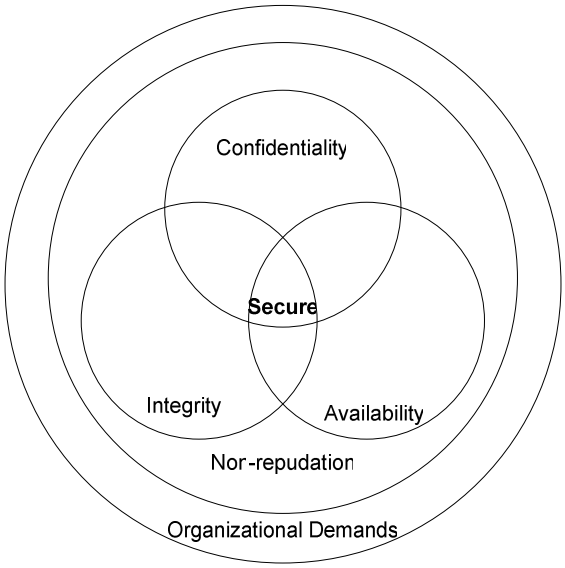

Figure 8: Relationship between aspects of security (the authors' own, inspired by H SÄK IT Hot (2001, p. 12) and Pfleeger (2003, p. 11)).

It is important that a secure system incorporates all these aspects, and that the aspects often, but not always, overlap. An illustration of how the aspects of security fit together can be found in Figure 8 above.

Physical security is the protection against physical damage or access to components of an information security system (Nickerson, 2000). H SÄK IT Hot (2001) also includes environmental concerns, such as weather. The typical example would be someone walking in to a server room and simply stealing a server to get to the information.

H SÄK IT Hot (2001) and Mitrovic (2001) also includes "Administrative threat" which is incidents that occur because of flawed routines or administration, for instance because of insufficient training or control functions.

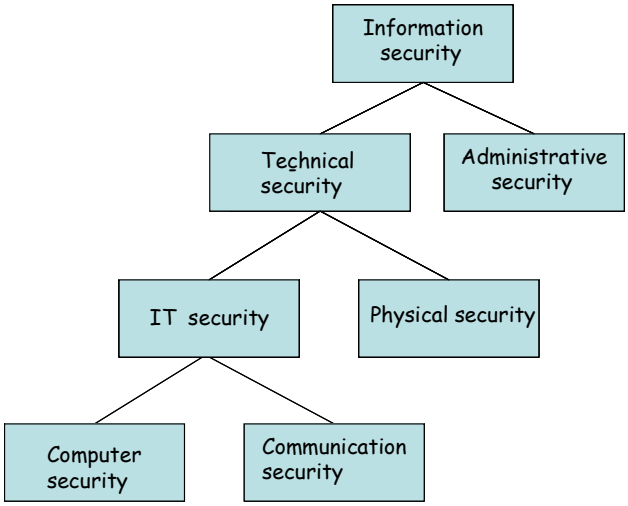

Figure 9: SIS illustration of information security, SIS (2003).

Another model for describing information security is the one used by the Swedish Standardization of Information Technology (SIS, 2003) where they argue that information security is the protection of information assets,

something done by maintaining secrecy, integrity, availability and accountability of information. SIS (2003) illustrates these terms in a hierarchical figure, where the terms in are also classified a hierarchical order, see Figure 9 above. I find that this model is suboptimal, especially in the areas concerning Administrative security that are poorly described. Considering the SIS model of security, my area of research would be based between Technical security and Administrative security, with the majority of work within administrative security. This would still not describe my work, as the limitations of the model are too great. Another area needs to be added to the model. A suggestion would be "Cultural" in order to cover a broader approach to security. The majority of my work would fit into this new area combined with the administrative area. The SIS model is more a model of the hierarchical set up of an information security organization, than a good description of the term information security in my opinion. In fact, the efficiency of social engineering attacks against a organization that has modeled its security tightly after the SIS-model would probably be great, due the attack falling "between the cracks" in the structure. A better model of security is the SBC model proposed by Kowalski (1994) which gives a more useful description of security, as seen in Figure 10 below.

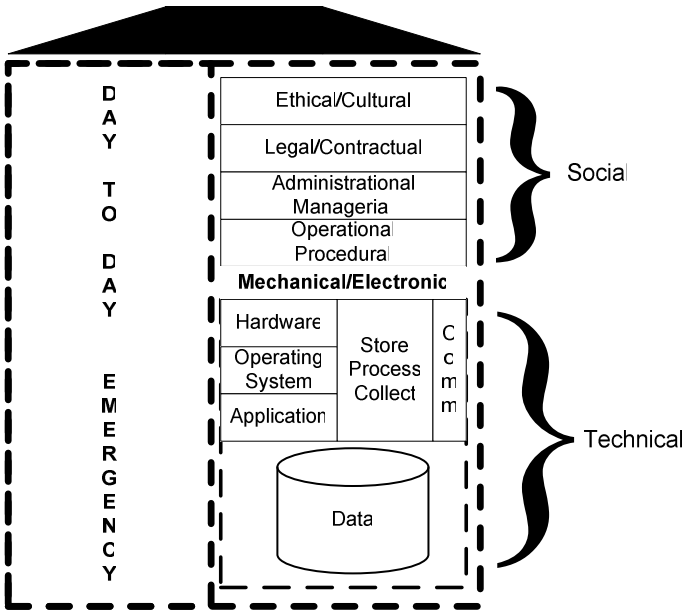

Figure 10: SBC Model, from Kowalski (1994, p. 19).

In the SBC (Security By Consensus) model a greater emphasis is put on a holistic approach, thus including the social aspects that are pretty much completely lacking in the SIS model above. 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 the use or own. It is notable here that the perpetrators are not included in the model due to the fact that is almost impossible to collect enough data on the perpetrators to enable a crime prevention program for IT crime (Kowalski, 1994).

Using the SBC model, my area of research would be based within the social area, except for the Legal/Contractual areas that are outside of my scoop. Some technical areas are also influenced, mostly "Communications" due to Phishing attacks, as described further in 3.3 below.

3.1.2 Perpetrators

An aspiring computer criminal must possess three qualities (Pfleeger, 2003):

- *Method*. He or she must have the skills and tools and other necessary resources to perpetrate the attack
- *Opportunity*. The perpetrator must have the time and the access to perform and succeed with the attack.
- *Motive*. There must be a reason for the perpetrator to perform an attack on the system.

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

Most people have a very specific notion of who the computer criminals are. They are pale, socially awkward teenagers with high IQ's, low EQ's and a desire for destruction. They are extremely good at what they do, and their competence often surpasses even the most skilled professional. At least, that is the way they are in the movies, and, perhaps, the way they were in the beginning of the computer era. But 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 the old days. The next phase was one where the gathering of information was the goal, and the phase we are in now is one where financial gain is the goal. The changing of goals has also meant changing of the perpetrators. Rogers (2000), updated in Wilson (2007), use eight categories of hackers:

1. The Novice: Often called script kiddies. Limited skills and often uses software developed by someone else.
2. The cyber punk: Young, often male, with higher skills. Often after high profile targets. No stranger to vandalism.
3. The Internal: Insiders using their access either for financial gain or for revenge if they are disgruntled.
4. The Petty Thief: Perpetrators, who starts of 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: Sees hacking as a challenge for the mind, and are quite curious. Often very skilled and also often lacking criminal intent. Will share their findings.
6. The Virus Writer: Mostly young males, mostly 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, using their skills for financial gains. Seldom caught, and working 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.

3.2 Social Engineering

Social engineering is a technique in which an unauthorized person manages to pose as an insider or an authority to successfully get 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). Perhaps the best definition was given by Mitnick 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."*

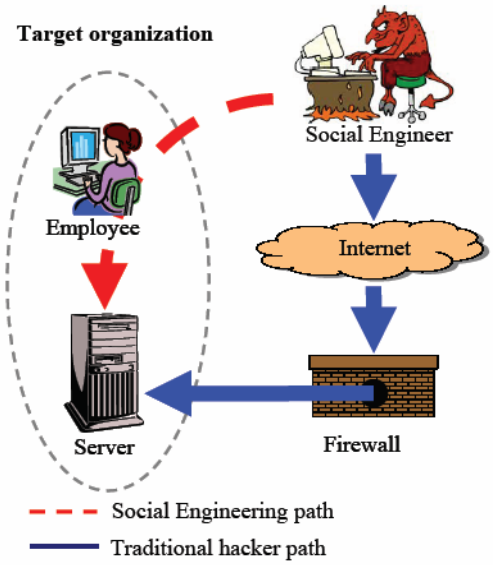

Figure 11: The social engineering approach (Hermansson & Ravne (2005) p. 17).

A social engineering attack focuses primarily on the people vulnerability, and is based almost entirely on using "the principle of easiest penetration" (Pfleeger, 2003). An illustration can be seen in figure 3. 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 2002 etc.). Social engineering can be used instead of, or in combination with, threats and bribes. The classic social engineer aims towards 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 2002). They can still be used, for instance by foreign intelligence officers (H SÄK IT Hot, 2001).

Social engineering is used because it is often much easier to simply ask someone, a mark, for information, than to prepare and conduct a complicated software or hardware attack (Granger, 2001; Mitnick, 2002).

A "mark" is the person being the target by the perpetrator.

3.2.1 Potential targets

Mitnick (2002) provides a list of typical targets for social engineering attacks. They are:

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

In general, typical targets are those that lack a certain insight into security, that work with helping others, that have high access rights, or specific knowledge, or 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).

3.2.2 Examples of Social Engineering Attacks

There is a vast selection of social engineering attacks and some of the classic examples are presented below. Most of the attacks, however, follow a typical attack cycle as presented in figure 4 below.

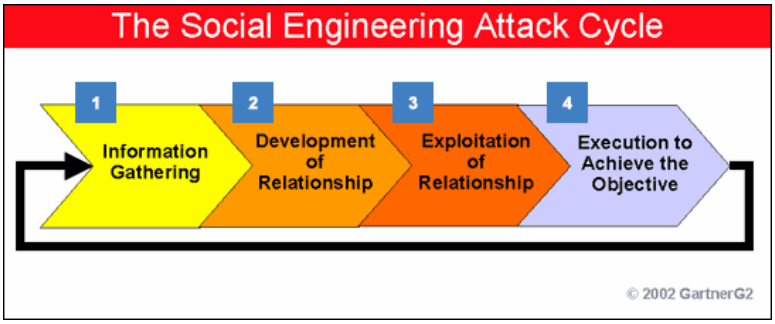

Figure 12: The Social Engineering Attack Cycle (Hiner, 2002).

The description of the cycle comes from Gartner (2002a):

The first step is to gather information. This can be information from public sources, such as phone books, web-pages etc. 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 human tendency 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 etc. This information can be the ultimate goal of the attack, or a starting point for the next stage.

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

The Technical Approach

A user suddenly gets a phone call where a person tells them that their system is not updated, and that it needs to be fixed as soon as possible. They tell the users to go to a webpage and install a piece of software they can download there (Gulati, 2003).

This is social engineering by using technical means (Mitnick, 2002). Other examples could be forged web pages.

Over the Phone (Pretexting)

Social engineers often prefer to use the telephone. It leaves no easily traced trail, is quick, and quite flexible. A classic example from Gupta (2002) is a perpetrator calling an unsuspecting employee, posing as technical support or some other preplanned background history (pretext). Beforehand, the social engineer has gathered information enough to be able to pose as technical support in a convincing manner. He then proceeds to ask the employee to run the command "ping localhost" and then acts troubled by the results. If the employee does not react to this, the social engineer calmly continues to explain that there might be the employee's machine causing trouble for the entire company. He then asks the subject to start performing ever more complicated commands. When the employee reacts and start to think it is hard, the social engineer offers to do the testing himself, if the employee would just provide him with her login information.

Dumpster Diving

A surprising amount of information can be collected gathered from the trash. This is something obvious to the paparazzi covering celebrities, and it is really obvious for the competent social engineer. Only imagination is the limit here, but some examples of highly useful information that can end up in the trash are:

- *Printing cover sheets.* Common practice in many offices and schools is to print a page with the users name and file name first when a print job has started. This can be used to learn the patterns of usernames, and since many users name their files quite descriptively, it can also be a basis for knowing what projects the company is working on at the moment (Gupta, 2002).
- *Post-It notes.* These are typically used for jotting down small pieces of information, such as telephone numbers, login information, server

names, email addresses and so on. Then they just get thrown away (Gupta, 2002).

- *Other examples* of sensitive material as given by Granger (2002) are: Calendars, phone books, organizational charts, manuals, vacation lists, policy manuals, disks and tapes, letterheads etc. Even if it is outdated, it can still be valuable.

On-Line Social Engineering

The on-line approach is often technical, as above, but can also be a combination. It is common for users to have the same password for several on-line services, making it an even more tempting target (Granger, 2002). Another method is to, by some means, perhaps a website, or by an e-mail, exposes the user to a pop up window, claiming network problems and instructing the user to log in again, using the window. When the user has "signed in" the window disappears, and everything continues as normal for the user. The social engineer now has the users password and login name (Gulati, 2003). This is similar to Phishing, discussed below.

Reverse Social Engineering

Perhaps the most advanced method of social engineering is when the social engineer manages to create a persona the victims are asking for information (Granger, 2002). There are three parts of a reverse social engineering scam (Mitnick, 2002):

1) *Sabotage*, where for instance the network is caused to stop functioning.
2) *Advertising*, when the social engineer establishes that he is there to help fix the problem.
3) *Assisting*, this is when the social engineer fixes the problems, by requesting certain pieces of information. Since the network is fixed, everyone is happy and no one at the target suspects foul play, and the social engineer has acquired the information that he needed.

Road Apple

The attacker leaves some kind of computer artifact where the mark might find it. It might be a CD, USB-memory stick or similar. It might have been made to look legitimate or even to look secret and classified. When the user use the artifact a Trojan horse is installed.

Desktop Hacking

Desktop hacking is a less messy approach to "dumpster diving". Most users never lock their screens while away from their workspaces, and they leave useful notes around their desks (Gupta, 2002).

3.2.3 Protection against Social Engineering

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, 2002; Gupta, 2002; Granger, 2002 etc.). Mitnick (2002) also provides a couple of guidelines to what should be taught to the

users regarding social engineering. It is what kind of attacks that can happen, how to detect and where to report. There is also a lesson on not to trust everyone.

Hiner (2002) presents a couple of clear guidelines when it comes to education for protection against social engineering attacks:

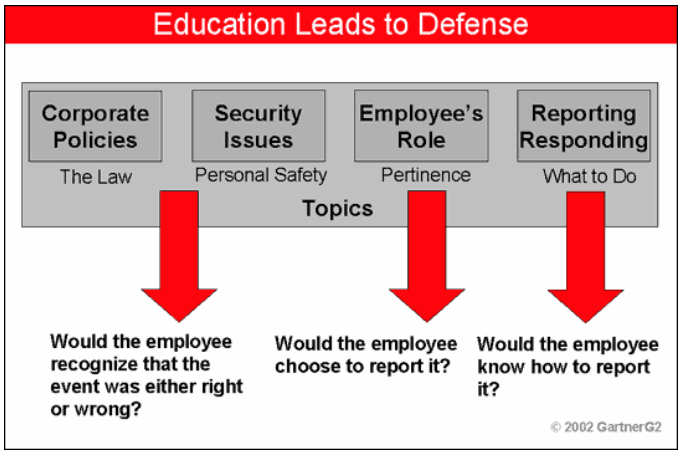

Figure 13: Education Leads to Defense (Hiner, 2002).

One should begin with 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 consider these three questions:

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

If the answer to any question is no, then further education is needed using the organizations security policy as a foundation. Figure 5 describes the different areas of the policy that should cover each of the questions above.

Other examples of things that are important to consider when building a defense against social engineering are (Hiner, 2002):

- Do background checks when hiring employees.
- Screen temporary and ancillary workers.
- Set up 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 cut down on disgruntled employees.
- Publish a formal written company 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 accompany visitors.

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

- Have clear, consistent, comprehensive and enforceable security policies.
- The single strongest defense against social engineering attacks is an educated employee.
- Establish procedures that eliminate *any* exchange of passwords.
- Avoid using passwords or authentication questions an attacker can easily discern with a little research.
- Security plans must be coordinated with physical/organization 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 defense in several layers:

Foundational Level: Security Policy Addressing Social Engineering

The foundation of any security is a thorough security policy (Gragg, 2002). This 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 user's resistance to persuasion because the users feel support from 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 key points are that the personnel must be able to realize when someone is trying to manipulate them, and the second is 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 in used in several ways, some examples by Gragg (2002):

- *The Justified Know It All.* This is a person who has been given the task to question why everyone he or she doesn't know is on the floor. Everyone should be questioned, and the person should have a decent knowledge of the security risks.
- *Call Backs by Policy.* Whenever any questionable request is being made by phone, personnel should do a call back, and check what number they are calling, so that it belongs to someone with suitable permissions. If, for any reason, a call back isn't 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 her target, users should be instructed to put any questionable user 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 either a *three-question rule* (three questions that only the real users could know, such as the name of certain pets) to use as a mean for identification. This is easy to remember, and should be available in a database for the personnel. Another mean of control are the *bogus question* that implies false knowledge, that the real user 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 realized. This should be part of an incident response unit, who immediately informs the users that an attack is in progress and what to expect. The unit also starts investigative work on who the social engineer is, and what the target really is (Gragg, 2002).

While Gragg's (2002) "Multi-layered defense against Social Engineering" probably does provide quite extensive protection against social engineering, it is also a rather big commitment for the organization, especially considering the fact that many organizations do not inform at all about the risks with social engineering.

3.3 Phishing

Before explaining Phishing further, it is probably important to explain the difference between Phishing and social engineering. In my opinion, the difference lies within the scope of the attacks, and the delivery. A social engineering attack is targeted towards a single, often specifically selected person (or organization), where a Phishing attack uses techniques used by spam in order to target thousands, or even millions, of users. The difference is, however, not always clear. 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). They can even be seen as simple variants on attacks on humans.

Microsoft, for instance, sees Phishing as the primary attack, while social engineering is simply a sub-technique used in Phishing (Microsoft, 2005a). Others view Phishing as simply social engineering using technical means (Mitnick, 2002). Whether social engineering or Phishing should be regarded as the "main" technique is not of crucial importance, as they are both targeted towards humans. In this thesis Phishing will be seen as Jakobsson (2005) does:

> *"Phishing can be described as the marriage of technology and social engineering". (Jakobsson, 2005, p. 3)*

Phishing is considered by me to be an attack mainly against the human element, and therefore a subset of social engineering.

3.3.1 What Phishing is

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

> *"Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware." (*Anti-Phishing Working Group, 2006).

Phishing typically use less personal means than a telephone for message delivery, e.g. e-mail or instant messages. This difference in the delivery, however, is not a definition shared by all. For instance, Microsoft has a broader definition:

> *"Phishing is a type of deception designed to steal your identity. In Phishing scams, scam artists try to get you to disclose valuable personal data—like credit card numbers, passwords, account data, or other information—by convincing you to provide it under false pretenses. Phishing schemes can be carried out in person or over the phone, and are delivered online through spam e-mail or pop-up windows."* (Microsoft, 2005a).

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, 2006a):

1) Acquire personal information.
2) Get the user to install programs.

Phishing should not be confused with Pharming, which is a technique of misdirecting the users to fraudulent sites or proxy servers, typically through

DNS hijacking or poisoning (Anti-Phishing Working Group, 2006). As this is a primarily technical attack, it will not be covered further in this thesis.

Spear Phishing

Spear Phishing is a relatively new technique that does not use the wide attack patterns of Phishing, but instead send highly targeted e-mails. The trick is to make the sender seem like someone the mark actually knows, or have a relation with. While the goal of Phishing is to steal information from an individual, the goal with Spear Phishing is to gain access to an organizations computer system (Microsoft, 2005b).

This specific targeting makes Spear Phishing much more dangerous than ordinary Phishing, and probably more prone to be used by professional attackers in order to get financial gains, trade secrets or even military information (O'Brien, 2005).

Spear Phishing could be seen as the "perfect" mix of social engineering and Phishing, and it seems that it is also a lot more efficient, and dangerous, than ordinary Phishing (O'Brien, 2005). It uses a higher degree of authority and the fact that the attackers pretend to be someone that the mark has a relation with.

Context-Aware Phishing Attacks

Jakobsson (2005) presents a novel possible future Phishing attack, where the Phisher not only uses techniques as those described in Spear Phishing, but also uses social context to send a message that not only are from a person that can be expected to send such a message, but also in a context and time where the recipient would anticipate receiving such a message, for instance sending a faked e-mail from eBay directly after the user has placed a realistically winning bid on an auction. This is a possibly devastatingly efficient attack, although it has not yet been reported in a large scale in the real world.

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.

3.3.2 Examples of Phishing Attacks

While it always has been a goal for computer criminals to acquire data and access to other resources, the name Phishing does not have a long history. The word comes from the analogy of fishing for information by using e-mails as lures, combined with the "classic" hacks "phreaking", using a child's toy to get free access to telephone systems (Trend Micro, 2005). The first mentions of the term online are from 1996, and the first media citation is from 1997 (Ollmann, 2004).

In the early days the primary goal for the attacks were America Online accounts, that then were used to trade for other services, such as pirated software (Ollmann, 2004).

Most of the communication channels used over the Internet can be used for Phishing attacks.

Attacks Using E-mail

The most common example of Phishing attacks are those that are done 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 14: Phishing example – e-mail text (Anti-Phishing Working Group, 2006)

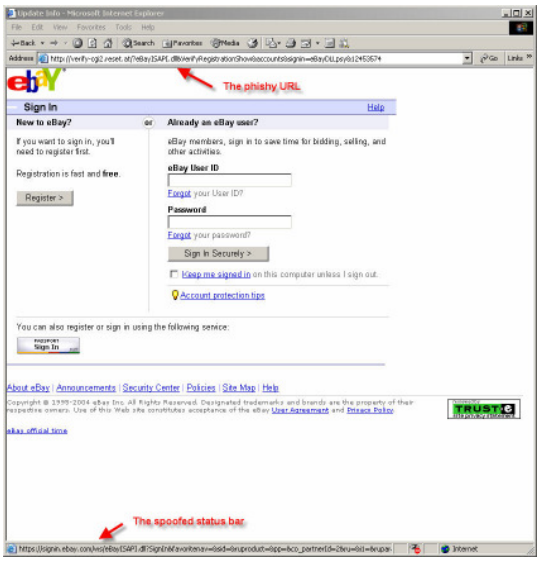

Figure 15: Phishing example – fake web page (Anti-Phishing Working Group, 2006)

An example of a Phishing e-mail sent out to thousands of eBay customers (as well as other Internet users) can be seen in Figure 15 above. The goal is to get the receiver to click on the attacked link, which will lead to an official looking webpage created by the attackers (as seen in figure 8), where the user might try to login using her information and thus, unknowingly to the user, submit the login information to the attackers.

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

- Official looking and sounding emails
- Copies of legitimate corporate emails with minor URL changes
- HTML based email used to obfuscate 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 for disguising the source of the email

Web-based Delivery

By using malicious web-site content, an attacker can perform a Phishing attack against the unknowing mark. This can be performed either on a website run by the attacker, or by embedding code on a third-party site (Ollmann, 2004). 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 are to use fake banner advertising and to obscure where the mark end up after clicking on the banners (Ollmann, 2004).

Instant Messaging and IRC

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

3.3.3 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 proper ways to act in order to avoid getting tricked by Phishing. In general, the advices 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 are protected.
- Keep an eye on your account balance.
- Keep your computer updated and use a firewall and anti-virus software.

There are also more technical approaches to protect against Phishing attacks. The most obvious are using anti-Phishing software, which in some ways tells the user if she is at risk or not. Some of the newer web browsers have this to some degree built in and there are software programs that can be downloaded to protect against Phishing, for instance the software developed by Netcraft (http://toolbar.netcraft.com/).

On 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 be vulnerable to Phishing attacks, by for instance employing encryption, digitally signed e-mail, using strong token-based authentication, monitoring of the system as well as strict host and linking conventions.

As these are mostly technical solutions, they will not be covered further in this thesis.

3.3.4 Impact of Phishing and New Threats

Stolen data can have many uses. Credit card information can be used to purchase goods and services, ATM card information might be used to duplicate ATM cards and use them for withdrawal of cash. Account information can be used to steal information or to be able to act as another user online (Trend Micro, 2006).

It is complicated to actually make reliable estimates on how successful Phishing is, because many of the victims do not know they have been fleeced (Hansell, 2004). It is also complicated to calculate the real costs, as it is not well known how successful the attacks are. Reasonably reliable sources are talking about costs in the area of $1.2 Billion a year in the US alone, and that 57 million Americans had received these fraudulent emails in the year 2003 (Gartner, 2004).

More recent findings indicate a continued increase in Phishing activity. Symantec (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. Anti-Phishing Working Group (2006) reports an increase from 8829 unique submitted Phishing reports in December 2004, to 15244 reports in December 2005.

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 Phishing attacks. In general, it seems the trend is that the motivation for computer criminals are no longer doing attacks for fun, or bragging rights, instead attacks are done more often by economic criminals, doing them for financial gain (Trend Micro, 2006). There are also suggestions that organized crime might be behind Phishing attacks (Hansell, 2004).

3.4 Why it works

There are a number of psychological issues that can be used to create the perfect environment for the attack. The easiest, and most obvious however, is to be kind. A bit of kindness goes a long way since most average users really want to be helpful (Granger, 2002). It is also common to disguise as a trusted third part; as a repairman, technician or manager etc. and to use the conformity factor: "everyone else is doing it" (Granger, 2002).

There is quite a selection of materials on influence, that to some extend explains why and how humans react to certain techniques of influence. Most of them are using the book "Influence" by Robert Cialdini as their primary source, something that seems to be the case with for instance the frequently cited study by Rusch (n.d.). Below are the six techniques for influence described by Cialdini (1993). They are highly likely to affect decisions, and therefore can be used to influence others.

One of the fundamental issues with influencing humans is the fact that a good motivation is seldom crucial when asking people to do something, it was found that simply using "because" is as effective as using it in together with an actual motivation (Cialdini, 1993). Another fundamental principle is to use the contrast principle, where e.g. something expensive is contrasted against something inexpensive, or in a security setting, something extremely insecure ("could you give me your keys, wallet and login") is contrasted against something clearly less extreme ("Could I get your login"). This is a simple technique, but it is often successful (Cialdini, 1993).

3.4.1 Deception

The attacks against the human element all use deception to some extent. Deception can be defined as:

> *"Everything done to manipulate the behavior of the other side, without their knowledge of the friendly intent, for the purpose of achieving and exploiting an advantage is deception. The "what" of deception is the manipulation of behavior. The "why" is to exploit the advantage achieved." (Feer, 2004).*

Deception is thus the reason to influence others. Wikipedia (2006) talks about two kinds of deception:

Dissimulation (hiding the real, (Bowyer, 2003)) deals with concealing the truth. This can be done by (Jordan & Goudey, 2005):

- Masking – camouflaging and/or hiding features that are nefarious.
- Repackaging – give new characteristics to the real, e.g. connect a Trojan to legitimate software.
- Dazzle – to shock or surprise etc., for instance sending nudity in an e-mail.

Simulation (showing the false, (Bowyer, 2003)) deals with exhibiting false information. This can be done by (Jordan & Goudey, 2005):

- Mimicking – spoofing or imitating reality, for instance a Phishing attack.
- Inventing – creating a new reality. E.g. false messages from Microsoft informing about attached security patches that needs to be installed.
- Decoying – create a diversion, for instance a divergence from the real object.

This can be seen as the basic toolkit to use for all deception techniques.

The efficiency of deception is made even clearer when one considers the phenomenon called "truth bias", the widespread assumption that most people are telling the truth (Martin, 2004) and the phenomenon "lie-detection bias", where individuals almost always overestimates their ability to detect lies (Marett et. al,. 2004).

3.4.2 *Authority*

People are likely to respond obediently to authority. We are often brought up to respect authority, and the extremes this can push humans to was shown by the famous Stanley-Milgram experiment (Obedience to Authority Study), where subjects thought that they were administrating electric shocks to other subjects, in order to test their willingness to administer painful, or potentially even lethal, doses of electricity while being told to do so by an authorative test supervisor. The study showed that a disturbingly large percentage (65 %) were willing to continue the experiment even though the subjects were administrating, to the best of their knowledge, extremely painful and potentially lethal doses of electricity (Blass, 2002).

But authority is not only someone telling us what to do. Other aspects are also influencing who we think are a person of authority. One example of this is uniforms. Uniforms are a cheap and simple way to be perceived as a person of great authority (Mitnick, 2002). Uniforms can be of the obvious kind (police uniform, doctor's coat, soldiers uniform) but perhaps the most effective kind of uniforms are those that we don't normally perceive as a uniform. Examples of this kind of uniforms are technicians and maintenance personnel's clothing and the clothing worn by the cleaners. This is a group of people that often tend to have full access to most areas, often at times

when there are little or non regular staff around, and they are also often employed by someone else than the organization in which they work. This gives them full access, and they are seldom questioned. Another kind of uniform is the title of a person, where an impressive title, such as professor, doctor, lord, sir etc. can influence the amount of authority we perceive that someone has (Cialdini, 1993).

Other examples that make us perceive someone as having authority are purely material artifacts, such as wealth, fancy clothing, jewelry and expensive cars. Humans are easily influenced by these things, and having the right clothes can make a big difference, something which is well known by con men (Cialdini, 1993).

The practical consequences of this weakness for uniforms and fancy attributes are that an attacker would benefit from using either a specific uniform to make desktop hacking easier, or for instance specific titles to make a social engineering attack over the telephone be more efficient.

3.4.3 Scarcity

When told that something they want is in short supply, people tend to want it even more. The information that others might be competing for the same thing triggers the sense of competition. This can be observed in ads everyday, where terms as “limited supplies” are frequently used. Time is always a factor, it is efficient to make the mark see that time is in limited supply, thus leaving less time for reflection (Cialdini, 1993). The things that are hard to possess, are valued higher and seen as better, than those that are easy to possess. This has interesting consequences on how people value information that are banned or made secret. When information is banned, humans have a greater desire to receive it, and they also have a more favorable attitude towards it than before it was banned. Humans also have a greater interest in what have become scarce, rather than what have always been scarce (Cialdini, 1993). That people value banned information more is a noteworthy piece of information for organizations that begin to employ more strict secrecy policies, or who have a rigorous security classification. It also explains some of the basics for the hacker culture: information wants to be free, because if it is secret, it must be interesting.

Scarcity could be used by attackers by providing a “limited service offer” or by pressing on time “Sure, I could help, but I’m leaving soon so we’ll have to fix it quickly”. Another consequence is that making information harder to get, could actually make more users interested in it, actually making it less secret.

3.4.4 Liking and Similarity

People favor others that are like themselves. If people share similarities they are more prone to react favorably to that person because of the similarity. One influencing factor here is the physical attractiveness of a person. A person who is very attractive can be perceived as a purely attractive person, where attractiveness is the dominating characteristic of the person. This is called the “halo effect” and it makes attractiveness a very influential factor (Cialdini, 1993).

Similarity can be of several different kinds, for instance how a person is dressed and a person's background and interests (Cialdini, 1993). This is also commented on in Neuro-Linguistic Programming, NLP, where a great focus is on developing rapport between people. In NLP rapport means being "in sync"with the person you are talking to. The common techniques are matching of body language, breathing (frequency) and maintaining eye contact (O'Connor & McDermott, 1996). Creating rapport increases liking, and is a powerful tool.

Other ways to increase liking is to have frequent contact with the mark, as familiarity increases liking, to share a common "enemy", to be in cooperation for mutual benefits, to meet during eating and to avoid meeting under bad conditions, as this also affects liking negatively, as do being the bearer of bad news (Cialdini, 1993).

This knowledge would be used by an attacker to befriend the marks, to build a liking, rapport, with the mark, for instance sharing an enemy (perhaps the boss), or by sharing a remarkable amount of interests. It is also practical for the attacker to have frequent contact (which is also used in examples by Mitnick (2002)) and to be basically a little more likeable than the regular person.

3.4.5 Reciprocation

If someone provides a favor for a person, the person feels that he should repay that service. Even if it was a favor the person did not want, he feels that he should repay it. This is a trick used by e.g. car salesmen who tend to tell customers that they really are doing them a favor by lowering the price, or by including rust proofing. Reciprocation is a very powerful technique that in many cases can be directly responsible for successful influence (Cialdini, 1993). One of the classic examples is the flowers that are given to passer-bys by Hare-Krishna's. The flower is free, they say, but it is customary to give a small donation in return. Even if the receiver of the flower does not want it, or even likes the Hare-Krishna's, he will feel obliged to return the favor, and to give a donation. In fact, this technique is so powerful that it is one of the major reasons for the success of the Hare Krishna's (Cialdini, 1993). The same thought is behind the free samples often given out at super-markets. Not only do they let the customers taste the product, they also have the aura of a gift around them, making it hard for people to resist buying the product.

What should be noted especially here is that people's sense of reciprocation will stand even if the gift is very small, and the request for return is far greater than what would be reasonable (Cialdini, 1993).

An attacker using manipulation on reciprocation would probably try to do a small, unwanted, favor for the mark to begin with, and then requesting a bigger favor in return. Here the attacker could also use knowledge from the contrast principle, which would make the suggestion even more powerful. If the perpetrator lower their first bid, the mark would feel obliged to do so too (Cialdini, 1993).

3.4.6 Commitment and Consistency

No one wants to be known as a failure. If a person has promised to do something, she will try her best to do it, to not be regarded by her peers as untrustworthy. Therefore people try hard to act consistent to the ways they have acted before. In the same way people find that they should stick to their choices when they have been made public in some way, when a stand has been taken. This is why a gambler is far more certain of the odds after placing a bid than before (Cialdini, 1993).

In order for a commitment to be most effective, it should be active, public and demand a certain degree of effort, and if a person is to accept responsibility for it afterwards, it should also be done without strong outside pressures (Cialdini, 1993). This have the interesting spin-off that it actually is harder to convince someone using a large bribe, or a really violent threat. This is something that was well known during the cold war, where most paid spies actually did not get paid a great deal of money. It was more efficient to get them to work for relatively little money, as they then would feel more personally responsible and to feel a greater commitment to the relationship.

Someone wanting to use this knowledge would influence someone could do it by trying to get the mark to express public support for the concept, as well as not making the support be too simple to express. If offering a bribe, it should be relatively small, and any threat made should be of the reasonable kind, not to spectacular, but threatening enough to "tip the edge". If it is too threatening, the mark will not feel obliged to follow through as soon as the immediate threat is removed.

3.4.7 Social Proof

People tend to rely on determining what course of actions would be the most appropriate when faced with a choice. People do this by seeing how others, especially those that are similar to themselves, in their vicinity act, a phenomenon known as "social proof". This is something that may cause people to do things not in their own self-interest. What is even worse, it can lead to a phenomenon called pluralistic ignorance (Cialdini, 1993). Pluralistic ignorance is when everyone is trying to see how everyone else is acting, leading to a situation where no one acts at all. This is most obvious in cases where crimes are committed in an area with a lot of witnesses and no one acts to help the victim, or when someone gets sick in the middle of the street and no one check to see if they are ok.

This could have a major influence on any organizations security, because people will adapt to the general attitude towards security in the organization. Even if management wants to have a high degree of security, the employees can nullify any attempts, unwittingly, by social proof. Examples of this are organizations where the sharing of passwords, while expressively forbidden in the policy, still is a sign of trust amongst employees. Not sharing would stigmatize a person as untrusting, paranoid, and not a part of the group as sharing is seen as a matter of trust (Brostoff et al. 2002).

An attacker could use this to enforce the techniques of persuasion by telling the mark that everyone else is doing what ever she ask the mark to do. If

there are proof, or if the mark believes this to be true, it would be very hard to resist the demand then.

3.4.8 Involvement

When the person asked to perform something has very little interest in it, they generally have low involvement. As they are detached from the task they are being asked to perform, they may easily be influenced by logical reasons for the task, urgency or authority. Examples of people with low involvement can be security guards, cleaners or receptionists (Harl, 1997). This group of people does not care as much about the quality of the arguments, but more about the quantity; the more the better (Harl, 1997).

In contrast, people with a high involvement, e.g. systems administrators, are persuaded more by the quality of the arguments, than the quantity (Harl, 1997).

A more general approach to why it works is the following: (Schneier, 2000, p 269) "People are basically helpful. And they are easily duped". People tend to actually believe that they will not be tricked or duped, making them easier to exploit (Brostoff et al, 2002).

3.4.9 Other factors that affect influence

Other factors that could influence people's choices are (Gragg, 2002):

- *Strong affect.* If the victim is feeling a heightened sense of anger, surprise or anticipation, he will be less likely to think through the arguments presented to him. This can be done either by aggravating the mark or simply by surprising him, with a demand that was completely unanticipated.
- *Overloading.* When someone has to deal with a great deal of information and does not have enough time to think about it, this lowers the ability to think critically about the situation. An example of this would be to present and require a lot of technical information from a person with very little technical knowledge.
- *Deceptive relationships.* A powerful psychological trigger is to establish a relationship with someone, solely to exploit that person. This can be done effectively by sharing information and a common enemy. The attacker does this by using techniques for creating rapport for a long time, actually building up a (false) relation with the mark, befriending her, and then slowly starts to use the relationship for nefarious gain.

3.4.10 Social Psychological Vulnerabilities

Jordan & Goudey (2005) creates an interesting taxonomy of social psychological weaknesses. They build on the taxonomy created by Harley (1998) and have adapted it for the most recent development in modern Internet worms. The end results are twelve categories of social psychological vulnerabilities (Jordan & Goudey, 2005):

- Inexperience: People who are ignorant to the security needs are obviously at risk.
- Curiosity: Human curiosity can make people do things that can be dangerous, such as opening attached files.
- Greed: Classic examples here are the Nigerian scams, as well as e-mails informing of free bonuses etc.
- Diffidence: Respect for authority.
- Courtesy: It is in human nature to be helpful, and humans have hopes for reciprocation even when helping stranger.
- Self-Love: Humans pay close attention on how others regard us, something that can be exploited for instance by someone asking one's opinion on something.
- Credulity: Most humans take everything at face value, an approach which probably is required for society to work. It does, however, present a notable vulnerability.
- Desire: In this case it is the material desire to own, and the fear of being left out of potential gains.
- Lust: One of the most powerful emotions. Not the same as desire, because it motivates on its own accord. For instance the promise of nudity, or even sex, can act as a motivator using Lust.
- Dread: The fear of harm to oneself, or something/someone treasured. An example is a threat of data loss if specific patches are not installed.
- Reciprocity: The obligation to repay favors and injuries, perhaps one of the most fundamental requirements for a working society. This can be done by suggesting that the mark is indebted to the attacker in some way.
- Friendliness: When being approached in a friendly manner, the reaction is likely to be friendly. An example of attack is for instance Christmas Greetings, birthday gifts etc.

This taxonomy can explain many of the vulnerabilities, and is, in my opinion, quite useful for understanding the human element.

4 Results from My Earlier Works

This chapter briefly presents my earlier work, as well as a synthesized view on the contribution with the earlier works.

Paper 1: System and Network Security in a Heterogeneous Healthcare Domain. Presented at the

The results show major variances in the level of information security in the different medical record systems and networks in the investigated healthcare organizations. Examples are: organizations' security requirements on the system; existing policy documents in the organizations; security mechanisms such as automatic functions for managing user accounts and signing techniques; and common security awareness in the organization, for instance, managing passwords, system logs etc. Variances are especially located in the medical record systems even if they also exist in the network system, for instance; organizations view of authentication, security in mobile devices; and management of logs.

The results also show that further research about security issues is necessary when different healthcare performers will exchange sensitive patient information in a distributed healthcare environment.

Paper 2: Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned. Presented at the 4th Security Conference, Las Vegas, USA, 2005.

In this paper a novel approach to doing social engineering penetration testing using a false pretext, thereby conning the users to be more honest when it comes to their security behavior was used. There are several benefits to using this quantitative approach to penetration testing for social engineering, the most notable are the ethical advantages, and that a far greater amount of employees can be audited, than by traditional means. It also indicates a very high degree of vulnerability to social engineering attacks, even among highly trained IT consultants.

Paper 3: Talking Security to Management: How to Do it. Submitted paper.

Seven security specialists working with management were interviewed about what management wanted to know about security, as well as other security issues and asked to fill out a scenario. This information was analyzed, and the major conclusion of the study is that managers are interested in knowing about security mainly regarding financial and strategic matters, formulated so that they can understand it and grouped in sets rather than individual detailed data. A trend of giving the users themselves more responsibility for security was also noticed.

A model for communication with management is presented.

Paper 4: User-Centered Security Applied on development of a Management Information System. Accepted to the HAISA 2007 conference.

The purpose of this study has been to do a user-centered security development of a prototype graphical interface for a management

information system dealing with information security. The interface was perceived as successful by the test subjects. The major conclusion of the study is that management uses knowledge of information security mainly for financial and strategic matters. To facilitate the need of management the study presents three heuristics for the design of information security interfaces:

1. Provide overview information very early in the program

2. Do not overwhelm the user. Management is not interested in the details of information security, but if they need details, they should be provided in a logical place.

3. Provide information in a way that is familiar to the manager. Provide contextual help for expressions that must be presented in a technical way.

4.1 Synthesized Results

Based on the results from earlier works, figure 9 below highlights the respective areas that have been studied this far.

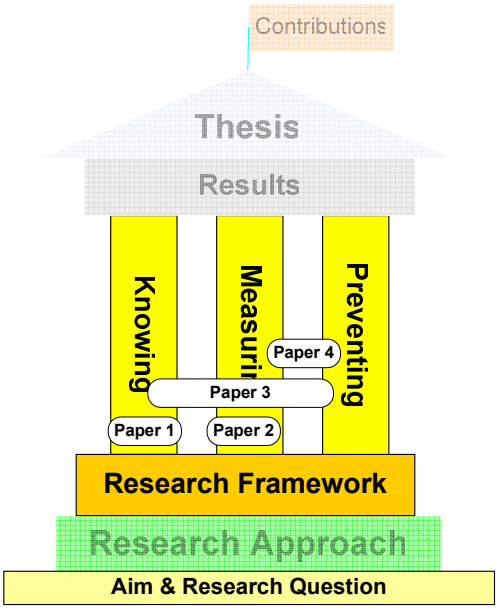

Figure 16: Synthesized results, author's own.

Paper 1 deal with getting to know the area, but its focus is not solely on the human element; instead it has a more general focus. This was somewhat corrected with paper 3, which covered both the knowing and the preventing aspect as it dealt with communicating security to management. The second paper dealt with how to measure vulnerability to social engineering, and the forth paper dealt with the development of a user interface for a security information system, something covering both the preventing and the measuring aspects of the area.

5 Research Approach

This chapter presents the research strategy, the methods to be used as well as a suggestion on the overall research process.

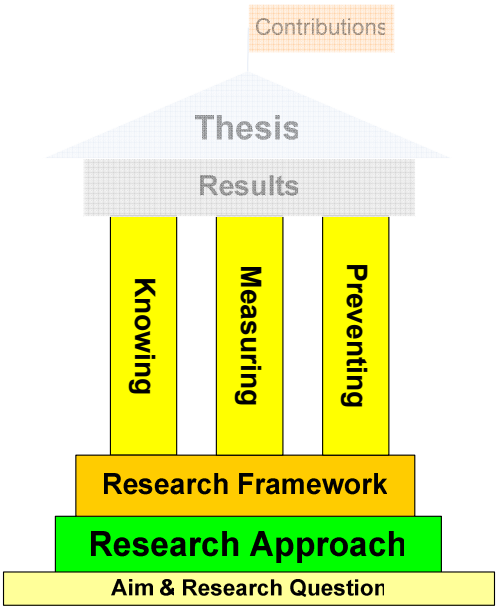

Figure 17: Research Approach (author's own.)

5.1 The Research Strategy

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

The intention with this research is not to base it on certain case studies on a single organization, but to try to achieve some more general knowledge, and to cover as wide an assortment of organizations as possible, in as many different businesses as possible. This gives a broader understanding, but it also exposes the research to the vulnerability of being too broad to actually offer any useful results, due to the variance of the studied organizations. This will be addressed by careful selection of both the organizations to be studied, as well as contrasting research where possible.

The focus will be on small to medium sized organizations. This is because of the different situations facing smaller organizations and the major ones, but it is also a delimitation made because of the problems to get major organizations involved in these kinds of studies. This delimitation mainly influences the areas dealing with prevention and measuring, as the knowing-area remains basically the same no matter the size of the organizations that is intended to be studied. If possible, however, at least one major organization will be studied to provide information and a broader understanding of the field.

There is little possibility of covering the whole field of the human element as it covers several research disciplines. It is unavoidable that there is a need to learn from other fields of research, such as sociology, psychology etc. while still maintaining the information systems focus.

One problem is when can the area be said to be sufficiently studied, in order to be able to draw any final conclusions? The easy answer is probably never,

due to the complexity of the field, but by doing sufficiently broad studies from enough viewpoints, a valid contribution can be made.

5.2 Data Collection Techniques

There are three different research methods more probable to be used. The first is the common quantitative study, to be used for instance in the evaluation of awareness training as well as in penetration testing. This method allows a larger group of subjects to be studied, and is also quite good at maintaining a sense of anonymity, something I believe to be extra important when studying human, individual, weaknesses.

The second technique is the qualitative approach, specifically interviews. This has been used in previous works, and will be used to further understand the area of human security, by interviewing experts. The interviews will be semi-structured, recorded and later transcribed.

The third technique is the literature study, which together with interviews will be used to form a broader understanding of the human element.

5.3 Expected Results of the Continued Work

A majority of the following results are planned to be included in the PhD thesis:

- A book chapter on why and how the manipulation of humans works. This chapter will focus mostly on the sociological and psychological aspects of security (Chapter 1, chapter proposal accepted).
- A paper evaluating the implementation of online awareness training on security in general, with a specific focus on the human element of security. The studied organization might be a major corporation (Paper 5).
- A paper using Transactional Analysis to educate users on how to identify social engineering attacks. This paper will give suggestions of how syntax analysis can be used to improve the "security awareness" training in an organization (Paper 6). Accepted to be presented at the International Transactional Analysis Conference 2007, San Francisco, California, USA.
- A further paper on the metrics involved with penetration testing for social engineering. This paper will contrast a couple of different metrics, in a couple of different organizations, with the aim to find the pros and cons with the approaches and mapping them against a taxonomy of attacks (Paper 7).
- A paper with a conceptual model of social engineering, describing to a greater extent how it works and what it involves. This model is to be validated by interviewing experts in the field (Paper 8).
- Using a combination of the knowledge gathered from the study in Paper 6, combining it with another personality test, Enneagram, a bot will be created that facilitates training and penetration testing for social engineering, while avoiding several of the ethical and practical

dilemmas of other penetration techniques, and also providing education to the users (Paper 9).

- A paper on the awareness of social aspects of information security among nurses in a health-care setting, using the SBC-model as a tool for analysis of the results (Paper 10).
- A paper discussing the problems with the current security market, and why it can be seen as a dysfunctional market, combined with an improved model using value chains to describe it. This is suggested as a new paradigm in information security (Paper 11).

The planned works described above, can be contrasted towards the previous works and the overall planning as in the figure below.

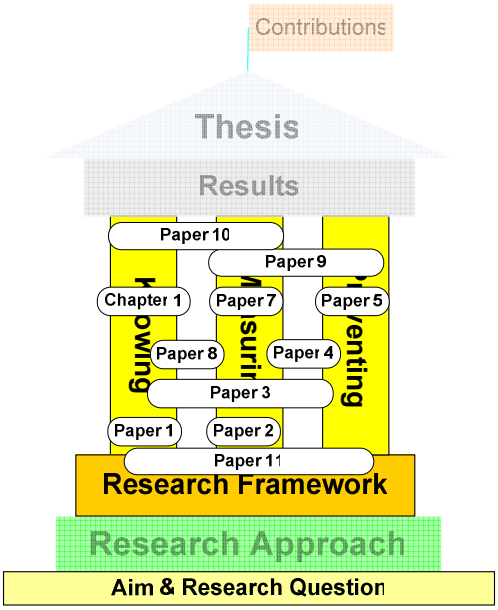

Figure 18: Synthesized results including future work, author's own.

5.4 Research Process

In Figure 19 below a broad planning can be seen, mostly focused on the order in which the materials will be completed, as well as an historical view of the order the previous materials were completed.

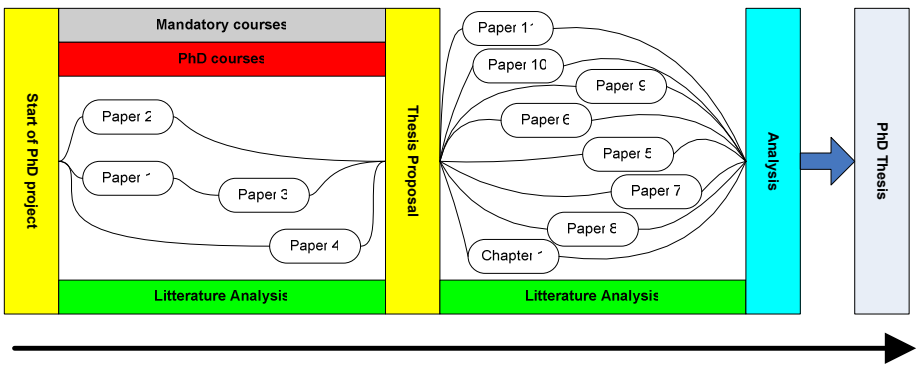

Figure 19: Research process, author's own.

This research is done in parallel with my work in an information security company, called Siguru. 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 etc. All in all they gave a good background and understanding of the field of research. Together with input and considerations acquired at conferences, symposiums, workshops etc. as well as the previous papers, this has been the background for the thesis.

The planned papers and the chapter are described further in 5.3 above.

Literature analysis does not consist solely of literature, but also an evaluation of the knowledge gained from seminars, conferences etc. and also my daily work as a security specialist. This is done in parallel to the writing of papers. Several of the different studies are going to be done, to some extent, simultaneously.

Using the classification presented in chapter 2 above the planned and the completed papers have been added in accordance to where they could be considered to be positioned. Some minor position changes have been made in order to make them legible. Most of the research will be/have been done in, or near, the informal research area with an empirical focus, as shown in Figure 20 below.

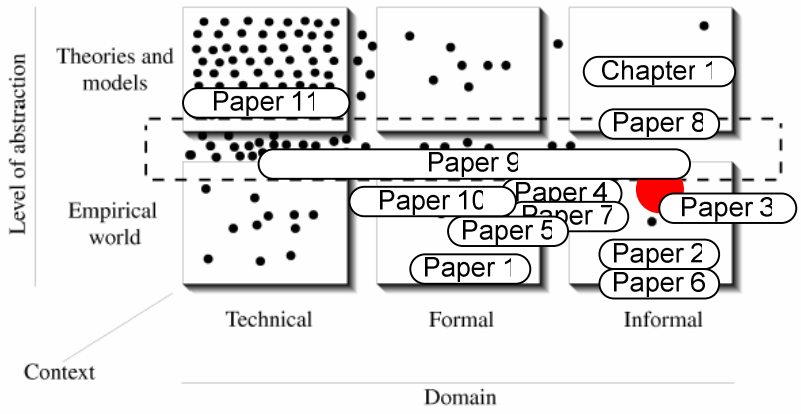

Figure 20: The classification of the 125 papers from the SEC 2000 proceedings (Björck, 2005, p. 234). The large, red, dot marks my research position, and the relative position of each paper/chapter has been added.

The analysis is the analysis of the materials gained to that point, and in the PhD Thesis part the summary, discussions, conclusions that can be etc. are formalized into a PhD thesis.

6 Expected Results and Contributions

The area of information security is filled with more or less efficient means for protection, products to be sold, experts with contradictory ideas and, perhaps even, snake-oil. While social engineering is an area to some extent free from commercially based research so common for instance in the field of anti-virus, it is also an area that has only been explored to a lesser extent. The ongoing trend of attacks on online banks where the users are, to some extent, the primary target, makes this research area highly relevant, and perhaps even necessary.

While research on the human element of security in general, and social engineering in particular, is complicated, lined with ethical dilemmas, and perhaps by some even seen as not purely belonging in the field of information security, this study is not only relevant, as shown by the literature, it is in fact perhaps even crucial. Because it is hard, because it is "un-pure", because there are complications, that is why there are such weaknesses today! Only if we embrace the area and try to learn from what is hard, and outside of our areas of expertise, can we prevent this attacks and bridge the gaps of our knowledge.

6.1 Expected Results

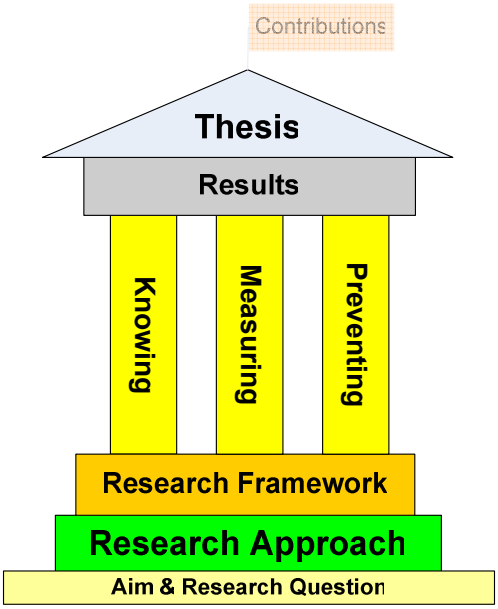

Figure 21: Expected Results (author's own.)

This research will use a rather broad approach will hopefully give useful and new knowledge to a wide audience, both academia and professionals. The broad approach might also prove useful for coming researchers, who can find a good starting point for further research in this thesis. The results will be presented in an academic manner, but it is certainly an aim that they should be highly useful for non-academia.

The results should be a vast improvement of today's knowledge of social engineering. This is achieved by merging knowledge from other disciplines, as well as trying novel approaches to both protection and auditing. These

results will be highly useful for professionals working within information security, as well as researchers in the field, which hopefully in the long run will lead to more secure information systems.

The PhD thesis will be a combination dissertation including the papers mentioned above.

6.2 Contributions

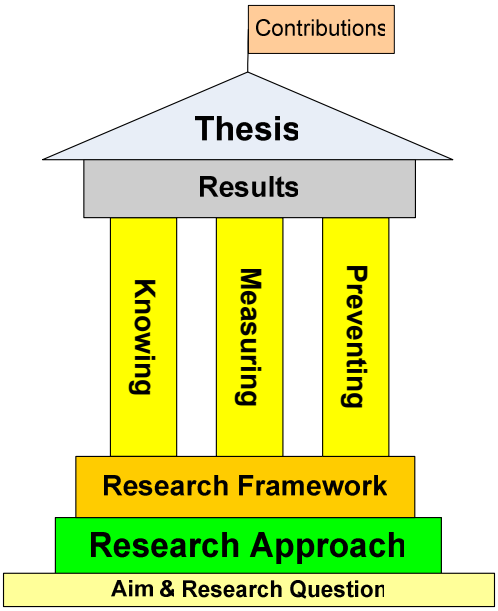

Figure 22: Contributions & complete figure (author's own.)

The concrete contributions from this research should be:

- A deeper understanding of the socio-psychological factors that makes people susceptible to attacks in the form of a book chapter. This should be able to give insights of how humans can be, and are, manipulated, especially useful for those with a limited knowledge of social psychology and an interest in information security.
- A conceptual model describing what a social engineering attack is, how it can be performed, the attack stages and what other factors that are involved. This will also include a taxonomy of attacks used today. This can be used to get a wider understanding of social engineering.
- Recommendations on the best approach on how to do social engineering penetration tests, as well as recommendations on how to do penetration tests for specific attacks. Some of these will be evaluated in practice; others will be suggested due to ethical considerations of doing the tests in an academic setting. This should be useful for most professionals working with audits and penetration tests, as well as for other academics in the field.
- Recommendations for protective measures, considering both education and novel approaches to protection. This is useful for organizations wishing to improve their protection, and for other academics studying penetration testing.

- A novel new tool to use for education, training and penetration testing of users in the form of a social engineering AI-bot. This bot will include most of the contributions mentioned above in an automated program that can be useful for both professionals and amateurs with an interest in the subject, as well as for education in a professional setting.

7 References

Adams A. & Sasse M. (1999) *Users are not the Enemy: Why users compromise computer security mechanisms and how to take remedial measures,* Commun. ACM 42

Anti-Phishing Working Group (2005) *eBay- 'UpdateYour Account.'*. [Online]. Anti-Phishing Working Group. Available from: http://www.antiphishing.org/phishing_archive/05-03-05_Ebay/05-03-05_Ebay.html [Accessed 23 Feb 2006].

Anti-Phishing Working Group (2006) *What is Phishing and Pharming?* [Online]. Anti-Phishing Working Group. Available from: http://www.antiphishing.org/ [Accessed 23 Feb 2006].

Bank, D. (2005) *'Spear Phishing' Tests Educate People About Online Scams.* [Online]. The Wall Street Journal. Available from: http://online.wsj.com/public/article/SB112424042313615131-z_8jLB2WkfcVtgdAWf6LRh733sg_20060817.html?mod=blogs [Accessed 2 Mar 2006].

Barret, N. (2003) Penetration testing and social engineering: hacking the weakest link. *Information Security Technical Report.* **8** (4), 56 – 64.

Berne, E. (1996) *Games people play: The psychology of human relationships.* New York, Ballantine Books.

Biros, D. P. (2004) "Scenario Based Training for Deception Detection." Information Security Curriculum Development Conference, (InfoSecCD 2004), September 2004.

Björck, F. (2005) *Discovering Information Security Management.* Diss. University of Stockholm. Report series No. 05-010, Stockholm.

Brandon, M. (2003-12-10) *IT-säkerhet till varje pris för svenska storföretag* [Online]. IDG. Available from: http://www.idg.se/ArticlePages/200312/10/20031210112521_ITB/20031210112521_ITB.dbp.asp [Accessed 10 Jan 2006].

Blass, T. (2002) *The man who shocked the world.* [Online]. Psycology Today. Available from: http://www.psychologytoday.com/articles/pto-20020301-000037.html [Accessed 9 Mar 2006].

Bowyer, B. (2003) Toward a Theory of deception, *International journal of. intelligence and counterintelligence,* 16, 244-279

Brostoff S., Sasse A. & Weirich D. (2002), Transforming the ”weakest link”: A Human-computer Interaction Approach to Usable and Effective Security, *BT Technology Journal* 19(3), 122-131.

Cao, J., Lin, M., Deokar, A., Burgoon, J. K., Crews, J. M., and Adkins, M. (2004) Computer-based Training for Deception Detection: What Users Want. Proceedings of the second NSF/NIJ Symposium on Intelligence and Security Informatics (ISI 2004), Tucson, AZ.

Cialdini, R. (1993) *Influence: the psychology of persuasion.* New York, Quill.

Conti G., Ahamad M. & Stasko J. (2005) *Attacking Information Visualization System Usability Overloading and Deceiving the Human,* Symposium On Usable Privacy and Security (SOUPS). Available from: http://cups.cs.cmu.edu/soups/2005/2005proceedings/p89-conti.pdf [Accessed 11 Mar 2006].

Dalrymple, M. (2005) *Auditors Find IRS Workers Prone to Hackers*. [Online]. AP. Available from: http://sfgate.com/cgi-bin/article.cgi?file=/news/archive/2005/03/16/national/w162055S07.DTL [Accessed 6 Mar 2006].

DeMelo, D. (2007) *Sutherland's Differential Association*. [Online]. Available from: http://home.comcast.net/~ddemelo/crime/differ.html [Accessed 29 Jan 2007].

Gartner (2002a) *There Are No Secrets: Social Engineering and Privacy" (TU-14-5662).* [Online]. Gartner. Available from: http://www.gartner.com/gc/webletter/security/issue1/index.html [Accessed 13 Mar 2006].

Gartner (2002b) *Protect Against Social Engineering Attacks, TG-14-7359.* [Online]. Gartner. Available from: http://www.gartner.com/gc/webletter/security/issue1/article2.html [Accessed 13 Mar 2006].

Gartner (2004) *Gartner Study Finds Significant Increase in E-Mail Phishing Attacks.* [Online]. Gartner. Available from: http://www.gartner.com/5_about/press_releases/asset_71087_11.jsp [Accessed 12 Jan 2006].

Gragg, D. (2002) *A Multi-Level Defense Against Social Engineering* [Online]. SANS Institute. Available from: http://www.sans.org/rr/papers/index.php?id=920 [Accessed 17 Sep 2003].

Granger, S. (2001) *Social Engineering Fundamentals* [Online]. Security Focus. Available from: http://www.securityfocus.com/printable/infocus/1527 [Accessed 18 Sep 2003]

Grazioli, S. (2004) Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. *Group Decision and Negotiation*, 13, 149-172.

Gulati, R. (2003) *The Threat of Social Engineering and Your Defense Against It* [Online]. SANS Institute. Available from: http://www.securitytechnet.com/resource/security/hacking/1232.pdf [Accessed 10 Jan 2006].

Gupta, A. (2002) *The Art of Social Engineering* [Online]. InformIT. Available from:

http://www.informit.com/isapi/product_id~%7B29543BE0-E535-4ADC-8FA5-E2C16295C8A1%7D/content/index.asp [Accessed 10 Feb 2006].

Feer, F. (2004) *Thinking About Deception.* [Online]. Available from: http://www.d-n-i.net/fcs/feer_thinking_about_deception.htm [Accessed 11 Mar 2006].

FraudWatch International (2006) *Tips to Protect Yourself from Phishing Scams.* [Online]. Available from: http://www.fraudwatchinternational.com/internet/phishing/protect.shtml [Accessed 8 Mar 2006].

H SÄK IT Hot (2001) *Handbok för Försvarsmaktens Säkerhetstjänst Informationsteknik Hotbeskrivning*

H SÄK IT (2001) *Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik.*

Harl (1997) *The Psychology of Social Engineering.* [Online]. Available from: http://searchlores.org/aaatalk.htm [Accessed 12 Mar 2006].

Harley, D. (1998) *Re-Floating the Titanic: Dealing with Social Engineering Attacks.* [Online]. EICAR Conference Proceedings. Available from: http://cluestick.me.uk/hoax/harley_eicar98.htm [Accessed 12 Mar 2006].

Hancock, B. (1996) *Can You Social Engineer Your Way into Your Network?* Network Security (Apr 96) pp 14-15.

Hansell, S. (2004) *Organized crime may be behind Phishing.* [Online]. New York Times. Available from: http://www.sfgate.com/cgi-bin/article.cgi?f=/chronicle/archive/2004/03/29/BUG8F5S1011.DTL [Accessed 5 Mar 2006].

Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes, E. (2005) Measuring Resistance to Social Engineering. In Proceedings of the First International Conference on Information Security Practice and Experience - ISPEC'05 (LNCS 3439), 132-143.

Hermansson, M. & Ravne, R. (2005) *Fighting Social Engineering.* [Online]. University of Stockholm. Available from: http://www.dsv.su.se/research/seclab/pages/pdf-files/2005-x-281.pdf [Accessed 12 Mar 2006].

Hiner, J. (2002) *Lock IT Down: Change your company's culture to combat social engineering attacks.* [Online]. Available from: http://techrepublic.com.com/5100-1035_11-1047991.html# [Accessed 7 Mar 2006]

ISACA (2004) IS AUDITING PROCEDURE SECURITY ASSESSMENT– PENETRATION TESTING AND VULNERABILITY ANALYSIS. [Online]. ISACA. Available from: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=18750 [Accessed Mar 10 2006].

Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F. (2005) *Social Phishing.* [Online]. School of Informatics & Dept. of Computer Science,

Indiana University. Available from: http://informatics.indiana.edu/fil/Net/social_phishing.pdf [Accessed Mar 10 2006].

Jakobsson, M. (2005) *Modeling and Preventing Phishing Attacks.* [Online]. School of Informatics & Dept. of Computer Science, Indiana University. Available from: http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf [Accessed Mar 5 2006].

Jones, C. (2003) *The Social Engineering: Understanding and Auditing* [Online]. SANS Institute. Available from: http://www.sans.org/rr/whitepapers/engineering/1332.php [Accessed Nov 10 2005].

Jordan, J. & Goudey, H. (2005) The signs, signifiers and semiotics of the successful semantic attack. Presented at the *14th Annual EICAR Conference*, St.Juliens/Valletta, Malta, 2005.

Kajava, J. & Siponen, M. (1997) *Social Engineering - IT Security Threat of Informatics* [Online]. Available from: http://iris.informatik.gu.se/conference/iris20/9.htm [Accessed 5 Oct 2003].

Krebs, B. *Paris Hilton Hack Started With Old-Fashioned Con* [Online]. Washington Post. Available from: http://www.washingtonpost.com/wp-dyn/content/article/2005/05/19/AR2005051900711_pf.html [Accessed 4 Mar 2006].

Kowalski, S. (1994) *IT Insecurity: A Multi-disciplinary Inquiry.* Diss. University of Stockholm. Report series No. 94-040, Stockholm.

Lee, A. & Harley, D. (2002). Back to the Future – Fresh Approaches to Malware Management. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings pp. 76-109. Copenhagen: EICAR. Available from: http://www.aomr.co.uk/papers/lee-harley.pdf [Accessed 5 Mar 2006].

Lindström, K. (2003) *Dålig kunskap om IT-säkerhet* [Online]. IDG. Available from: http://www.idg.se/ArticlePages/200312/01/20031201154919_CS/20031201154919_CS.dbp.asp [Accessed 1 Feb 2006].

Marett, K., Biros, D., Knode, M. (2004) Self-efficacy, Training Effectiveness, and Deception Detection: A Longitudinal Study of Lie Detection Training, Lecture Notes in Computer Science, Volume 3073, Jan 2004, 187 - 200

Martin, B. (2004) Telling lies for a better world? *Social Anarchism*, 35, 27-39.

McCullagh, A. & Caelli, W. (2000) *Non-Repudiation in the Digital Environment.* [Online]. First Monday. Available from: http://www.firstmonday.dk/issues/issue5_8/mccullagh/index.html [Accessed 3 Feb 2006].

Microsoft (2005a) *Help prevent identity theft from Phishing scams.* [Online]. Microsoft. Available from: http://www.microsoft.com/athome/security/email/phishing.mspx [Accessed 2 Mar 2006].

Microsoft (2005b) *What is spear Phishing?* [Online]. Microsoft. Available from: http://www.microsoft.com/athome/security/email/spear_phishing.mspx [Accessed 5 Mar 2006].

Mitnick, K. (2002) *The Art of deception.* Indianapolis:Wiley Publishing, Inc.

Mitrovic, P. (2001) *Handbok i IT-säkerhet.* Sundbyberg: Paginas Förlags AB.

Nickerson, R. (2001) *Business and information systems* (2nd ed). Upper Saddle River: Pearson Education.

Nohlberg, M. (2005) *Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned.* In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.

O'Brien, T. (2005) *Gone Spear-Phishin'.* [Online]. The New York Times. Available from: http://www.nytimes.com/2005/12/04/business/yourmoney/04spear.html?ex=1291352400&en=2f313fc4b55b47bf&ei=5088&partner=rssnyt&emc=rss [Accessed 12 Jan 2006].

O'Connor, J. & McDermott, I. (1996) *Principles of NLP*. London, UK: Thorsons.

Ollmann, G. (2004) *The Phishing Guide.* [Online]. Next Generation Security Software Ltd. Available from: www.ngssoftware.com/papers/NISR-WP-Phishing.pdf [Accessed Oct 8 2005].

Orgill, G., Romney, G., Bailey, M., Orgill, P. (2004) The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems, Proceedings of SIGITE'04, Salt Lake City, UT 2004

Pfleeger, C. (2003) *Security in Computing* (3rd ed). Upper Saddle River: Prentice Hall.

Post- och telestyrelsen (2003) *Oavvislighet* [Online]. Post-och telestyrelsen. Available from: *http://www.pts.se/internetsakerhet/Sidor/sida.asp?SectionId=1959* [Accessed 25 Nov 2003].

Post- och telestyrelsen (2006a) *Vilka är riskerna?* [Online]. Post- och telestyrelsen. Available from: http://www.pts.se/internetsakerhet/Sidor/sida.asp?Sectionid=1796 [Accessed 3 Mar 2006].

Post- och telestyrelsen (2006b) *Hur skyddar jag mig?* [Online]. Post- och telestyrelsen. Available from:

http://www.pts.se/internetsakerhet/Sidor/sida.asp?Sectionid=1858 [Accessed 3 Mar 2006].

Rogers, M. (2000) *A New Hacker Taxonomy*. [Online]. University of Manitoba. Available from http://homes.cerias.purdue.edu/~mkr/hacker.doc [Accessed 13 Mar 2007].

Rusch, J. (date unknown) *The "Social Engineering" of Internet Fraud* [Online]. United States Department of Justice. Available from: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm [Accessed 10 Sep 2003].

Schneier, B. (2000) *Secrets & Lies Digital Security in a Networked World.* New York: John Wiley & Sons Inc.

SIS 2003. SIS Handbok 550. *Terminologi för informationssäkerhet.* SIS Förlag AB. Stockholm (in Swedish).

Symantec (2006) *Symantec Internet Security Threat Report Tracks Notable Rise in Cybercrime Activity.* [Symantec]. Available from: http://www.symantec.com/about/news/release/article.jsp?prid=20060307_01 [Accessed 8 Mar 2006]

Tanneeru, M. (2005) *A convicted hacker debunks some myths.* [Online]. CNN. Available from: http://edition.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html [Accessed 1 Dec 2005].

The Department of Trade and Industry (date unknown) *The Business Manager's Guide to Information Security* [Online]. The Department of Trade and Industry. Available from: http://www.dti.gov.uk/industry_files/pdf/bus_man_guide.pdf [Accessed 17 Sep 2003].

The Department of Trade and Industry (2004) *Information Security Breaches Survey 2004* [Online]. Department of Trade and Industry. Available from: http://www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf [Accessed 8 Mar 2006]

Thomson, M.E., von Solms, R. (1998) Information security awareness: educating your users effectively. Information Management & Computer Security 6(4): 167-173

Trend Micro (2005) *Hook, Line and Sinker* [Online]. Trend Micro. Available from: http://www.trendmicro.com/NR/rdonlyres/8329E15A-B0B5-4392-AF55-C2E2B9A1601E/17124/PhishingPaper_FINAL.pdf [Accessed 11 Mar 2006].

Trend Micro (2006) *The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast.* [Online]. Trend Micro. Available from: http://www.trendmicro.com/NR/rdonlyres/D0FC5C5F-B8CC-4269-ADC0-ABF3B8DB7F6B/19323/TrendAnnualroundup.pdf [Accessed 11 Mar 2006].

Vroom C. von Solms R. (2004) Towards information security behavioural compliance. Computers and Security 2004,23(3): 191-198

Wagner, M. (2004) *Will Trade Passwords For Chocolate.* [Online]. Security Pipeline. Available from: http://www.securitypipeline.com/news/18902074 [Accessed 2 Mar 2006].

Wikipedia (2006) *Deception.* [Online]. Wikipedia. Available from: http://en.wikipedia.org/wiki/Deception [Accessed 12 Mar 2006].

Wilson, T. (2007) *Eight Faces of a Hacker*. [Online]. Darkreading. Available from: http://www.darkreading.com/document.asp?doc_id=120800 [Accessed 18 Apr 2007].

Åhlfeldt, R-M. and Nohlberg, M. (2005) *System and Network Security in a Heterogeneous Healthcare Domain: A Case Study.* In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.