2009

Information technology social engineering: an academic definition and study of social engineering - analyzing the human firewall

Nathaniel Joseph Evans
Iowa State University

Information technology social engineering: an academic definition and study of social engineering - analyzing the human firewall

by

Nathaniel Joseph Evans

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Computer Engineering

Program of Study Committee:
Doug Jacobson, Major Professor
Kevin Amidon
Thomas Daniels
Mani Mina
Roger Smith

Iowa State University

Ames, Iowa

2009

DEDICATION

This dissertation is dedicated first to my grandmother, Mary Lou Villinis. Without her wonderful example of kindness and patience, I could never have completed this. Second, I would like to dedicate this to Walt Disney, who has been a guiding light for me for since my internship in 2003. Disney said, "If you can dream it, you can do it," and that has been the magic that has gotten me so far in this process. When you put your mind to something, it's amazing how things fall into place. To all of my friends, pets, and family, this work is also dedicated to you. Your encouragement and support has been a blessing throughout this process. I could not ask for a better family, more loving pets, or better friends.

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

In order to succeed in this world, one must have knowledge: knowledge to do one's craft, knowledge to apply one's knowledge, etc. In short, knowledge is power. On the flip side, any company, government, individual, or power can be destroyed due to a lack of knowledge.

Security deals with keeping knowledge hidden and only available to those who need the knowledge. It's an extremely difficult job because security efforts must find each and every hole through which knowledge can slide though. All an attacker needs to do is find one hole, while, theoretically, the defender has to find and fix all holes.

People have knowledge and people control knowledge, whether through a computer, papers, or memory; people are ultimately in charge; and people are a hole in security. In order to fully understand security, people must be understood, specifically people's relationship with information technology networks.

However, very little existing research has studied the relationship of people to information technology networks. This work plans to contribute to the body of research that exists about social engineering to try to define and understand the problem of social engineering so eventually solutions can exist that will increase the security of knowledge and eliminate the security hole people so often create.

Why Should I Care About Social Engineering? Is This Even a Problem?

Over the past six days (June 1, 2009 through June 7, 2009), there have been 12 social engineering stories on Google. These include:

- a new scareware—a form of software which scares the installer into installing something detrimental to their system—introduced on Twitter, which makes the users believe they have a virus and the tool will remove it (Leyden, "Twitter Trends Exploited to Promote Scareware," par. 1-2).
- an article in *PC Magazine* detailing how malware from social engineering attackers outweigh malware installed through technical means by 10 to 1 (Seltzer, "Drive-by Attacks vs. Social Engineering," par. 1-2).
- a flurry of phishing attacks targeting bank customers of Commonwealth Bank (Constantin, "Flurry of Phishing Attacks Targeting Commonwealth Bank," par. 1-2).
- a story about a recently released keylogger, a piece of software that records key strokes. The story includes tips and suggestions on how to install the software on an unknowing person's computer (Battersby, "Sector Pro 2009," par. 1-2).

Over the last month, this number of stories increases to 250 stories, with and a little over 700 in the past six months. Clearly social engineering is making some headlines and is being featured in stories containing a variety of topics and ideas. However, let us look at some specific stories and surveys to see what type of mess are we dealing with.

An article published in 2008, stated that "Millennials buck IT security policies." This article explained how younger people are more inclined to combine personal Web applications with business applications. For example, according to the survey, 75% of employees 28 years or younger check personal e-mail at work compared to 54% of other workers, 66% accessed Facebook or MySpace compared to 13% of other workers, and 51% access personal finance

applications compared with 27% of older workers. 75% of them admitted to downloading software and installing it compared to 25% of the older workers, even when this downloading was against company policy. (Tucci, *"'Millennials' Buck IT Security Policies,"* par. 1-2). The claim that "Millennials buck IT security policies" is a dangerous claim as those Millennials are the future of the industry. As people get more and more electronically interconnected as the world metaphorically flattens, it will be interesting to see how this apathy shown by Millenials effects security.

Another story published earlier in the year shows that men are more likely than women to fall for Internet fraud. In fact, the Internet crime center shows that men lost $1.67 to every $1 lost by women. According to the author, "Men tend to fall victim ... to business investment schemes and some other schemes that have a higher dollar loss... Total losses from 2007 complaints came to $239 million, up $40 million from 2006." (McMillian, "Men Fall Harder Than Women for Internet Fraud, Study Finds," par 1-2). The last line in this article about the total losses is the most intriguing to me. When scamming becomes profitable, it matters less and less how legal it is.

"The Human Factor of Corporate Security," a story published a couple months later, showed that anyone, knowingly or not, can be recruited to spy against his or her interests or company. (Chabrow, "The Human Factor of Corporate Security," par. 1-2). Even the most loyal person can hurt the company by believing that they are helping the company. This idea of doing a favor and the concept of framing will be something I discuss about in a following chapter and is rooted deeply in psychology.

The Philosophy of Security

Security itself can take on many definitions and ideals. In order to understand how social engineering fits into the picture of security, we must first understand what I would like to refer to as the philosophy of security.

Companies and people have tried to define this term, the philosophy of security. The biggest problem is that security keeps changing, and what was a good practice or idea one day is outdated the next. This reminds me of a quote from a song by Weird Al Yankovic: "You say you have had your desktop for over a week, throw that junk away man, it's an antique. Your laptop is a month old, well that's great, if you could use a nice heavy paperweight..." Security is a very fast-paced, cutting-edge field and the specifics change on an almost daily basis. Security mechanism that were valid today may not be valid tomorrow. As such, research much be done to continue to innovate defenses in all of security.

Moreover, security needs to be thought of as a process and not as individual hardware or software technologies. This way when technology changes, as it inevitably does, the process can easily be applied instead of needing to change. This makes the policies much more realistic and thought out. Another metaphor to look at the difference between process versus specific knowledge is the difference between a university's bachelor's degree program and a technology institute's bachelor's degree program. You could say both teach science; however, the university teaches the concepts involved in science, how to think, and how to apply your knowledge even when the current technology changes, while the technical institute teaches what is needed to know to do the job now. Right out of school, the technical institute student has an advantage because he/she knows the most current ideas, but once those change, the university student becomes much more attractive. The process is more important than the specifics!

Ira Winkler stated the overall technology security concept very well:

> For example, a car is extremely complicated, probably more complicated than computers. Not only do you have to worry about the car itself, you have to worry about other drivers on the road, criminals who will vandalize or steal the car, failure of different components of the car, filling the car with gas, changing the oil, red lights, street signs, emergency vehicles, and so on. There is an infinite number of ways that you can be hurt either through your own actions or those of others. This could be very overwhelming, yet people get in their car every day and generally survive. (Winkler 13)

People seem to classify computers as something much more complicated than a car. If someone believes that something is impossible then it normally is. The approach to the idea of security needs to be manageable and positive. Savvy Internet users have no special training but only a little common sense and some very basic knowledge.

The idea of security comes with a series of questions, and this is the best way to think about this problem. How do you perceive what you are securing? Do you believe it is possible to secure said object? Is security a ubiquitous part of overall operations? How these questions are answered determines security.

In short, anyone can be taught to do a competent job in security. There is nothing special the average person has to know to decently secure his/her computer just like there is nothing special a driver has to know to drive his/her car. The driver doesn't need to be an auto-mechanic and the computer user doesn't need to be a security engineer. Everyone just needs to believe that security is possible.

What is This Paper About?

So now that we understand how to think about security, what is the rest of this paper about? As mentioned above, people are clearly the biggest problem in security. A person's mind is fairly easy to manipulate as shown in the fact that scams have been so successful and have been around since the 1800s. For instance, in 1849 William Thompson was tried and convicted as a "confidence man" who would ask people to borrow their watch and walk off with it (Halttunen 9). And before that a Scottish con-man tried to attract investors and settlers for a country which didn't exist, which he called Poyais (Sinclair 20).

In addition, people write all the software and design all the hardware, which have flaws that hackers or crackers take advantage of. Not only is a person's mind not to be trusted but also the actions that mind makes the person take. In short, we can blame every security breech on a person somewhere.

This dissertation has a threefold purpose all based on this idea that people are to blame for security problems. First, I hope this will show that social engineering is definitely a problem that needs to be researched further. To do this, I developed a survey and had agents perform a small social engineering penetration test on 64 companies. Using the data collected, I will show that social engineering is a problem and even draw some parallels between common security practices and the effectiveness against the ever changing attacks using social engineering. Second, I will help define the concept of social engineering, which is much more of a debated and confused term then most people realize. This will help people know what is included in the term and what is excluded from the term. Plus, I hope this helps clarify how complicated of an idea social engineering is. Third, I will provide a starting framework to help answer the common questions about social engineering: How is a social engineering attack performed? Why is the

attack successful? I hope to show some of the concepts and ideas that make sense and are commonly accepted in psychology and history and how they apply to social engineering.

This dissertation will show that people are not only to blame for every hole in security but also are a large hole in every company no matter size or specific type. Security tells us we need to find a method to fix this hole and prevent the vulnerability people present from being exploited. This dissertation will mention a variety of vulnerabilities people present in the security paradigm but will not lay out specific defenses for these attacks.

Summary of Chapters

Chapter 1: Introduction

The introduction will include an overview of the problem, including why it's important, a summary of new stories that exists in this area, and a discussion of how social engineering has not been explored in any sort of academic sense and is a weak link in security.

Chapter 2: Definitions

In this section, I show all the diverse definitions that exist for the term "social engineering." I plan to compare and contrast these definitions and define my own Information Technology Social Engineering (ITSE) term.

Chapter 3: Literature Review

In this chapter, I will show what areas have been well researched within the social engineering subject and where there are holes.

Chapter 4: Measurements and results

In this chapter, I will detail the method I used to obtain this data, explain the data itself, explain how I analyzed the data, and explain the results of the analysis. I also discuss the results given by "other" tests and publications and see if my results match what was stated but not shown in other publications.

Chapter 5: Conceptual reasons and models

In Chapter 4, I analyze a few different models of social engineering. One is the relationship between IT networks and the German Nazi party, which will be introduced in this chapter for the first time. The others will be analysis and summaries of already published models. In short, this section is an answer to the questions of "Why is social engineering a problem?" and "How is a social engineering attack performed."

Chapter 6: Corollaries and consequences

In this chapter, I will explain the parts of this research that could be expanded, and I offer some ideas and extensions for future work.

Chapter 7: Conclusion and contribution

This chapter will wrap up everything discussed earlier in the dissertation.

CHAPTER 2. DEFINITIONS

In this section I define terms and abbreviations I will use throughout the paper as well as spend considerable analysis on the core term for this dissertation, social engineering. The goal of this section is to clear up misconceptions that may exist.

Department of Homeland Security (DHS): This department is charged with "leading the unified national effort to secure our country against those who seek to disrupt the American way of life" (DHS, par. 1). This includes the obvious: protecting against hackers, terrorists, and criminals, but also includes natural disasters. DHS focuses on protecting the nation against current and future threats. As such, DHS performs a variety of disaster recovery tests on various places across the nation.

Social engineering: This section will elaborate on the definition of social engineering as it is used in information technology circles. There are many definitions out there and this section will analyze them and see what common threads tie them all together.

First, let us analyze the basic definition of social engineering. To people familiar with information technology, social engineering has many definitions, but even people outside of the field think of negative connotations for the term social engineering. This term makes people think of and remember the Nazi party "engineering" its citizens to be the perfect race. A simple Google search will reveal many places where social engineering can be applied as "the government engineering its people through social means." As you will see in Chapter 3, many similarities connect this definition with the definition used here.

To help separate the Nazi idea of social engineering from the hacker idea of social engineering, a new term was introduced called Information Technology Social Engineering, or ITSE (pronounced "itsy"). However, some controversy exists about ITSE's definitions, particularly about ITSE's nature and goals. The argument about the nature of ITSE comes from the idea that social engineering can be done without the use of a computer; so, it is technical or psychological? Does there need to be a technical piece of the manipulation to constitute ITSE or is being a run-of-the-mill con man sufficient?

The second argument revolves around the goals of ITSE. Generally, most authors agree that IT social engineering attacks have the goal of collecting a certain amount of data to be used later in a technical attack or a "hack" however others say that the goals don't matter and any motivation still counts as social engineering.

So, let us now take a look at some common information sources to see what everyone thinks about the definition of ITSE

Wikipedia defines ITSE as, "the act of manipulating people into performing actions or divulging confidential information." It continues to say that ITSE is "for the purpose of information gathering, fraud, or computer system access," (2009). This definition doesn't really comment on the technical vs. psychological argument, but it does take a very broad approach when explaining the goals. Under this definition, the con man borrowing people's watches and never returning them constitutes social engineering.

Moreover, Ira Winkler, one of the current experts in the field of ITSE wrote the following:

> To the unexposed reader, social engineering (ITSE) is the hacker term for performing non-technical attacks. To most hackers, these attacks are typically pretext telephone calls

> where the hacker pretends to be someone to dupe an unsuspecting person out of information that can get the hacker access to a computer. Sometimes social engineering refers to going into offices and looking around for information about computer systems, such as passwords taped to monitors (Winkler 8).

Winkler clearly shows the confusion present in the definition and shows how different people take different sides. For example, the unexposed reader took a side on the nature of ITSE argument, stating that the attack has to be non-technical and not mentioning the specific goals. Under this definition, something like e-mail phishing would not count as social engineering as it is a technical attack.

Matt Bishop mentioned social engineering only once in the textbook he wrote, titled *Computer Security Art and Science*. He classified social engineering as something not of the technical arena. He stated that "social engineering attacks are remarkably successful and often devastating," (Bishop 21). Furthermore, Charles and Shari Pfleeger wrote another widely used textbook about security called *Security in Computing*. They defined social engineering as the "easiest attack" and provided the following definition for social engineering: "Social engineering involves using social skills and personal interaction to get someone to reveal security-related information and perhaps even to do something that permits an attack." They went on to say, "The purpose of social engineering is to persuade the victim to be helpful," (Pfleeger 233). Pfleeger and Pfleeger tried to answer the questions above, but they didn't really take a side on the nature argument, while Bishop agreed with Winkler's unexposed definition. What they did take a side on is the goals argument, stating that social engineering's only goal is persuasion. Using this definition, an individual lying about all the break-ins he has had to convince his neighbor to build a security fence would classify as social engineering.

Hacking Exposed, one of the most recognized consumer hacking books, identified social engineering as "a description of techniques using persuasion and / or deception to gain access to information systems," (McClure 623). This "socio-technical attack," as it is called in the book, generally takes place in human conversation and is "a fusion of basic human trickery and sophisticated technical sleight of hand." According to *Hacking Exposed,* social engineering must not only be psychological but it must specifically be persuasion or deception.

A definition listed on one of the prime penetration testers for social engineering, RocketReady, defines ITSE as: "An attack based on deceiving users or administrators at the target site. Attacks are typically carried out by phoning or emailing users and pretending to be an authorized user to gain illicit access to systems," (Rocketready.com 1). This definition is a little more "hands-on," providing examples and mentioning users and administrators as the target, gaining access as the goal and deceiving as the method.

As these examples show, literature defines this term in quite a few different ways. As such I have formed my own definition and answered the important questions. This will be the definition that I use throughout this dissertation.

My definition for social engineering is as follows: People are vulnerabilities in the common security paradigm, which was discussed in the philosophy of security section above. Social engineering is the exploitation of said vulnerability. Unfortunately, as one of my favorite T-shirts states, "There is no patch for human stupidity." This T-shirt is an example of how people perceive social engineering: A problem with no solution. On the argument of the nature of social engineering, I take the stance of it being always psychological and sometimes technical. For example, a person who calls up someone pretending to be the help desk (a pretexting attack), the attack is generally considered non-technical but psychological. However, the same attack

occurring over e-mail is technical and also psychological. The psychological aspect of social engineering is what makes the attack, not the technical.

However, to limit the scope of a social engineering attack, I support the fact that the goal must be to obtain knowledge or permission to gain access to information technology. This access could arguably be physical, sitting in front of the computer, but if the digital data, generally in the form of a computer, is not present and all that was happening was an illegal entrance into the room, then social engineering has not occurred. If I break into your room and nothing is in there I have not committed social engineering no matter the method I used to break in. In contrast, if this room contains the control for a computer banking system, then I have used social engineering if the method was psychological.

A social engineering attack: A social engineering attack is an attack that uses social means such as deception and manipulation in order to gain access to information technology. An example of this would be an attacker calling up an employee, pretending to be from the IT team and convincing them to give up a password.

Pretexting attack: Pretexting is an attack in which the attacker creates a scenario to try and convince the victim to give up valuable information, such as a password. The most common example of a pretexting attack is when someone calls an employee and pretends to be someone in power, such as the CEO or on the information technology team. The attacker convinces the victim that the scenario is true and collects information that is sought.

Identity theft: Identity theft is an attack where the attacker steals a victim's identity in the form of a social security number, bank account information, or other personal information. The attacker can use this identity to take out loans, run up medical bills, apply for credit cards, or just steal money from the victim. This is a very hard crime to defend against. Some states don't even have laws against identity theft, placing the blame on the victim for not keeping their data secure (Schmidt 1-9). Due to this attack's social nature, pretending to be someone else, I believe this fits under the umbrella of social engineering.

Phishing: Phishing is the process of illegally obtaining information by faking an electronic communication, generally by pretending to be something real and legit. An example of this could be an e-mail pretending to be from a bank asking you to change your password. Sometimes these e-mails even look like a real e-mail or send you to a Web site that looks identical to your bank (Schmidt 41-50). Information technology professionals debate if phishing should be considered part of social engineering. However, as with identity theft, I think phishing fits within my definition of social engineering quite well and would classify phishing as a specific attack within social engineering.

Malware: Malware is software that is put on a victim's computer, generally without their consent. Malware has many purposes, including identity theft, phishing, or sometimes just general information gathering. For example, an attacker may collect all the Web sites you visit to help generate ads which may interest the victim. This, of course, may be helpful to the installer of the software (the victim), but it may also slow down his/her computer. The main difference between this and other software is the person who initiated the install. When the user

initiated it, it's called "software" and when someone else does it without the user's knowledge it's called "malware," (McClure 630-634).

Hack: A hack is a technical attack performed against a computer or server as opposed to a social attack described throughout this paper. Sometimes information gained in social attacks is used during a hack.

Social engineering attacker or hacker: This is the person who actually manipulates the victim through any medium, including e-mails, face-to-face conversations, or via phone calls.

CHAPTER 3 LITERATURE REVIEW

Introduction

Miles Orvell, a professor at Temple University wrote "One indication that a new scholarly field is emerging is the appearance of the conferences, journals and books on that theme." Judging by this criteria, ITSE still has a long way to go. In this chapter, I will lay out some of the work that has been done and highlight some large holes in ITSE research.

Curriculum Research

Douglas Twitchell of Illinois State University proposed a curriculum to teach social engineering attacks and defenses. In his study he showed that social engineering is only briefly mentioned in about 30% of security curriculums and ITSE defenses are never taught (Twitchell 1).

Agent Based Research

Some of the most interesting and newest research into social engineering was first proposed by Stephanie White in 2003 and involves an agent based system (White 1-2). This idea of fitting people, or agents, into models is an idea, which is catching on. This idea ties a process or a role to each individual agent or team to produce what Ms. White calls an "artifact" or simply a result (White 2). Argonne National Laboratory recently won a large grant to build an Agent Based Modeling and Simulation (ABMS) system to see how people effect complex processes such as social engineering (Macal, "Complex Adaptive Systems," par. 1)

Raymond Parks worded this well in an IEEE article he published called "Attacking Agent Based Systems." He stated that

> Intelligent, autonomous agents sense and react to their environment, learning from the effect that their own actions have on their environment. The more intelligent the agent, the more it is like a human mind, which means that agents inherit the weakness of human minds – gullibility. If the relatively new field of attacking computer security can be said to have a tradition, a major element of that tradition is the art of "social engineering", the action of influencing a human, or in this case, an agent to perform some function helpful to the attacker. Social engineering is the old con game with a new purpose. Agents operate according to algorithms and internal logic specific to their functions and can be social engineered just like human beings. Agent social engineering is limited by the range of senses and responses within the target agent. The attacker must present the agent with a sensed environment that will cause a response favorable for the attacker (Parks 2).

Agent based modeling provides a great method to study social engineering in a controlled atmosphere. Its current focus is only on attacks so it lacks the ability to develop defense mechanisms, except through the modeling of attacks. There is some potential with this thought process, but I don't see the logic in limiting the field to attacks only at this point.

History

There has also been a minor amount of research done concerning the history and evolution of social engineering. In 2004, Tim Thornburgh from Kennesaw State University discussed a little bit about what has changed throughout time involving social engineering. He traced this idea of manipulation through the dark ages into today explaining how it is in our nature to persuade and manipulate. He provided a lot of very interesting examples such as the

famous Trojan Horse story. Thornburgh introduced four stages of social engineering: research, developing rapport and trust, exploiting trust and utilizing information (Thornburgh 1-4).

Trust Model

These four stages are not a new concept and bring me to the next large area of research

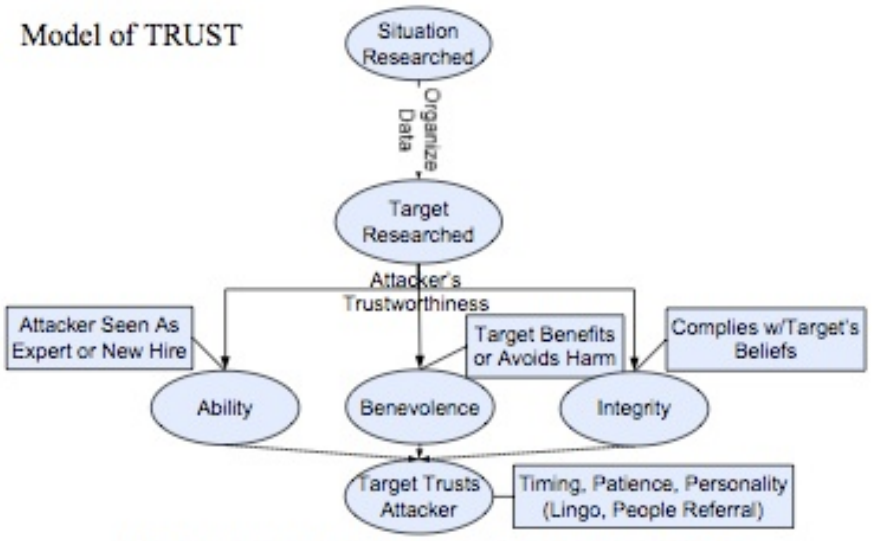

Figure 1: Social-Engineering Trust Model.

that has been performed regarding social engineering: the Trust Model.

The trust model as seen above lays out the groundwork to show how people develop trust relationships other people. This model shows all the ties which tie people together into trust circles (Laribee 2).

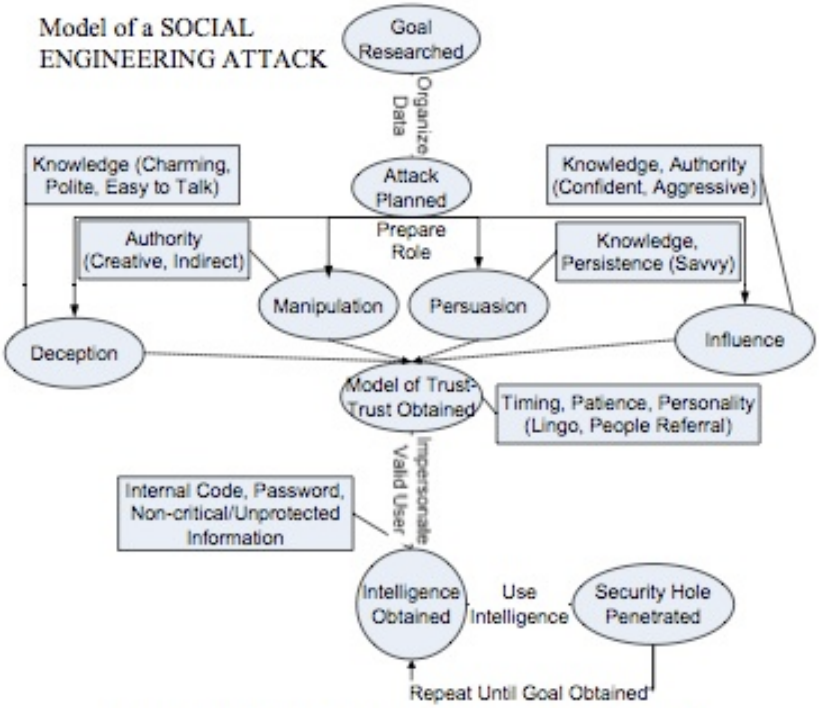

Figure 2: Social-Engineering Attack Model.

Some authors have even taken this trust model and even built an attack model on the top of it (Laribee 2). Moreover, quite a few authors have taken these trust models and built defenses on top of it including privacy regulations and rules (Orgill 2).

Missing Pieces

And thats about it. All of the research I could locate about social engineering could be classified into those areas mentioned above. The most developed area is the trust model, containing practical reaches into the attack and defense arenas. However, I don't hold much promise to there being a solution to the problem of ITSE by studying the trust relationships of people. This approach is very limiting and depends on the idea that every attack is an attack based on trust and the manipulation of the trust. Besides, as Tim Thornburgh mentioned earlier, people can never stop trusting others; it's too much part of our human nature.

I think a promising area is the agent based modeling. This model has a lot of unique ideas, potential, and benefits that will benefit social engineering research quite dramatically. As mentioned above, this has the ability to change and grow, and I believe it will be where the big breakthroughs happen involving behavior management.

As you can see, there isn't much existing core research about social engineering. Some of the most basic research involving the historical study to even the specific questions regarding social engineering's use today have not yet seen a considerable amount of work. However, as you can see from the sources, most of this research has happened in the last 10 years, and I expect to see a continued growth.

CHAPTER 4: CONCEPTUAL MODELS

Introduction

This section explores the prevalent concepts in social engineering attacks. These concepts help answer two questions about social engineering attacks: What exactly happens during an attack, and why are these attacks possible? Exploring these questions to determine the anatomy of an attack will help develop strategies to defend against these attacks.

The first concept that seems to arise when thinking about social engineering focuses on psychology. Psychology should be able to explain why people can be social engineered into giving up sensitive data. Accordingly, quite a bit of research has been done in regards to psychological persuasion, but, surprisingly, only one behavior concept has been applied directly to social engineering: neuro-linguistic programming. The following section explores how neuro-linguistic programming and other psychological principals apply to social engineering. This section includes summaries of research that has already been completed and some new thoughts and research directions.

While social engineering in the context of technology is a relatively new phenomenon, the idea of manipulation of a communication network is not a new idea and has quite a history behind it. In order to understand this problem, the second part of this chapter will take a step back beyond the common perceptions of the time and analyze manipulation in the context of one of the most famous large scale manipulations of all time — the Nazi Party manipulating the German people. By exploring the relationship between the individual and the Nazi state, I will draw parallels between the way the Nazis manipulated the German people into genocide and today's how nefarious characters — hackers — manipulate seemingly innocent people in the networked information technology world.

Psychology

Applying psychology, especially neuro-linguistic programming, to social engineering is not a long stretch by any means. People use language to influence each other, and social engineering is generally seen as tricking people into giving up passwords or giving up access. However, social engineering is really the same act as any other act of influence. People do many things to influence and "social engineer" people on a day-to-day basis. This could include lying to your boss when you're 5 minutes late for work, or saying you ate Chinese yesterday just because you don't feel like eating it for lunch today. People naturally lie and manipulate others for their own gain and language is the tool we use for this. If I want to communicate my thoughts to you and manipulate you, I have to use language either via conversation, e-mail, or on the telephone.

An interesting way to look at language is to think of it as a computer program. Language as a program or as a "thing" has one main purpose of communication. The words you hear are the inputs to language and the stream of thought is what comes out or vice versa. Either I listen to what you are saying and attempt to visualize it, or I try to put into words what I am visualizing.

More specifically, language has three main functions: deletion, distortion, and generalization (Stanojevic 5). Deletion removes unneeded information from your thoughts to simplify the transition into words. For example, while I type this paper, I might say "I am writing a paper." What you are missing is everything else, such as that my body is noticing the room is hot, I have a candle lit, and I am on a Macintosh laptop. All this extra information is deleted. Distortion effects what exactly I am doing or what is actually happening. For example

the same sentence above stated, “I am writing a paper;” however, I am actually typing the paper. The actual term was slightly distorted to help the listener understand the sentence. I like to call this the “dummifier.” Generalization takes what you are doing and generalizes it. For example in, “I am writing a paper,” I am actually typing the letter “I” now followed by the letter “space,” etc. Language generalizes what I am doing (Stanojevic 1-43).

According to Stanojevic, there are two major models used to analyze language, the Meta Model and the Milton Model. The Meta Model is what the brain uses to try to decipher and reconnect the meaning behind the words. This model tries to reverse the damage language does to the specificity of messages; it tries to reverse deletion, distortion, and generalization. For example a simple example is if I say, “The car drives to the store.” The Meta Model tries to reassemble this language into something you can understand, even though all the information is missing. What color of car? What kind of car? Did it go fast or slow? What store did it go to? All these pieces are not part of the sentence but you can still picture the message based on your experiences. This is very useful when trying to understand someone. The more you know someone, the more you can decipher using body language and what experiences you have in common to determine meaning. For instance if you and the speaker both drive a red car, there is a good chance you will be visualizing the same red car (Stanojevic 1-43).

In the context of social engineering, The Meta Model is usable only in data collection or recon. If an attacker it trying to find out information about you and you suddenly tense up when he states, “The car drives to the store,” at the very least that statement struck a nerve with you. Maybe you forgot something at the store today or maybe you had a loved one die on their way to the store. However, this model cannot be used to manipulate someone as it is only a data collector.

To examine the influence on the individual, we need to look at the other model, the Milton model introduced by Milton Erickson. He is regarded as one of the world's greatest hypnotists, and he noticed that the hardest way to convince someone of something was when you disagreed with what they thought (with the implication that you are smarter than they are). He came up with the idea that in order to influence people you need to convince them that they came up with the idea themselves and that they have been smarter than you all along. An attacker should make sure no one ever disagrees with him. The most common way to do this, as suggested by Erickson, is to lead victims through the argument using very big generalizations. For example, let's say the attacker and the victim disagree on the color of the ceiling tile. The attacker believes the tile is white, and the victim thinks the tile is gray. But, both will agree with statements such as "The tile is a color." An attacker, cyber or otherwise, would use these generalizations to help persuade and influence people to do what is wanted (Bandler 24-35).

Another key thing Erickson noticed was the lack of negation in our mind. In fact, the idea of negation really doesn't exist except in language. If I say the car is not driving to the store. How do you visualize that? You can only visualize the action then wipe it away. Yet another of Erickson's key ideas is the idea of tag words. If I say, "you will go to the store, won't you?" or "I am tall as a sign, aren't I?" That ending negation coupled with the earlier positive in the sentence confuses the mind. In a lot of ways this confusion is similar to a computer becoming overloaded because the mind has limitations on memory in the same way that a computer does.

For example, a study done by Mike Murray in 2004 showed that you are four times more likely to do what I command you to do if I preceded the command with a seemingly non-grammatical or complex sentence, than if I use a grammatically correct or simple sentence. This goes something like this: "Do you realize that you're not thinking right now of what I am not

saying? And can you realize that it's not that easy to not know what I am going to say next, but even when you're not knowing it I am knowing it and you're not?" When faced with a similar message, a brain just shuts down. It's very much like a buffer overflow. Anything done to overwhelm the brain creates an opportunity for influence (Murray par. 45-100).

But, what is it overflowing into? When a hacker uses a buffer overflow attack against a computer system, they overload a variable with so much data that they start to write into system memory, allowing them to do as they please. A person's mind doesn't have this type of system memory, but similarities can be seen in the idea of consciousness vs. unconsciousness in the human mind. People have a fairly small conscious mind and a very large unconscious mind, but most people don't realize all that their unconscious mind is doing. It is making the heart beat, controlling breathing, and monitoring nerve reaction, etc. The unconscious mind alerts the conscious mind using the critical faculty, which is the barrier between these two parts of the mind (Murray par. 45-55).

An interesting study about this overflowing idea examined two groups of college students. Both had to listen to a lecture on "why fraternities were evil." One listened via lecture only and were given a test over the topic. The other group listening to the same lecture but with a TV on. The second group was 50% more likely to be swayed by the arguments according to the test. It is interesting to see that the second group, which was clearly more distracted due to the television being on seemed to absorb the information more thoroughly. Not only did they absorb it, but they were persuaded by it (Murray par. 66-67).

Using buffer overflows to affect the mind works well. Another manipulation trick taken right out of the computer hacking textbook is "fork bombs." A fork bomb is a program or script

that opens an exponentially growing amount of processes on a system by duplicating itself. For example, a simple fork bomb on a Windows computer looks like this:

```
:c
start %0
goto c
```

:c is the name of the program, start %0 starts a copy of itself, and goto c returns to the top. So the first time this program runs, it creates a copy of itself and starts over, then two programs make copies of themselves, then four, then eight, 16, 32, 64, and so on.

The same process can be done on the mind. Tell a story. Don't finish. Tell another story, don't finish. Tell another story. Repeat. This cyclical pattern is actually used quite a bit during political speeches. Politicians talk about taxes, immigration, foreign policy, etc. They don't finish each idea until much later and this style almost makes it appear boring to the listener. That "zoning out" is what allows the speech giver, or attacker if that's the case, to put real information directly into the listener's unconscious mind (Bandler 24-35).

All these manipulation tools almost seem like back doors into the human mind, but the biggest tool is part of the language program we discussed earlier. In order to listen to a sentence we have to visualize it (Bandler 24-35). In the above example, negation was used in the statement, "The car did not go to the store." In order to process that language one has to translate the words into the images in the mind then erase those images. However, the mind has already generated the images. Negation allows an attacker to control what a person is visualizing if only for an instant. The same process works with questions, if an attacker asks the question,

“Can you imagine what it would be like to give me your password?” The victim has now thought about giving the attacker his/her password. By reading this you have given me control—to some extent—of your mind because the question introduced an idea or a concept into your consciousness. At this point, in the case of cyber attacks, the attacker has the victim confused and visualizing the act. The attacker now has some form of influence over the victim, which may be all the attacker needs to make someone act on that influence.

People generally will not act against what they believe. There is a built in set of morals people develop over the years and these morals are very difficult to break. However, the field of psychology has defined a way around this, called framing. Framing, or priming, states that if one is put in the right context, he or she will do things inconsistent with established values. Context is more important than content.

Milton Erickson experimented with this idea of framing. He was a military hypnotist and was in charge of finding a way to get a subordinate to kill his commanding officer. The military trains people to follow orders and respect the chain of command very well. Simple hypnosis would not even come close to working because the officers truly believed they shouldn't kill. The training had instilled within them morals that told them, “Do not kill your commanding officer.” However, put the same message of killing an officer in the right frame and things change completely. If the commanding officer is said to be a traitor suddenly getting someone to go against his or her values becomes possible (Erickson 70-76).

How does an attacker put people in the right frame of mind? Robert Cialdini identified three frames that would be very useful to an attacker.

- *Reciprocation*. When someone does something for a person, her or she wants to do something back. This is how timeshares sale pitches work. Timeshares give people enough free stuff, such as a free night stay or a free meal, and you want to give something back to them and purchase a timeshare. People are generally nice, and so it is said that the best way to seal a friendship is to ask a favor of that friend. Receiving a favor is stronger for a relationship then doing a favor. In the case of social engineering, the attacker might do a favor for the victim to entice the victim into reciprocating (Cialdini 76-82).

- *Social proof*. You walk down the street and see two restaurants. One is completely empty and one is packed with lines out the door. Generally, people decide to go to the busier restaurant. People trust what everyone else thinks, even though they may have just been following what the people before them thought. In the case of cyber attacker, an attacker just needs to convince the victim that everyone else is doing whatever the attacker is (Cialdini 76-82).

- *Authority*. People generally do what those in authority tell people to do. In social engineering, an attacker might try to establish authority over others by pretending to be the boss or part of the IT team (Cialdini 76-82).

Put people in the right frame, ask the right questions, and the chance of succeeding is greatly increased.

Neuro-linguistic Programming

I remember the first conference I attended, The Computer Security Institute's NetSec in 2005. There was a course titled "Neuro-Linguistic Programming (NLP)" and had the description as follows:

> *Advertisers use it, many Federal agencies teach it to their operatives, and psychologists use it to gain patient trust, now you can learn these valuable social engineering skills. These secret concepts are rarely taught outside of a closed circle practitioners. Used properly, these skills will help you gain the trust and confidence of anyone, from your children, to helping your staff comply with security rules. This How-To session gives you a model for impactful communications and skills in influencing a subject's experiences. Learn 3 key power moments in conversations, understand the concept of and state 4 ways of making people feel at ease, in any situation. Learners will be able to practice these skills during this session, so mastery comes easier in the "real world." Articles, on-line references and a checklist make this session valuable for anyone who needs to gain the trust of others. Someone could be using these on you right now!* (Smith 1).

Ever since reading this description, the concept of NLP has intrigued me very much. I attended the conference session and have talked with Brad Smith quite a bit since then.

Neuro-linguistic programming is "a model of interpersonal communication chiefly concerned with the relationship between successful patterns of behavior and the subjective experiences (esp. patterns of thought) underlying them" and "a system of alternative therapy based on this which seeks to educate people in self-awareness and effective communication, and to change their patterns of mental and emotional behavior" (Grinder). Brad Smith took this idea

and applied a social engineering framework to it to help explain the anatomy of a social engineering attack.

Specifically, NLP takes the concepts from counseling and psychology and applies those behaviors to explain how people manipulate others into giving up information or how people give information without knowing it, similar to covert channels. For example, when an attacker is trying to convince someone to give up a password using a pretexting attack, it may sound something similar to this:

Victim: Hello. How may I help you today?
Attacker: Hello. I am from the IT Department. What is your password?

Generally, something like this doesn't work or shouldn't work. However, in a study performed in 2008 in London, 80% of people would give up their passwords with a simple question like this and a bribe of 5 Euros (Egan,"20 Idiots Give Up Password for £5 Mark & Spencer Department Store Voucher," par. 1).

However, let us assume that most companies train their employees to have some common sense and at least adhere to the most common security principle: "Trust no one until they prove it" or as Ronald Reagan would say, "trust but verify." Someone looking to employ the use of NLP usually will do so with a little more finesse and manipulation than simply asking for information.

Indeed, the psychology behind counseling and behavior manipulation involves persuasion. Our brain listens to the words of persuasion but our unconscious hears the gestures, voice tone, speed, pitch, and eyebrow movement. This non-verbal communication is how people

can read various connotations in the language and how two identical sentences can have very different meanings. People tend to look for these clues and use them to interpret messages. These non-verbal cues let the victims trust their "gut" and allows an attacker to manipulate that trust in our ability to interpret statements. Let us add some style, voice tone, speed, and pitch to the cyber attack above and see how it sounds.

Victim: Hello. How may I help you today?

Attacker: Hello. My name is Adam. (Pause) I am from the (raise voice for next 2 words) IT department upstairs, and I was wondering if you would ***please*** *(pause) help me and tell me your password?*

That sentence feels and sounds much more believable. A key point in NLP manipulation is that one cannot make someone else change—that's his or her decision. If the target did not want to give up their password, you would not be able to make them change their mind. People generally act in their own best interest, for their own reasons and are always looking for "WIIFM" or "What's in it for me?" Consequently, to be successful a cyber attacker's offer needs to be specific and attractive to the individual. An attacker must show that this request meets a need, both a need for the attacker and the person being attacked. This motivation could be many things from a desire to succeed, to making a difference, or even just being remembered.

The cyber attacked process suggested in NLP counseling by Mike Murray is as follows:

1) Ask them what you would like them to do or what you recommend.

2) Give them a reason and use the word "because."

3) Sincerely ask for help.

4) Give them a chance to say "yes."

(Murray,"The Science of Social Engineering" par. 3-5)

Now, let us add some motivation to the attack mentioned above and see what it looks like:

Victim: Hello. How may I help you today?

Attacker: Hello. My name is Adam. (Pause.) I am from the IT department upstairs, and I was wondering if you would ***please*** *help me. I was recently changing passwords and I accidentally changed yours. I am so* ***sorry*** *for this inconvenience. Can I please have your old password so I can change it back* ***because*** *I really don't want to cause you any hassle?*

This attack is much more persuasive than the original attack or even the second version because it includes motivation.

NLP also includes the concept of "power moments" and "power words." Power moments are moments that are the best time to act, and include three main moments: "Thank You," "Yes," and "No." The first two seem pretty obvious:

"Thank you for working late on Friday."

"You're welcome. How about that raise?"

However, "no" requires a little more explanation. But, remember that power moments are moments that offer an opening or an opportunity.

"No."

"How about you tell me how long your password is then?"

Another key concept in NLP is the idea of power words, which are words that have hidden influence on people. These words are have used by politicians, advertisers, and salespeople for years to manipulate people and crowds. Power words include things such as *sale, free, bonus,*

select, unique, limited, secret, secure, family, safe, and *love*. For example, an attacker may send you a phishing e-mail talking saying "CLICK HERE FOR A **LIMITED** TIME **SALE**!" or the infamous "I **Love** you" e-mails popular a few years ago. It even works cross culturally assuming good translation (Smith 2003).

Process

Originally, NLP was created by John Grinder and Richard Bandler as a model of how communication impacts and is impacted by subjective experiences (Smith 4). The theory was developed to help people, and four simple steps were created:

1) Speak to others with direction (power words).

Make sure statements are descriptive, use all senses, and the engage memory recall. For example instead of saying, "I ate chocolate today" say, "I had chocolate today that was melting in my fingers. I couldn't help but smack my lips from the pure chocolate smell."

2) Make yourself believable (facials).

One should do some motion whenever he or she wants others to remember something. For example, someone could raise their eyebrows while saying your name. This is a subconscious, micro-motor way to get recognized in others' minds.

3) Speak like those you are speaking with.

Match speaking partners' pitch, speed, and word choice because "birds of a feather flock together."

4) Sit like those you are speaking with.

Match conversation partners' body language.

Conclusion

NLP provides many principles, which when combined with the psychological principles above, allow for numerous access points into a person's mind, and, thus, access for social engineering. This section has hopefully tackled some of the many "hows" when talking about social engineering.

IT Networks and Nazism: Unwitting participation

In 1969, ARPAnet—the original Internet—was created and computers were interconnected effectively for the first time. The Michigan Terminal System and many other systems tried similar less effective things long before. While many of the details of how computers communicate with each other have been worked out, such as security mechanisms and a variety of protocols, the idea of how people fit into the computer communication network still is a fairly new idea.

One new method to think about how computers communicate with each other and how people fit in is the most basic model of computer communication, the OSI Model. The OSI Model, developed in 1977, consists of seven layers that describe how computers communicate with each other. These layers include the following (in order from top to bottom): application, presentation, session, transport, network, data link, and physical. Recently, the idea of people or "the user" has been added to the top of the OSI model, creating eight layers.

Placing "user" at the top layer of the model makes a lot of sense, and doing so will draw some interesting comparisons. The OSI model was built to help people understand that each layer can only actually communicate with the layer above or below it; however, a layer can

virtually communicate with itself on another machine. The best way to describe this concept is with an example.

If a machine is communicating using an IP address, it would be found on the network layer. To communicate with another machine it would need that machine's IP address, and it would look as if traffic was going from one IP address to another. However, quite a bit more is actually going on in this simple example. The IP address is translated to the layer below (the data link layer) where it becomes a mac address, and it then is transformed to the physical 1's and 0's, which are transferred across the actual wire to the destination machine. That machine then receives this data via the 1's and 0's, which it translates up to a mac address and eventually back to an IP address.

This same type of process holds true for the user layer. When a user uses a computer to send an e-mail, as far as the user is concerned, they are communicating directly with the person they are sending an e-mail to. However, this e-mail is actually being communicated down all the layers, across the wire as 1's and 0's, and back up through all the layers to the receiving user. To the user, all this translation is transparent: The only translation a user understands is that an e-mail address translates to a person. Many people view the Internet just like they view the transmission in their car. It works and they don't care how or why. However, a car transmission, unlike the Internet, cannot be used directly for malicious purposes to cause someone else to lose money or steal information.

Hackers try to manipulate a communication network to gain access to data and systems they should not have access to. The idea of using social means to manipulate an individual into unknowingly giving up sensitive data is known in information technology circles as social engineering. This effort to manipulate a communication network is, surprisingly, not a new idea

and has quite a history behind it. In order to understand this problem, I will take a step back out of the common perceptions of the time and analyze manipulation by one of the most famous large scale manipulations of all time—The Nazi Party manipulating the German people. By exploring the relationship between the individual and the Nazi state, I will to be able to draw parallels between the way the Nazis manipulated the German people into genocide and the way nefarious actors—hackers—manipulate seemingly innocent people in the networked information technology world.

The Nazi State

Historian Kevin Amidon defined the Nazi state as a system for the "generation of complicity" (Amidon 103-37). The Nazi leadership set up everything in society, such as industry, education, and politics, in ways that set groups against one another in competition to look like the best Nazis. Below you will find details about the ways in which the Nazi state as a whole generated complicity. Hitler was at the center of this system and to some extent generated complicity, but he wasn't alone. He, along with a group of other Nazis leaders around him, worked the system of complicity out ad-hoc (similar to how a wireless network is set up). To manipulate the German people, the Nazis used a few key techniques, which have much similarity to networked information technology systems.

Technique 1: Bring a whole bunch of smart people trying to gain prestige and to be productive in the system and use their ambitions and talents to strengthen the totalitarian system (put everyone in its service). To do this the Nazi system had to embrace technology and encourage the growth of technology.

Gottfried Feder, an engineer who designed a concrete ship at the end of WWI (a notable though not economically viable achievement), stated that technology was bound to the soil and the nation (Peukert 94). This idea of connecting technology to the Nazi ideals served to help motivate intelligent people to participate in this generation of complicity. These scientists and engineers participated in this system in order to become successful. The Nazi system encouraged these intelligent people to help design the system, but in order to do so they needed to progress deeper into the system of inclusion and exclusion. This set up a competition, in which scientists competed with other scientists to not only come up with the newest and greatest ideas but also to include and exclude the right races. Even Fritz Todt, a leader in the design of the Autobahn system, got in on the action and sketched a plan, which Hitler supported, to put industry and technology in a central role of Nazi society (Peukert 94). However for all his support of Hitler, Todt was killed in a plane crash in suspicious circumstances in 1943 after he started to doubt that Germany could win the war.

The same drive for productivity can be found on networked information technology systems. This drive is what originally started the big dot com bubble that saw online companies for everything from diapers to T-shirts pop up. The desire for productivity forced people to either modernize and industrialize or be left behind. With the reduced cost of shipping, suddenly a world of cheap labor opened up and companies began to globalize and outsource production. This idea, as referred to by Thomas Friedman, is called the "flattening of the world." This "flattening" of the world has put the Internet, a network of computers, central in the lives of many, much like the Nazi system put this idea of inclusion and exclusion central to the lives of everyone involved (Friedman).

Technique 2: Pick specific people to exclude (communists and Jewish people in particular) as being nefarious or, as the Nazi's put it, "unworthy" or "impure." This strategy created a constant sense that something—or someone—was endangering the system. As a result, all who wanted to participate in the Nazi culture had to also be involved in the process of excluding the "bad guys." And so this new world of inclusion and exclusion drove everyone who wanted to participate into even greater levels of participation until complicity stopped being simply going along and became actually perpetrating crimes or what we might even call evil.

In a culture like the Nazi culture, an individual derived his sense of having a place in the world only from his belonging to a movement or his membership in the party (Arendt 323). Hannah Arendt called this movement a "classless society." Indeed, totalitarian movements like the Nazi movement are mass organizations of atomized, isolated individuals, rather than a collection of groups. Compared with all other parties and movements, totalitarian movements' most conspicuous external characteristic is their demand for total, unrestricted, unconditional, and unalterable loyalty of the individual member (Arendt 323). Totalitarianism, as defined by the Nazi culture, was best described by Hannahh Arendt as "...a form of government together with its accompanying ideology."

On the Internet, with the invention and popularity of forums and blogs designed so individual users can share their thoughts, people have created a "classless society" where "every word is created equal." This idea can easily be taken a step further to the current political debate about the Internet—the concept of net neutrality. Net neutrality states that every packet is created equal as it travels across the Internet. This can be a good thing in the sense that everything is given equal rights and everyone and anyone can share information. However, this

can also be a bad thing because everything, even nefarious packets, can be transmitted equally across the Internet.

Another concept Hannah Arendt touched on was the "banality of evil." Evil happens because someone like Adolf Eichman focused on rubber stamping papers rather than the larger implications of orders on the papers he was stamping. As a result, it didn't matter if those papers were railroad car tickets or orders for the deportation of 400,000 Jews from Budapest to the gas chambers. The focus was on the paper and the focus on the banal bits of activity. Getting your work done and not thinking about the broader picture creates a causal link between the banal focus on minor bureaucratic activity and destructive consequences resulting from that bureaucratic activity (Arendt 300-400).

This type of tunnel vision is also a concern in information technology. The function of the system in IT networks is not transparent to the people who work on them, and in many cases people desire not to know about how the structure functions, a common feeling for most who use all types of technology. But users not knowing how IT networks function may be a danger. Hackers can use IT networks to steal passwords, credit card numbers, and a variety of other private data by gaining access to even one system. For example, most people couldn't care less how the transmission works in your car but just cause you don't know how it works doesn't mean it can be "caused" by someone else to murder someone or cause a million credit numbers to be released to criminals.

In less than one hour, an unpatched computer system running the Windows operating system placed on the Internet will be taken over by numerous programs. These programs may be simple spyware, which inform some company of your browsing habits, or simple malware, which allow a hacker to use your system to attack other networked systems. When the innocent

individual who owns the computer is tried for this crime, they generally try to defend it by denying that they knew what they were doing. This idea of causing others to do the evil work because of their naivety is a common connection that can be made and a common defense used during the Nazi Nuremburg trials (Grodin 40).

Technique 3: Use propaganda to scare people into participation. According to Hannah Arendt, "the masses have to be won by propaganda" (Arendt 341). Propaganda is rampant across the Internet in the form of ads. It is hard to travel around the Web without seeing some advertisement for something somewhere. Generally these advertisements try to scare you into checking your computer's security settings and purchasing some software.

In some ways, these ads, which try to convince you that your computer is infected, or the spyware around the Internet, which acts like a scanner saying you have a virus (Windows AntiVirus 2008), constitute terror. The bad guys are trying to convince you that something is wrong and you need to secure your system by purchasing this product. In a lot of ways the same can be said for some legitimate business practices. For example, the idea of a virus scanner is a necessity for most people with a Windows computer across the Internet. However, these are also sold for Linux and Macintosh systems, both of which would constitute an even low risk of getting a virus. The companies scare the customers into purchasing the product in the same way that hackers do it for their own profit.

"Terror continues to be used by totalitarian regimes even after its psychological aims are already achieved: Terror's real horror is that it reigns over a completely subdued population" (Arendt 343). "Where the rule of terror is brought to perfection, as in the Nazi concentration camps, propaganda disappears entirely. Propaganda, in other words, is one, and possibly the

most important, instrument of totalitarianism for dealing with the non-totalitarian world; terror, on the contrary, is the essence of its form of government" (Arendt 344). The Nazi use of terror in the working-class districts and the continuous pressure to conform combined to generate a ubiquitous sense of persecution and insecurity (Peukert 105).

Living in the Nazi State

Life in the Nazi culture meant living the concepts of conformity, opposition to conformity, and racism every day. As a result, a distinct line was drawn between insiders and outsiders and this distinction affected everyone. The common people in the Nazi state were divided into two groups, the white collar workers and the blue collar workers. The white collar workers were more of the managers and business leaders running the factories and companies across Germany. They had lost the most over the past years of economic depression and wanted the most change and success within the new structure: "White collar workers were attracted less by the craft work and 'blood and soil' romanticism then by the modern aspects of the National Socialist ideology and propaganda" (Peukert 94).

In this same way, people are attracted to the Internet due to its "flattening effect" on the world. People can now communicate with people across the world via text, audio, or video at the speed of light.

During the Nazi reign, blue-collar workers were less drawn to this ideal of success and productivity. The blue-collar workers' attitude of non-compliance during the Third Reich, was summed up by Detlev Peukert in his book, *Inside Nazi Germany*. The lack of enthusiasm for the character and politics of the regime and the lack of zeal in the workplace went along with a wary retreat into privacy and into the atmosphere of solidarity in small, intimate groups within the

working-class social environment (Peukert 110). This allowed the populations that actively participated to be the ones who were seen and heard and quieted opposition. This is similar to online usage where people who are most active are the ones heard and respected. The most frequently updated blog or Facebook page comes to the forefront more often as opposed to the solitary individual quietly writing to himself.

This brings up the idea of how outsiders were viewed in the Nazi structure and in the IT network structure. Towards aliens, or immigrants from outside of the German borders, the most common attitude of the Nazi people was indifference tempered by occasional sympathy (Peukert 142). This is similar to how we view aliens online now because we are often indifferent as to which country you are from. Everyone's ideas are equal and have the possibility for equal say if enough people are listening; however people generally only subscribe to forums and blogs that fit into what they want to read about and listen to.

The only way for the Nazis to make up for lack of substance in the Volksgemeinschaft idea, or the people's community, was to produce passive loyalty (Peukert 188), which they did through this idea of complicity. In order to succeed and do well, Germans had to not only do well, but also participate, at growing levels, in the process of inclusion and exclusion.

The belief that social problems could be finally and scientifically solved by a joint application of educational and social reforms and measures of racial hygiene and improvement of the hereditary stock was especially widely canvassed in the popular scientific literature and was by no means restricted to extreme right-wing circles (Peukert 222).

Many Germans who supported the Nazi Regime, or at least accepted it, believed the "Führer" when he promised the he would deliver them from the "abnormal" conditions that had been brought about by the upheavals of modernization and the hardships of the depression.

Germans were looking for a return to normality, to regular work, to secure planning of their lives, and certainty of their own place in the social scheme. In face of this basic, long-lost sense of private well-being, various other warning signs were thrust to one side, virtually excluded from everyday awareness: employment was serving the cause of war-readiness and terror against "community aliens" was continuing, and becoming more and more radicalized, not scaled down. People didn't talk about these things. But they dreamed about them at night. Their dreams betrayed the oppressive presence of anxieties which were all too willingly denied in the light of day (Peukert 236).

The ranks of the Nazi movement were swollen with a large number of groups and individuals from all areas of society from the lowest class to the white-collar class, all whom had lives that were shattered from the economic and social dislocations of the Great Depression (Peukert 36). Indeed, "In the end what the Nazis achieved was not a new case of Germany but the validation of new social roles. Those social roles created expectations and assumptions" (Evans 98). Nazism was, in its most simplest form, a set of possibilities for the participation in the state's function, or being complicit in the state or becoming part of that state as a whole (similar to the world of a Borg in Star Trek).

People became part of troublesome and ever destructive social activities even if they themselves have no conscious desire to participate in destructive activity. Their own narrow sphere of work did not contain the broad picture so they did not see the broad picture.

IT Networks

Social engineering in information technology networks is an investigation of phenomenon whereby people are manipulated without their consent into assisting unwittingly in

security breaches in the networked information technology world. Similarly, in German Nazi totalitarianism, people were manipulated without their consent to participate in a system of government, a system of the operation and management of society that is destructive.

Several key points of similarity exist between the lifestyle of an individual within the Nazi regime—along the Nazi form of manipulation—and information technology networks. Employees of IT networks often do not understand how the Internet or the network works; they just know how to do their assigned job. For example, a secretary at her desk enters data into a database, such as names, addresses, and telephone numbers for a donation. This data is then used by people across the world to generate letters to individuals. The secretary doesn't know how this works and might not even know what this data is for. Another example would be basic typing. People can easily pick up typing even when there is no familiar alphabetical order to the keyboard layout, remember the skill, and type without thinking. This idea of focusing on the banal bits of data was mentioned above when discussing the "banality of evil" and it is related to the Nazi manipulation. Information, false or real, travels much faster now. Information posted on the Internet can be viewed by anyone across the world.

In reality no code, computer, or program can be ever be completely trusted. Ken Thompson wrote an interesting article called "Reflections on Trusting Trust." In this short paper, Thompson talked about how you can't actually prove anything with a computer, program, or code because everything from the compilers to the code on the chip itself can be tampered with (761-763). So there is an explosive situation brewing with cyber attack. On the one hand, the press, television, and movies make heroes of vandals by calling them whiz kids. On the other hand, the acts performed by these "whiz kids" will soon be punishable by years in prison. Ira Winkler stated, "I have watched kids testifying before Congress. It is clear that they are

completely unaware of the seriousness of their acts. There is obviously a cultural gap. The act of breaking into a computer system has to have the same social stigma as breaking into a neighbor's house. It should not matter that the neighbor's door is unlocked. The press must learn that misguided use of a computer is no more amazing than drunk driving of an automobile" (Winkler 33).

Conclusion

This section touched on the problem of the complicity in a bureaucratic system represented by Nazism. The Nazi system manipulated individuals who became complicit in its destructive activity. An easy parallel can be drawn with how individuals work in and on networked IT systems share aspects of these problems. They focus on narrow aspects of the work and do not see the big picture, they are not even interested, or they are vigorously disinterested in asking why the whole system works at all. Therefore, if the system comes under the control or can be manipulated by those who seek the destructive ends, the work of the bureaucratic individuals can become part of the process of the perpetration of the attacks.

So in the end, the fact that people themselves exist at large scale in non-transparent IT networks cause individuals to be put in the same position as the Nazi's placed the German people. The Nazi system for the generation of complicity parallels as an analogue of the kind of computer security issues prevalent today in which unwitting participants are co-opted into participation in destructive attacks on computer systems and networks.

CHAPTER 5. EXPERIMENTAL MEASUREMENTS

Method

To determine how large a problem social engineering is in a wide variety of companies and organizations, a survey was developed for the Department of Homeland Security (DHS) to use during its perimeter tests. DHS sets an annual goal to survey important facilities across the United States and recommend simple adjustments to improve facilities' security. This process is defined as a physical perimeter test.

In the past, security has been focused on the physical security mechanisms at each location - sometimes defined as operational security. These physical measures included things like locks on doors, key management, video cameras, and barriers. However, data security has recently become a bigger threat and a larger security requirement due to laws such as The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Sarbanes-Oxley Act of 2002 (SOX). As this need grew, a mechanism was needed to help provide a digital security rating for each facility as opposed to the physical security rating already in use. The biggest problem with developing a new security rating is that the people doing the surveying or responding to the surveys have varying knowledge about security definitions and may not know what something like a firewall is.

As such, I developed a survey of simple yes or no questions that a tester could easily answer by looking around or asking a company or organization. These yes or no questions allow for a digital security rating to be developed (as compared with the physical security rating already developed and implemented). The survey was developed to be a simple, best-practice survey of a company's general security. This rating system defined points and security practices using a scale ranging from 1 (Needs Improvement) to 5 (Perfect) in each of the following three

areas: confidentiality, integrity, and availability.

This digital security rating developed was modeled after the CIA model of security —not defined as the Central Intelligence Agency—which also breaks security down into three categories of confidentiality, integrity, and availability (CIA). Confidentiality is defined as the idea that sensitive information must be available only to a set of predefined individuals. Unauthorized transmission and usage of information should be restricted. For example, confidentiality of information ensures that a customer's personal or financial information is not obtained by an unauthorized individual.

Integrity means that information should not be altered in ways that render it incomplete or incorrect. Unauthorized users should be restricted from the ability to modify or destroy sensitive information.

Availability states that information should be accessible to authorized users any time that it is needed. Availability is also a warranty that information can be obtained with an agreed-upon frequency and timeliness, and this is often measured in terms of percentages and agreed to formally in Service Level Agreements (SLAs) used by network service providers and their enterprise clients.

To view a sample of the survey, please see appendix A.

In addition to this security rating, a scan of social engineering exploits was performed on each of the surveyed sites. All this information, along with general demographics of each surveyed site, was given to the researcher to analyze. General demographics included the companies' locations (Midwestern, eastern, western, or global), size (small or large), and category of company (manufacturing, academic, financial, media, medical, or government). Each of these demographic characteristics was defined subjectively by the tester except for size.

A small company is defined as less than 100 employees and a large company as 100 employees or more.

Results

Data was collected across 64 sites across the Midwest. Of those, 12 were manufacturing, 10 were financial, six were media, and 36 were medical. Detailed results are available in appendix B.

Table 1. Distribution of companies

	Count	Percentage
Manufacturing	12	18.75%
Small	8	12.50%
Large	4	6.25%
Financial	10	15.63%
Small	4	6.25%
Large	6	9.38%
Media	6	9.38%
Small	4	6.25%
Large	2	3.13%
Medical	36	56.25%

	Count	Percentage
Small	24	37.50%
Large	12	18.75%

The first set of results divides the companies up to see how each scored on the three security measurements: confidentiality, integrity, and availability.

Confidentiality rating of companies

As part of the confidentiality section of the survey the agents were looking at the following points (to see a complete list see appendix A):

1 - All sensitive data is encrypted.

2 - All access to data on a “need to know” basis.

3 - A risk assessment performed regularly by a third party with zero knowledge.

4 - Passwords are enforced and changed regularly.

5 - A Data Leak Protection product is in place to prevent data from leaking outside the network on unfirewalled ports.

Table 2. Confidentiality Rating of Companies

	Count	Min	Max	Average
Manufacturing	12	1	4	2.333

	Count	Min	Max	Average
Small	8	1	4	2
Large	4	2	4	3
Financial	10	3	5	4
Small	4	3	4	3.75
Large	6	3	5	4.1666
Media	6	2	4	3.1666
Small	4	2	3	2.75
Large	2	4	4	4
Medical	36	1	5	2.555
Small	24	1	4	2
Large	12	2	5	3.666

As we see in table 2, financial companies generally have the best scores when it comes to confidentiality. A surprising low score is in the medical arena where most people assume confidentiality of data. This surprises me because HIPPA regulations have been in effect for almost five years longer than SOX or PCI regulations.

Integrity rating of companies

As part of the integrity section of the survey the agents were looking at the following points (to see a complete list view appendix A):

1 - Logs are kept, maintained, and reviewed regularly.

2 - Intrusion detection software is in place and updated regularly.

3 - Backups are made and verified regularly and drills are performed to ensure the process of restore is well known.

Table 3. Integrity Rating of Companies

	Count	Min	Max	Average
Manufacturing	12	1	3	2.08
Small	8	1	2	1.666
Large	4	2	3	2.5
Financial	10	3	5	3.9
Small	4	3	4	3.75
Large	6	3	5	4
Media	6	2	4	3
Small	4	2	3	2.75
Large	2	3	4	3.5
Medical	36	1	5	2.97
Small	24	1	4	2.416
Large	12	3	5	4.08

As we see in table 3, large medical companies have the highest integrity, while small medical companies have one of the lower scores. The lowest score goes to the manufacturing companies, who seem place very little emphasis on security protocols.

Availability rating of companies

As part of the availability section of the survey the agents were looking at the following points (to see a complete list view appendix A):

1 - Backup servers are in place at an offsite location in case of failure.

2 - Backups to the information technology staff exist and no reliability is placed solely on any individual.

3 - A disaster recovery plan exists and is regularly updated and tested.

4 - A single employee cannot do significant damage to the computer infrastructure.

5 - Redundant systems exist for all single points of failure in the infrastructure.

Table 4. Availability Rating of Companies

	Count	**Min**	**Max**	**Average**
Manufacturing	12	1	4	2
Small	8	1	4	1.87
Large	4	1	4	2.25
Financial	10	3	5	3.5

	Count	Min	Max	Average
Small	4	3	4	3.5
Large	6	3	5	3.5
Media	6	3	5	4.33
Small	4	3	5	4
Large	2	5	5	5
Medical	36	1	5	2.33
Small	24	1	3	1.70
Large	12	1	5	3.583

As we see in table 4, media companies dominate this category, which makes sense given that availability relates directly to the bottom line of any media company. If the TV isn't receiving a signal, then the media company isn't making any money. The lowest score is manufacturing, a business area that doesn't place much emphasis on availability because information technology is not a core service provided.

Small vs. large comparison

Table 5. Average CIA ratings compared to size

Size of Company	C	I	A	Avg
Small	2.25	2.475	2.15	2.291

Size of Company	C	I	A	Avg
Large	3.708	3.75	3.45	3.64

As seen in table 5, large companies do better in all areas. I assume this is because the size of the company usually directly relates to the size of the IT budget. Large companies also generally have teams of information technology staff vs, a small company's one or two IT employees.

CIA average across company types

Table 6. Average CIA ratings compared to company type

	C	I	A	AVG
Manufacturing	2.333	2.08	2	2.14
Financial	4	3.9	3.5	3.8
Media	3.16	3	4.33	3.5
Medical	2.55	2.97	2.33	2.62

As seen in table 6, the highest score across company lines, and arguably the most secure, would be the financial company followed very closely by a media company. I argue that this is due to the modernity of the information technology infrastructure at both of these types facilities.

The medical industry is working on becoming digitalized, but right now, especially in small hospitals and medical companies, it is still a basic pen and paper method.

ITSE vulnerabilities

As I mentioned above, in addition to this security rating (ranging from 1-least secure to 5-most secure) a social engineering scan was performed of the area. To perform this scan, a DHS agent was trained to identify social engineering vulnerabilities. This training was neither complex nor difficult as the agents already search for perimeter vulnerabilities. Below I list some of the common vulnerabilities found. There was not any company tested that did not have an ITSE vulnerability.

I could provide this data linking ITSE vulnerabilities to the specific security rating of the company: however, this might allow a skilled person to possibly identify the company and or individual whose fault this is. Since I am not in the business of costing people their jobs, I hope this will provide an eye opener without providing too many specifics.

There are two prominent ITSE vulnerabilities repeated time and time again across companies in the Midwest. First is the wiring closet and second are keys. Both of these vulnerabilities were seen across all sizes of companies and all types of companies examined here.

Companies spend a considerable amount of time securing a server room only to leave the wiring closet untouched and unguarded. Generally this is because the wiring closet also contains cleaning supplies, copy machines, fire alarms, or other office maintenance items. Leaving this door unlocked and allowing people access to your network means that anyone can plug in a device and see what data is being passed around the network. And since data in motion is rarely encrypted, (only one of the places examined here required encrypted communication between all

computers) an attacker has access to anything on your network. Of course, this assumes that the attacker can gain access to the storage closet somehow.

How many people in companies have a key to the server room? Is the "need to know" principle followed or do others have access? For example, does someone like the CEO or CFO have access and does he or she ever plan to be in the server room? Janitors? Department heads, housekeeping, etc? Remember, each of these people takes their keys home, puts them on a desk or on top of a fridge where they can easily be stolen. This even creates a danger for family that most people do not realize.

There are a few other ITSE vulnerabilities I would also like to mention. These all occurred on more than one site, and I will mention any commonality I noticed.

A couple of the companies went through the effort of having a server room with a very secure door (i.e. locked with a couple different mechanisms). Once access was granted to the server room, another door out of the room was clearly visible. This back door leads to a parking lot and is secured by a normal lock that could be easily forced open. Where a lot of thought and effort was put into door number one, door number two had little to no effort or thought put into it. An attacker is like an electron, they will generally take the path of least resistance.

A couple of companies in the smaller size category were not fortunate enough to have server rooms. As such, most of the companies' servers were sitting in a manager's office. Unfortunately, both managers have an open-door policy, meaning their door is always open, even when they are elsewhere.

One of the most common mistakes made by companies that have server rooms is that they label them. A few companies even had signs pointing the direction towards the server

room. I would hope the information technology staff would be able to find the server room without a sign, and I see no reason to label the server room.

Another interesting vulnerability found, which happens a lot in the medical companies but is also present randomly in others, stems from tape backups (a HIPPA requirement). Companies generally are fairly proud of themselves for running daily backups and feel safe about this. But, the two biggest conceptual problems they forget about are the fact that these tapes should be protected as rigorously as the original data and stored in a different location. It was surprising to see how many companies performed tape backups on a daily basis and just left the tape on top of the tape drive. If the server room lights on fire, so do the tapes. The tapes should be taken elsewhere, but most employees classify elsewhere as home. As mentioned above with the keys, it is going to be much easier to break into a home or vehicle and steal the tape than a server room or network. The data needs to be protected at the same level as the original.

Most manufacturing sites have very small information technology teams, usually consisting of only one or two employees. Generally, this means that if one takes a vacation, no one really knows what is going on and even when they are not on vacation, third party vendors are often hired to help out. It isn't hard for me to pretend I am a copy repair man to gain access to your network.

CHAPTER 6. CONSEQUENCES AND COROLLARIES

Doing research on something like ITSE provides both hardships and benefits, which I would like to highlight in this section. In addition, I will explain some of the contributions of this body of work, areas I think could be improved, and extensions for future work.

Hardships

One of the inherent problems with doing research on ITSE is the same thing that makes it a threat to security: people. Any time people are involved in research a number of complications arise. For example, I had to approve all my research through a local Institutional Review Board (IRB) to make sure I am not causing harm to the individuals participating in the research. And since the birth of the IRB regulations can be traced back to the Nazi trials, there are quite a few similarities which you could see in the chapter on IT networks and Nazism: unwitting participation.

As it is clearly seen, social engineering is not torture but simple persuasion. The problem comes with the fact that the traditional IRB committee is looking for research participants' informed consent. However, once informed consent is given, then social engineering deception becomes impossible as they are now informed. The logic gets inherently complex and this was one of the biggest challenges in my research.

The other challenge with social engineering is terminology. As stated previously, the term "social engineering" can mean anything from the intended meaning—a social attack against a computer system—to the government social engineering its people to take action. This is why I created the term ITSE defined as Information Technology Social Engineering. As a result, once you understand what social engineering is being discussed, there is much material out there

defining it in very different ways. I explored this problem above in the Chapter 2 and provided my own definition.

Another challenge I have run into is the fact that there are a considerable amount of news stories about social engineering on the Web. Currently, about five new stories are posted each day containing the words "social engineering." All these stories and data would be very interesting things to analyze; however, the biggest problem is that very few of them have any relevance to the research. This makes it very hard to find any creditable research because there is so much irrelevant material to sort through. In the journal world, social engineering is too new of a venture for much data to be present. The few articles I could find, I have cited in this paper.

Benefits

The last hardship, about the abundance of stories, is also a positive aspect of the research. Social engineering is clearly in the forefront of the media's and researchers' attention. There is clearly interest and willingness for more information in this area of expertise.

ITSE is a relatively new idea and, like most things in security, is very cutting edge. This means that there is a considerable amount of "new" research that needs to be done before ITSE can be fully understood. For more on some of the possible new areas, please view the future work section below.

Purpose of Work

This research effort may seem to some scattered and random, and I would like to address that here. My current research project is meant to be an exploratory study of social engineering

as it relates to information technology networks. This is meant to raise awareness, create questions, and provide directions for people to pursue and continue the work.

Probably the most significant effect of this work is the fact that it raises the right kind of awareness. Instead of scaring people, this research provides a framework to help people see some of the problems and understand some of the depth associated with the problems. The raised awareness is not on the client side but on the research side: the awareness that more work needs to be done and that it needs to be done in an academic, data-driven way.

I expect this work to raise a lot of questions, questions that I hope will turn into works of research. For example, I have clearly shown there is a link between Nazi manipulation and IT networks, but I wonder how many jobs in information technology have that "zoning out" effect I mentioned. It is clear to me that something like database entry does, but I wonder about staff dealing with administration. It would be interesting to think about how much thought goes into the commands system administrators type on the console while administering servers or machines. I know I have mistyped a command a few times to the detriment of what I was doing.

Future Work

I envision several ways this research can be improved and expanded upon. Let us start with the data collection piece and work towards the theories. Then I will discuss some of the left-field directions that I think would make the research much more interesting.

Clearly, the data-set could use some more entries and data points. In today's world, there is no such thing as too much data, and this study is no different. In addition to that, collecting more data items would be useful. For example, I think it would be useful to collect a time

variable by having the agent record either subjectively or objectively how long it took them to find the first social engineering vulnerability.

As was my original plan, I think it would be interesting to take this data up higher to a global level and lower to a more local level. Would it be easier to social engineer someone in the United States or Europe? Or Iowa or New York? It would be interesting to compare this to general assumptions about the areas such as the "niceness" of the people in the U,S. Midwest versus the "rudeness" of the east coast.

Also, due to the agents I was dealing with, the only kinds of companies I could obtain data for were in medical, manufacturing, financial, and media fields. It would be nice to diversify this list and possibly go outside the government arm. For example, I would love to add an academic category or a government category and see how they both compare.

At some point I envision being able to model this type of behavior using a computer test bed similar to ISEAGE - Internet Scale Event and Attack Generation Environment. I know there are new fairly new models in the research world modeling agent-based or agent-centric interactions. I think these could provide some very useful insights for my research once they mature.

I plan to continue the research and work I have started here. The Department of Homeland Security will continue to provide me with data for as long as I require. In addition to that, the more I wait, the more agents that will be able to assist by creating research that is hopefully much more diverse in both opinions and areas.

CHAPTER 7: CONCLUSION AND CONTRIBUTION

Intruders are always looking out for new ways to gain access to resources such as computer systems or personal information, which they can use maliciously for personal gain. Sometime attackers get their chance due to weaknesses found in people. These could be because behaviors due to trust or ignorance but could also be through simpler persuasion or manipulation. It is generally much easier to trick a person then it is to trick a complex computer.

Social engineering across information technology networks is a fairly new idea. With all new ideas come new questions. The questions raised in this dissertation only scratch the surface of what is out there and contributes to some of the major holes identified in Chapter 3. This dissertation contributes to four major aspects of social engineering: The history, the anatomy of an ITSE attack, the definition of ITSE, and examples of ITSE.

Chapter 2: Definitions explains the hardships and complications due to the term of social engineering. This chapter compares a variety of common sources to define a new term called Information Technology Social Engineering, or ITSE. This definition helps explain the term social engineering as it is used in relation to security and information technology networks. The term includes statements to make it both inclusive and exclusive.

Chapter 4: Conceptual Models includes two different contributions. The first half of the chapter discusses a variety of psychology principles and how they apply to social engineering. The second half of the chapter discusses one of the many origins of social engineering, specifically the Nazi manipulation, of its people and how this concept ties into information technology networks.

Chapter 5: Experimental Measurements provides concrete examples from my own experience and a research study I performed detailing a few examples of social engineering across a variety of companies along with a review of the companies' security protocols.

After reading this dissertation, researchers will have new thoughts and directions to pursue in the complex world of information technology social engineering.

This paper has a very subjective emphasis. All of the data collected on ITSE vulnerabilities was collected through subjective means, the attacks theorized within the psychology section are all subjective, and the historical comparison to the German Nazis has subjective overtones. This subjective approach makes sense because social engineering, and the attacks associated with it, is by its very nature, subjective.

However, the two objective points presented in this paper are as follows: 1) The blame for every security breech can be placed on a person somewhere, and 2) Social engineering on information technology networks is a problem for all organizations no matter the size or type.

Social engineering is an attack against the vulnerability people present within the security ideal. As long as people continue to be involved with computers, people will be a weakness that must be considered and factored into all security decisions. My dream is that one day, a patch will be developed to prevent people from being such a large vulnerability.

APPENDIX A. SURVEY INSTRUMENT USED

Confidentiality

Sensitive information must be available only to a set of predefined individuals. Unauthorized transmission and usage of information should be restricted. For example, confidentiality of information ensures that a customer's personal or financial information is not obtained by an unauthorized individual.

1. Is sensitive information encrypted?
   a. If Yes, is this information encrypted while "at rest" (ie stored on Hard Drives, Tapes, etc.)?
   b. Is this information encrypted while "in motion" (ie being communicated across the network)?
2. Is there a verifiable account of all sensitive information that has been stored on portable media (laptops, PDAs, thumb drives, etc)?
   a. Are backups of sensitive data (tapes, disks, servers, co-located facilities, etc) protected to the same extent as the original data?
3. Is there a policy in place enforcing the use of strong passwords?
   a. Does this policy make users change passwords regularly.
4. Is a security awareness program in place alerting employees of possible dangers including phishing attacks and new viruses?
5. Are Servers and data kept in an environment where only users who need access have access?
6. Are all individuals who can access sensitive data both remotely and locally accounted for and trusted?
   a. How many offsite locations or people can access the data?

1 - Needs Improvement	Sensitive Data is vulnerable to unauthorized access. Employees are unaware or don't communicate concerns about cyber threats.
2 - Weak	Sensitive Data is kept in a controlled environment (e.g., a locked room) but it not encrypted. Some sort of employee education program is in place to inform them of problems and threats. Backup data is kept in the same room as the actual sensitive data.
3 - Average	Sensitive information is encrypted and stored in a controlled area (e.g., a locked room). A two way communication mechanism is set up and used regularly to inform employees of threats and become aware of employee concerns. Passwords are regularly checked for policy compliance.

4 - Good	Sensitive information is encrypted and stored so only people who need access have access to the data. A risk assessment is performed annually to identify and fix vulnerabilities. Employees are informed of threats as soon as they become available including phishing attacks and viruses. Strong passwords are enforced.
5 - Perfect	Sensitive information is encrypted and stored so only people who need access have access to the data. A risk assessment is performed at least annually by an independency party with zero knowledge of your network to identify and fix vulnerabilities. Employees are informed of threats as soon as they become apparent, including phishing attacks and viruses. Strong passwords are enforced and changed regularly. A Data Leak Protection Solution is implemented preventing sensitive data from leaving the network.

Integrity

Information should not be altered in ways that render it incomplete or incorrect. Unauthorized users should be restricted from the ability to modify or destroy sensitive information.

1. Are measures taken to detect and isolate threats to your network (e.g., intrusion detection/prevention system, anti-virus, anti-spyware, surveillance cameras, employee training)?
    a. If, Yes - Are these measures routinely reviewed and/or updated?
2. Are regular, verified backups made of sensitive data?
3. Does each user have a separate account secured with a policy-compliant password?
    a. If Yes – Are users required to change the password at a regular interval?
4. Is there a verifiable account of all access to sensitive information?
    a. Is this log periodically reviewed for unauthorized accesses?
5. Is there a system in place to detect unauthorized changes to files, computer systems, and/or network hardware?
6. Is all outside access logged, monitored and controlled?
    a. Are these occasionally reviewed for unauthorized access?

1 - Needs Improvement	No anti-spyware, anti-virus or Firewall is installed or used. All users share one log in. Nothing is logged. No backups are done.

2 - Weak	Basic logs are kept but not regularly reviewed. Users have a variety of shared accounts to log into (e.g. cashiers have an account, managers have an account). Basic anti-virus Software, anti-spyware software and firewalls are installed but may not be customized for your environment. Periodic backups are made.
3 - Average	Users each have their own account with their own password to each system. Logs are kept and reviewed regularly. Backups are made regularly but not verified.
4 - Good	Logs are kept of all unauthorized changes to data and equipment, and are reviewed regularly. Logs of outside access are kept, reviewed regularly, and problems are investigated. Intrusion Detection Software is installed and used. Backups are made and verified regularly.
5 - Perfect	Logs are kept of all unauthorized changes to data and equipment, and are reviewed regularly. Logs of outside access are kept, reviewed regularly, and problems are investigated and reported. Intrusion Detection Software is installed and used to stop malicious or unauthorized access. Backups are made and verified regularly, and drills are performed to ensure the ability of all employees to restore them.

Availability

Information should be accessible to authorized users any time that it is needed. Availability is a warranty that information can be obtained with an agreed-upon frequency and timeliness. This is often measured in terms of percentages and agreed to formally in Service Level Agreements (SLAs) used by network service providers and their enterprise clients.

1. Have efforts been made to identify and mitigate any single points of failure that may prevent access to sensitive data?
2. Is there an off-site backup facility?
3. Is a tested disaster recovery plan in place?
4. Do multiple employees know how to support your computer infrastructure?
5. Could any single disgruntled employee do significant damage to your computer infrastructure?
    a. Is this personal identified?
    b. Are measure in place to prevent data loss if this happens?

1 - Needs Improvement	Data is not always available when it needs to be. Only one employee knows how to support your infrastructure. No disaster recovery plan exists. No single points of failure have been accounted for.

2 - Weak	Data is available when it needs to be. IT employees specialize and do not overlap in specialties. A simple disaster recovery plan exists but it is not tested or updated regularly. A single employee could do significant damage to your computer infrastructure. There are a large number of single points of failure in the network.
3 - Average	Data is available when it needs to be, even in the event of equipment failures (with backup servers for main systems). Employees are well trained to handle problems regardless of staffing. A simple disaster recovery plan exists and is tested and updated regularly. A single employee could not easily do significant damage to your computer infrastructure. There are a considerable number of single points of failure in the network.
4 - Good	Data is available when it needs to be, even in the event of equipment failures (with backup servers for all systems). Employees are well trained to handle problems even when many are gone. A disaster recovery plan exists and is tested and updated regularly. A single employee cannot do significant damage to your computer infrastructure. An offsite-backup facility exists. Redundant systems exist for most single points of failure in the infrastructure.
5 - Perfect	Data is available when it needs to be with backup servers for all systems both at the location and in an offsite back-up facility. Any single IT employee can support the infrastructure of the network or a backup for each person exists. A disaster recovery plan exists and is tested and updated regularly. A single employee cannot do significant damage to your computer infrastructure. Redundant systems exist for all single points of failure in the infrastructure.

APPENDIX B. SURVEY RESULTS

Location	Size	Type	Confidential	Integrity	Availability	Avg
Midwest	1	Financial	3	3	3	3.00
Midwest	1	Financial	4	4	3	3.67
Midwest	1	Financial	4	4	4	4.00
Midwest	1	Financial	4	4	4	4.00
Midwest	2	Financial	4	4	4	4.00
Midwest	2	Financial	4	4	3	3.67
Midwest	2	Financial	3	3	3	3.00
Midwest	2	Financial	5	5	3	4.33
Midwest	2	Financial	4	4	5	4.33
Midwest	2	Financial	5	4	3	4.00
Midwest	1	Hospital	1	1	1	1.00
Midwest	1	Hospital	2	3	2	2.33
Midwest	1	Hospital	2	3	1	2.00
Midwest	1	Hospital	2	2	2	2.00
Midwest	1	Hospital	1	1	1	1.00
Midwest	1	Hospital	1	2	1	1.33
Midwest	1	Hospital	2	2	1	1.67
Midwest	1	Hospital	2	3	1	2.00
Midwest	1	Hospital	1	4	2	2.33
Midwest	1	Hospital	1	2	2	1.67
Midwest	1	Hospital	3	2	1	2.00
Midwest	1	Hospital	2	2	1	1.67
Midwest	1	Hospital	2	3	2	2.33
Midwest	1	Hospital	3	2	1	2.00
Midwest	1	Hospital	3	3	3	3.00
Midwest	1	Hospital	1	2	2	1.67
Midwest	1	Hospital	4	2	1	2.33
Midwest	1	Hospital	3	1	1	1.67
Midwest	1	Hospital	2	3	3	2.67
Midwest	1	Hospital	3	4	3	3.33
Midwest	1	Hospital	2	4	3	3.00
Midwest	1	Hospital	1	3	3	2.33
Midwest	1	Hospital	2	2	2	2.00
Midwest	1	Hospital	2	2	1	1.67
Midwest	2	Hospital	2	3	4	3.00
Midwest	2	Hospital	3	4	5	4.00
Midwest	2	Hospital	3	4	4	3.67
Midwest	2	Hospital	3	3	3	3.00
Midwest	2	Hospital	5	4	3	4.00
Midwest	2	Hospital	4	4	1	3.00

Location	Size	Type	Confidential	Integrity	Availability	Avg
Midwest	2	Hospital	4	4	4	4.00
Midwest	2	Hospital	4	5	5	4.67
Midwest	2	Hospital	3	4	5	4.00
Midwest	2	Hospital	3	5	5	4.33
Midwest	2	Hospital	5	5	3	4.33
Midwest	2	Hospital	5	4	1	3.33
Midwest	1	Manufacturing	2	2	2	2.00
Midwest	1	Manufacturing	3	3	4	3.33
Midwest	1	Manufacturing	1	2	2	1.67
Midwest	1	Manufacturing	2	1	1	1.33
Midwest	1	Manufacturing	1	2	2	1.67
Midwest	1	Manufacturing	1	2	2	1.67
Midwest	1	Manufacturing	2	2	1	1.67
Midwest	1	Manufacturing	4	1	1	2.00
Midwest	2	Manufacturing	3	3	4	3.33
Midwest	2	Manufacturing	2	2	2	2.00
Midwest	2	Manufacturing	4	3	2	3.00
Midwest	2	Manufacturing	3	2	1	2.00
Midwest	1	Media	3	3	4	3.33
Midwest	1	Media	2	2	5	3.00
Midwest	1	Media	3	3	4	3.33
Midwest	1	Media	3	3	3	3.00
Midwest	2	Media	4	4	5	4.33
Midwest	2	Media	4	3	5	4.00

APPENDIX C. LIST OF SOCIAL ENGINEERING PENETRATION TESTERS

According to Google, here is a list of companies across the United States that do penetration testing with a social aspect.

Arizona:

Phoenix IT Solutions, L.L.C.
P.O. Box 862
Charles Town, WV 25414
PHONE: (304) 839-1309
FAX: (800) 603-5117
E-mail us: info@phoenixitsolutions.com
http://phoenixitsolutions.com/auditing.htm

Chief Security Officers
9821 N. 95th Street, Suite 105
Scottsdale, AZ 85258
Phone: 888-237-3899
FAX: 480-275-4818
E-Mail: info@chiefsecurityofficers.com
Twitter: http://www.twitter.com/csokenrowe
http://www.chiefsecurityofficers.com/index.php?option=com_content&view=article&id=100&Itemid=110

California:

Tevora
2081 Business Center Dr., Suite 245
Irvine, CA
Tel: 949.250.3290
Fax: 949.250.9993
Email: socal@tevora.com
http://www.tevora.com/View/?pid=3b2ddf389b7b42448690d3da4f0b0b9b

eEye Digital Security
111 Theory, Suite 250
Irvine, California, 92617-3039
United States
http://www.eeye.com/html/services/pen-test/index.html

Secure Content Solutions :
12532 Carmel Way Santa Ana CA 92705
(888) 299-3718

http://www.bestnetworksecurity.com/services/penetration-testing

Redspin, Inc.
6450 Via Real, Ste. 3
Carpinteria, CA
93013
http://www.redspin.com/

Web Safe Shield
1141 Catalina Dr.
Suite 203
Livermore, CA 94550
http://www.websafeshield.com/application-penetration-testing.html?gclid=CNXk-Ov88ZoCFc0tpAodqXOlMQ

Online Security
5870 West Jefferson Blvd., Suite A
Los Angeles, CA 90016
Tel: 310.815.8855
Fax: 310.815.8808
info@OnlineSecurity.com
http://www.onlinesecurity.com/subcategory/page383_36.php

NCC Group, Inc.
1731 Technology Drive
Suite 880
San Jose, CA 95110
http://www.nccgroup.us/penetration-testing/pen-testing.aspx

Altius Information Technologies, Inc. (Directions and map)
1506 Brookhollow Drive, Suite 122
Santa Ana, California 92705
Bus: (714) 442-6670
E-mail: info@AltiusIT.com
http://www.altiusit.com/assessmentpenetration.htm

McAfee Foundstone Division Office
27201 Puerta Real, #400
Mission Viejo, CA 92691
877.91.FOUND (877.913.6863)
949.297.5600
214.291.5317 | fax
http://www.foundstone.com/us/services-netw-internal.asp

En Pointe Technologies
18701 S. Figueroa Street,

Gardena, CA 90248-4506
http://www.enpointe.com/security/default.asp?Professional_Services:Security

NGSSoftware US
NCC Group
Inc.1731 Technology Drive
Suite 880
San Jose
CA 95110
http://www.ngssoftware.com/consulting/testing/penetration-testing.php

The Digitrust Group
5757 W. Century Blvd.
Suite 700
Los Angeles, CA 90045
http://www.digitrustgroup.com/assessment.html

Microland
2880, Zanker Road,
Suite # 210,
San Jose, CA 95134
Tel : +1 408 435 9999
Fax: +1 408 435 9939
http://www.microland.com/infrastructure-management/network-vulnerability-assessment-penetration-testing.html

AsTech Consulting
601 Montgomery Street
Suite 688
San Francisco, CA 94111
http://www.astechconsulting.com/security_assessment.html

Symantec
20330 Stevens Creek Blvd.
Cupertino, CA 95014
http://www.symantec.com/business/solutions/focus.jsp?solid=telco&solfid=tc_testing

Network Security Solutions Americas LLC
712 W. Onstott Road, Suite 106, Yuba City, CA 95993
http://www.mynetsec.com/services/penetration-testing-vs-vulnerability-assessment

Wipro Technologies
http://www.wipro.com/webpages/itservices/infrastrucmgmt/penetrationtesting.htm

Emagined Security
2816 San Simeon Way

San Carlos, CA 94070
Main: 888.235.1906
Fax: 775.205.2988
Email: info@emagined.com
http://www.emagined.com/security_penetration_testing.php

InfinIT
2051 Junction Avenue
Suite 208
San Jose, CA 95131
http://www.infinitconsulting.com/consulting/network-design/network-audit.html

---
Connecticut:

Audit Serve
27 Pine Street
Suite 700
New Canaan, CT 06840
http://www.auditserve.com/consulting/consult_PEN.htm

Integralis Inc. - Connecticut
111 Founders Plaza, 13th floor
CT 06108 East Hartford
Tel: +1 860 291 0851
Fax:+1 860 291 0847
E-Mail: us.info@integralis.com
http://www.integralis.us/Page-15794/Page-16097/Page-16601/Page-16513/Page-16543.html

Hill & Associates
44 Erdmann Lane
Wilton, CT 06897
http://www.hill-assoc.com/web/Portal?xml=services/service_detail&fid=19&cid=70

District of Columbia:

Control Risks
1600 K Street, NW
Suite 450
Washington, DC 20006
Tel: + 1 202 449 3330
Fax: + 1 202 449 3325
Email: crwashington@control-risks.com
http://www.controlrisks.com/default.aspx?page=951

Florida:

The Wackenhut Corporation
4200 Wackenhut Drive
Palm Beach Gardens, FL 33410
800.275.8310
www.ci-wackenhut.com

Secnap
6421 Congress Avenue, Suite 206
Boca Raton, Florida 33487
http://www.secnap.com/products/security/penetration-testing.html

Enterprise Risk Management
Douglas Entrance
800 Douglas Road
North Tower, Suite 835
Coral Gables, FL 33134
Phone: (305) 447 - 6750
FAX: (305) 447 - 6752
Email: info@emrisk.com
http://www.emrisk.com/ITSecurity/penetration_testing.aspx

Amgentech, Inc.
20533 Biscayne Blvd, Suite 41311
Aventura, FL 33180
Phone: (305) 937-4449
Fax: (786) 513-0487
Toll-free: (866) 937-4449
Emergency Hotline: (866) 267-7395
http://www.amgentech.com/InfoSec.html

Thales e-Security Inc.
2200 North Commerce Parkway
Suite 200
Weston, Florida, 33326
Tel: +1 1 888 744 4976
or + 1 954 888 6200
sales@thalesesec.com
http://iss.thalesgroup.com/en/Services/ICT%20Security/Security%20Audit/Penetration%20Testing.aspx

---

Georgia:

SecureWorks Corporate Headquarters
PO Box 95007
Atlanta, GA 30347
Main: 404-327-6339
Toll-free: 877-905-6661
Fax: 404-728-0144
http://www.secureworks.com/services/professional/penetration_testing.html

Greyhat, LLC.
Atlanta, Georgia, USA
http://greyhat.com/pen/

ControlScan
340 Interstate North, Suite 347
Atlanta, Georgia 30339
https://www.controlscan.com/products_professional_services.php

Vigilar
900 Ashwood Parkway
Suite 290
Atlanta, GA 30338
http://www.vigilar.com/services/pentrationTesting.php#

RBTI
http://www.rbt-inc.com/services/pentest.html

Idaho:

En Garde Systems, Inc
18352 S. Crossbill Rd.
Couer d'Alene, ID 83814
http://www.engarde.com/enterprise/pentest.php

Illinois:

Trustwave
70 West Madison Street
Suite 1050
Chicago, IL 60602
P: 312-873-7500
F: 312-443-8028

https://www.trustwave.com/elements-pentration-testing.php

Louisiana:

TraceSecurity Corporate Headquarters
TraceSecurity, Inc.
5615 Corporate Blvd.
Suite 200A
Baton Rouge, LA 70808
Phone: (225) 612-2121
Fax: (225) 612-2115
http://www.tracesecurity.com/solutions/penetration_testing.php

---
Maryland:

Password Crackers, Inc
http://www.pwcrack.com/penetration.shtml

Chesapeake NetCraftsmen, LLC.
1290 Bay Dale Drive – Suite #312
Arnold, MD 21012
Telephone: 888-804-1717
E-mail: info@netcraftsmen.net
http://www.netcraftsmen.net/Security.htm

Vesaria
722 Dulaney Valley Road, Suite 192
Towson, MD 21204
443 - 501 - 4044
http://www.vesaria.com/Network-Assessment/Penetration-Testing/

Kore Logic
P.O. Box 357
Deale, MD 20751
http://www.korelogic.com/assessment_overview.html

Massachusetts:

Core Scurity Technologies
41 Farnsworth St
Boston, MA 02210 | USA
Ph: (617) 399-6980 | Fax: (617) 399-6987

http://www.coresecurity.com/content/contact-us

Rapid7
545 Boylston Street
Boston, MA 02116
Tel: 617.247.1717
Fax: 617.507.6488
http://www.rapid7.com/services/pentest.jsp

SystemExperts Corporation
11 Spiller Road
Sudbury, MA 01776
http://www.systemexperts.com/penetration-testing-exposure-profiling.html

Akibia
4 Technology Drive
Westborough, MA 01581
http://www.akibia.com/solutions/support/

NSG
100 Cummings Center, Suite 421-G
Beverly
Massachusetts
http://www.nsgroup-inc.com/services.html

Michigan:

Samsa
5560 Gratiot, Suite D
Saginaw, MI
http://www.samsa.com/products_services/penetration-testing.htm

Rehman
5800 Gratiot Rd. Suite 201
Saginaw, MI 48638
Phone: (989) 799-9580
Fax: (989) 799-0227
http://www.rehmann.com/default.cfm?t=service_industry.cfm&L2=TECHNO&L3=SECURE

MIssouri:

BKD

Hammons Tower
901 E. St. Louis Street, Suite 1800
P.O. Box 1900
Springfield, MO 65801-1900
417.831.7283
FAX 417.831.4763
http://www.bkd.com/service/riskmanagement/informationsecurity/Penetration.htm

---
New England:

RVASI
P.O. Box 541025
Omaha, NE 68154 USA
http://www.rvasi.com/services/apptest/

Solutionary
9420 Underwood Avenue, 3rd Floor
Omaha, NE 68114
Phone: 402.361.3000
Toll Free: 866.333.2133
Fax: 402.361.3100
http://www.solutionary.com/solutions_services/tas_epa.html

New Hampshire:

Adaptive Communications, LLC
325 Corporate Drive, Suite 150
Portsmouth, NH 03801
Phone: 603-433-1700
Fax: 603-334-6501
Email: info@adaptcom.com
Website: www.adaptcom.com
http://www.adaptcom.com/penetration_testing.cfm

New Jersey:

Millennium Consultants, Inc.
2 Riverview Drive,
Suite 200 Somerset,
NJ 08873, United States
Tel: (732) 562 0200

Fax: (732) 562 8500
Email: millennium@millenniumci.com
http://www.millenniumci.com/penetration-testing.htm

Pivot Point Security
957 Route 33, Suite 111
Hamilton, NJ 08690
http://www.pivotpointsecurity.com/-application/

Icons Inc.
4 Independence Way
Princeton, NJ 08540
Phone: 609.720.1600
Fax: 732.875.0780
http://www.iconsinc.com/s_consulting.html

Miles Technologies
300 West Route 38
Moorestown, NJ 08057
http://www.milestechnologies.com/PublicPages/IS-Penetration-Testing.aspx

---
New Mexico:

EC-Council
North American Operations Division
3819 Osuna NE
Albuquerque, NM 87109
http://www.eccouncil.org/egs/PenetrationTesting/PenetrationTesting.html

---
New York:

IBM Corporation
1 New Orchard Road
Armonk, New York 10504-1722
United States
914-499-1900
http://www-935.ibm.com/services/us/index.wss/offering/gts/a1029491

Gotham Digital Science LLC
26 Broadway
Ninth Floor
New York, NY 10004
Phone: +1 (212) 514 8318

Fax: +1 (646) 349 3911
Email: info@gdssecurity.com
http://www.gdssecurity.com/i/pt.php

Synesis IT
44 Wall Street, 12th Floor
New York, NY 10005
Tel: (212) 608 6112
Toll Free: 1.877.HI.SYNESIS
info@synesisit.com
http://www.synesisit.com/solutions/penetrationTesting.jsp

Marvin and Company, P.C.
Attention: IT Services
11 British American Blvd,
Latham, New York 12110
Phone: 1-(518)-785-0134
FAX: 1-(518)-785-0299
Email: security@marvincpa.com
http://www.marvinitservices.com/pen.html

WhiteHat Inc.
300 International Drive
Williamsville, New York
http://www.whitehatinc.com/gc.php?p=7

North Carolina:

ATTUS Technologies, Inc.
15800 John J. Delaney Drive, Suite 250
Charlotte NC, 28277
http://www.attustech.com/External_Penetration_Test.aspx

Ohio:

Microsolved
2330 Briggs Road
Columbus, OH 43223
http://www.microsolved.com/files/awareness_brochure.pdf

Pennsylvania:

White Badger Group
One Tek Park, Suite 200
9999 Hamilton Boulevard
Breinigsville, PA 18031
http://www.whitebadger.com/solutions_penetration.asp

AccessIT Group Inc.
2000 Valley Forge Circle
Suite 106
King of Prussia, PA 19406
Phone: 610. 783. 5200
Fax: 610. 783. 5151
http://www.accessitgroup.com/services/penetration.php

AppLabs
1515 Market Street
Suite 1110
Philadelphia
PA 19102-1905
http://www.applabs.com/html/webapplicationpenetrationtesting.html

---
Tennessee:

Sword & Shield
1431 Centerpoint Drive, Suite 150, Knoxville, TN 37932-1984
Voice: +1 865.244.3500 Fax: +1 865.244.3599
http://www.sses.net/services/penetration_testing

Texas:

NSS
20333 State Highway 249, Ste 200
Houston Texas 77070
281-378-1551
http://www.netsecuritysvcs.com/menu/penetration-test

Digital Defense, Inc.
9000 Tesoro, Suite 100
San Antonio, TX 78217
Toll Free: 888.273.1412
Local: 210.822.2645
Fax: 210.822.9216

http://www.cusecure.com/solutions/security/penTest.php

Appin Technologies
9600 Great Hills Trail Suite 150W
Austin Texas 78759
Tel: +1-512-502-3032
Email: austin@appinonline.com
http://www.appinlabs.com/ethical-hacking.php

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Phone: +1-512-615-7300
Telefax: +1-512-615-7301
eMail: info@atsec.com
http://www.atsec.com/01/it-security-services-penetration-testing.html#down

The Garland Group
2610 West FM 544
Wylie, Texas 75098
http://www.thegarlandgroup.net/services/penetration-testing/

InfoDefense
401 E. Corporate Drive
Suite 100
Lewisville, TX 75057-6426
http://gov.infodefense.com/services/pentesting_mss.html

Utah:

The Cadence Group
750 E 9000 S, Suite A
Sandy, UT 84094
http://www.thecadencegroup.com/soceng.html

Security Metrics
462 East 800 North
Orem, UT 84097
https://www.securitymetrics.com/pentest.adp

Virginia:

Prolific Solutions, LLC

Midlothian, VA 23112
http://prolific-solutions.net/services.htm

Plynt
12801 Worldgate Dr., Ste 500
Herndon, VA 20170, USA
Phone: +1-703-871-3934
Fax: +1-703-871-3936
http://www.plynt.com/penetration-testing-value/

SecureInfo
1410 Spring Hill Road
Suite 250
McLean, VA 22102
703.245.9770 phone
703.245.8442 fax
http://www.secureinfo.com/solutions/threat-management/penetration-testing.aspx

Syrinx Technologies
7109 Staples Mill Road., #281
Richmond, VA 23228-4110
http://www.syrinxtech.com/index.html

Prometheus Global, Inc.
14121 Parke Long Court, Suite 220, Chantilly,VA 20151
http://www.progllc.com/services/security-services/pentesting.html

Control Case
2010 Corporate Ridge, Suite 700
McLean, VA 22102 USA
Voice: 703.483.6383
Fax: 703.636.4888
http://www.controlcase.com/managed_compliance_penetration_test.php

---
Washington:

Coalfire
150 Nickerson Street, Suite 106
Seattle, WA 98109
Phone: 206.352.6028
Fax: 206.633.0235
http://www.coalfiresystems.com/penetration_testing.aspx

IOActive

Corporate HQ (Seattle)
701 5th Avenue, #6850
Toll Free: 866.760.0222
Fax: 206.784.4367
http://www.ioactive.com/penetrationtesting.php

REFERENCES

Allen, Michael. "The Use of 'Social Engineering' as a Means of Violating Computer Systems", GSEC Practical Assignment, SANS. Aug. 13, 2001.

Amidon, Kevin S. "'Diesmal fehlt die Biologie!' Max Horkheimer, Richard Thurnwald, and the Biological Prehistory of German *Sozialforschung*." New German Critique 104 (2008): 103-37.

Arendt, Hannah. Eichmann in Jerusalem. New York: The Viking Press, Inc. 1963.

---, The Origions of Totalitarianism. Orlando: Harcourt, Inc. 1994.

Bandler, Richard, and John Grinder.. Reframing: Neuro-Linguistic Programming and the Transformation of Meaning. Utah: Real People Press. 1981.

---, Patterns of the Hypnotic Techniques of Milton H. Erickson, M.D. Volume 1. Cupertino, Meta Publications: Cupertino, CA. 1976.

Bidgoli, Hossein. Global Perspectives on Information Security. Chicago: Wiley Publishing. 2008.

Bishop, Matt. Computer Security Art and Science. New Jersey: Pearson Education. 2003.

Bosworth, Martin. "Survey: Employees Are Biggest Threat to Data Security." Consumer Affairs. June 2006. <http://www.consumeraffairs.com/news04/2006/06/data_breach_audit.html>.

Chabrow, Eric. "The Human Factor of Corporate Spying." CIO Insight. June 2008. <http://www.cioinsight.com/c/a/Opinion/Corporate-Spy-Story/?kc=CIOMINEPNL06252008>.

Cialdini, R. B. "The Science of Persuasion." Scientific American, Jan. 2001: 76-82.

David Sinclair. The Land that Never Was: Sir Gregor MacGregor and the Most Audacious Fraud in History. Cambridge: Da Capo Press. 2004.

Deichmann, Ute. Biologists Under Hitler. Cambridge: Harvard U. P. 1996.

Egan, M. September 25, 2008. 120 Idiots Give Up Password for £5 M&S Voucher. June 10, 2009 <http://www.pcadvisor.co.uk/blogs/index.cfm?entryid=104860&blogid=4>.

Erickson, Milton. "Two-Level Communication and the Microdynamics of Trance and Suggestion." The American Journal of Clinical Hypnosis. 1976.

Evans, Richard. The Third Reich in Power. New York: Penguin 2005.

Friedman, Lawrence. American Law in the Twentieth Century. New Haven: Yale U. P. 2002.

Friedman, Thomas. The World is Flat. New York: Farrar, Straus and Giroux. 2005.

Goodchild, Joan. Octtober 29, 2008. "3 Reasons Why Employees Don't Follow Security Rules." CSO Online. June 10, 2009 <http://www.csoonline.com/article/457575/_Reasons_Why_Employees_Don_t_Follow_Security_Rules>.

Grodin, Annas. The Nazi Doctors and the Nuremberg Code. Oxford: Oxford University Press. 1992.

Halttunen, Karen. Confidence Men and Painted Women. New Haven: Yale U. P. 1986.

Hermansson, M. and R. Ravne. Fighting Social Engineering. University of Stockholm / Royal Institute of Technology. 2005.

Laribee, Lena. Development of Methodical social engineering taxonomy project. Monteray: Navy Postgraduate School. 2006.

Leman-Langlois, Stephanie. Technocrime. Cullompton: Willan Publishing. 2008.

May, Larry. Crimes Against Humanity: A Normative Account. Cambridge: Cambridge U. P. 2004.

---, Aggression and Crimes Against Peace. Cambridge: Cambridge University Press. 2008.

McClure, Stuart, Joel Scambray and George Kurtz. Hacking Exposed Fifth Edition. New York: McGraw-Hill. 2005.

McMillian, Robert. "Men Fall Harder Than Women for Internet Fraud, Study Finds." IDG News Service. April 2008 <http://www.networkworld.com/news/2008/040308-men-fall-harder-than-women.html?nlhtsec=ts_040408&nladname=040408securityal>.

Messmer, Ellen. "IT Pros, Remote Workers Fess up to Security Lapses." Network World. June 2008 <http://www.networkworld.com/news/2008/020608-it-pros-remote-workers-security.html?nlhtsec=ts_020708&nladname=020708securityal>.

Mitnick, Kevin. The Art of Deception. Indianapolis: Wiley Publishing. 2002.

Mitscherlich, Alexander, and Fred Mielke. Doctors of Infamy: The Story of the Nazi Medical Crimes. Montana: Knickerbocker Printing Group. 1949.

Murray, M. Critical Health Psychology. New York: Palgrave Macmillan. 2004.

Orgill, Gregory. "The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems." SIGITE'04: ACM. 2004.

Orgill, G. L., G. W. Romney, M. G. Bailey, and P. M. Orgill. "The Urgency for Effective User Privacy-education to Counter Social engineering Attacks on Secure Computer Systems", in October 2004 Proceedings of the 5th Conference on Information Technology Education.

Parks, Raymond. "Attacking Agent-Based Systems." IEEE. 2004.

Peukert, Detlev. Inside Nazi Germany. London: Yale University Press. 1987.

Pfleeger, Charles. Security in Computing. New York: Pearson Education. 2003.

Qin, Tiantian. "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering." IEEE. 2007.

Redmon, Kevin. Mitigation of Social Engineering Attacks in Corporate America. Greenville: East Carolina University. 2005.

RocketReady.com. January 2008. June 10, 2009 <http://www.socialengineering.com/?gclid=CO_hzKeatJQCFRYLIgodvAGLTg>.

Schmidt, Steffen, and Michael McCoy. Who is You? The Coming Epidemic of Identity Theft. Urbandale, IA: The Consortium. 2005.

Smith, Brad. "AWR-7: Neuro-Linguist Programming in Social Engineering." 2005 Computer Science Institute Annual Conference Proceedings. 2005.

Stanojevic, G. D. Neuro-Linguistic Programming: Meta Model of Language. Belgrade: Linguistic and Speech Recognition. 1990.

Thompson, Ken. "Reflections on Trusting Trust." Communications of the ACM 27.8. (1984): 761-763.

Thornburgh, Tim. "Social Engineeirng: The 'Dark Art.'" InfoSecCD Conference 2004: ACM. 2005.

Tucci, Linda. "'Millenials' Buck IT Security Policies." SearchCIO.com. March 2008 <http://searchcio.techtarget.com/news/article/0,289142,sid182_gci1307031,00.html?track=NL-981&ad=632033&asrc=EM_USC_3391599&uid=1342711>.

Twitchell, Douglas. "Social Engineering in Information Assurance Curricula." InfoSecCD Conference 2006: ACM. 2006.

Vanderpool, Harold. The Ethics of Research Involving Human Rights: Facing the 21st Century. Maryland: University Publishing Group. 1996.

Arthurs, William. "A Proactive Defense to Social Engineering." GSEC Practical Assignment, SANS, August 2, 2001.

White, Stephanie. "Social Engineering." Proceedings of the 10 th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03). 2003.

Wikipedia. June 10, 2009 <http://en.wikipedia.org/wiki/Social_engineering_(security)>.

Winkler, Ira. Corporate Espionage. Roseville: Prima Publishing. 1997.

---, Spies Among Us. Hoboken: Wiley Publishing. 2005.

---, Zen and the Art of Information Security. Maryland: Syngress Publishing, Inc.. 2007.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my gratitude to those who helped me with various aspects of conducting research and the writing of this dissertation. It has been a long haul. First and foremost, I would like to thank Dr. Doug Jacobson for his belief in me, his encouragement to peruse projects such as the Cyber Defense Competition and IASG, and his support through the years, both financially and mentally. I have learned quite a bit working on the ISEAGE research project, and I know I will miss it. I would also like to thank my committee members for their efforts and contributions to this work: Dr. Thomas Daniels, Dr. Mani Mina, Dr. Kevin Amidon, and Dr. Roger Smith. I would also like to thank Phil Pitzen and the Department of Homeland Security for providing me with the data I needed. Finally, I would like to thank my parents, Tim and Luanne Evans, for encouraging my further education while instilling a persistent attitude in my work ethic.

There are two web sites, without which I would have never been motivated enough to finish my degree. I will list them here for anyone who is thinking about a doctorate degree or are already enrolled in the degree program:

http://www.physics.mcgill.ca/~burkes/scrat/scrat.html

http://www.cs.unc.edu/~azuma/hitch4.html