DECEPTION DETECTION: STUDY OF INFORMATION MANIPULATION THROUGH ELECTRONIC IDENTITY THEFT – EMAIL FORGERY IN THE U.S MILITARY

THESIS

Roy V. Rockwell, Captain, USAF

AFIT/GIR/ENV/03-16

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GIR/ENV/03-16

DECEPTION DETECTION: STUDY OF INFORMATION MANIPULATION THROUGH ELECTRONIC IDENTITY THEFT – EMAIL FORGERY IN THE U.S MILITARY

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Roy V. Rockwell, BSBA

Captain, USAF

December 2002

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GIR/ENV/03-16

DECEPTION DETECTION: STUDY OF INFORMATION MANIPULATION THROUGH ELECTRONIC IDENTITY THEFT – EMAIL FORGERY IN THE U.S MILITARY

Roy V. Rockwell, BSBA
Captain, USAF

Approved:

//SIGNED//
David P. Biros (Chairman) Date 9 Dec 02

//SIGNED//
Summer E. Bartczak (Member) Date 9 Dec 02

//SIGNED//
L. Kent Marett (Member) Date 9 Dec 02

Acknowledgements

I want to first give glory to the Lord Jesus Christ through him all things are possible, including this thesis. I want thank my wife my two sons, and my two daughters for the love and support each of them have given to me throughout this research endeavor. I have a lot of play time to make up to them! I want to thank my parents for their support through many prayers. I also want to thank Lt Col David Biros, Lt Col Summer Bartczak, and Kent Marett, my committee, for providing me the encouragement and the instruction necessary to complete this thesis; it has truly been a learning experience and a great capstone to challenging Master's program.

Roy V. Rockwell

Table of Contents

Page

Acknowledgements iv

List of Figures vii

List of Tables viii

Abstract ix

I. Introduction 1

Background 1
Research Applicability to the United States Air Force 3
Problem Statement and Purpose of Research 5
Summary 5
Thesis Organization 6

II. Literature Review 8

The Nature of Deception 8
Types of Deception 9
Interpersonal Deception Theory 13
Information Manipulation Theory 14
Trust and Truth-bias 18
Aroused Suspicion 21
Human Trust in Computer Systems (Artifacts) 22
Information Warfare 25
Identity Theft 30
Research Hypotheses and Model 35
Summary 40

III. Methodology 41

Study Summary 41
Participants 41
Procedures 42
Questionnaire 43
Pilot Study 44
Experiment 45
Summary 54

IV. Analysis 55

Overview of Questionnaire 55

Page

Factor Analysis of Questionnaire 55
Analysis of Variance for Warning and Non-Warning Groups 62
Experiment Analysis 66
Analysis of Variance for Deceived and Not Deceived Participants 69
Summary 70

V. Findings and Recommendations 71

Research Findings and Implications 71
Limitations 75
Recommendations for Future Research 77
Summary 79

Appendix A: Human Subjects Review Board Application 81

Appendix B: Warning Email 86

Appendix C: In-Text Message Manipulation for Experiment 2 88

Bibliography 89

List of Figures

Figure Page

Figure 1: Deception Etiology 12

Figure 2: Theoretical Research Model for Research in Electronic Identity Theft 39

Figure 3: Distribution Plot for System Trust of Warning and Non-Warning Groups 64

Figure 4: Distribution Plot for Awareness of Warning and Non-Warning Groups 65

List of Tables

Table Page

Table 1: Experiment 1 - Research Design 46

Table 2: Experiment 2 - Research Design 47

Table 3: Experiment 1 - Timeline for email forgery for each sub-group (Total time interval was two weeks). 49

Table 4: Experiment 1 - Questions asked at each of the different time frames. 49

Table 5: Experiment 1 - Questions asked at each of the different time frames. 51

Table 6: Experiment 2 - Questions asked at each of the different time frames. 51

Table 7: Combined Experiment Factor Loadings of System Trust 58

Table 8: Combined Factor Loadings of Awareness 60

Table 9: Descriptive Statistics for System Trust and Awareness 61

Table 10: Experiment 2 ANOVA Results for Warning and Non-Warning Groups 63

Table 11: Experiment 1 Results 67

Table 12: Experiment 2 Results 67

Table 13: Experiment 1 Responses to Forged Email Address 68

Table 14: Experiment 1 Responses to Forged Email Address 68

Table 15: ANOVA for Deceived and Not Deceived Participants 69

Table 16: Summary of Findings 75

Abstract

Computer users have depended on email communication since its advent. This dependency has created an increased level of system trust within email systems. Individuals can verify where an email came from and who sent the email by simply looking at the senders' email address. The sender's email address can be hidden from unsuspecting individuals who do not know how to verify an email address and from individuals too hurried to pay close enough attention to the email address. This system trust relationship can be broken when senders deceive receivers into believing senders are someone they are not. This type of deception is called email forgery and is a form of identity theft. This research describes the results of a field experiment which examines the effects of warnings on system trust and individual awareness in government computer systems through the use of email forgery. The experiment consisted of forging a trusted government email account and trying to get government computer users to reply to the forged email address. The results revealed that warning individuals about possible email forgery did not increase their awareness or reduce their level of system trust in the email system nor did it increase their ability to detect email forgery. The results did determine that government computer users are extremely vulnerable to email forgery and that new security measures need to be adapted to protect these systems from this type of threat. The use of authentication by the email sender through the use of the new common access card (i.e., smart card or CAC) by the military is one possible measure introduced by this research to protect these systems from this form of vulnerability.

DECEPTION DETECTION: STUDY OF INFORMATION MANIPULATION THROUGH ELECTRONIC IDENTITY THEFT – EMAIL FORGERY IN THE U.S MILITARY

I. Introduction

Background

The number of computers and information systems has grown exponentially since their beginnings in the latter part of the 20th century. *Moore's Law* claims that "computing technology advancement doubles every 18 months" (Moore, 2002). Of particular interest in the past several years is the explosive growth of communications, taking the world from isolated mainframes and microcomputers to global interconnectedness. Long gone are the days of the single-minded use of computers as large calculators only; it could be argued their primary purpose in today's networked world is *communication*. We have seen email communication grow from less then 100 million mailboxes before 1996 to over 800 million mailboxes in 2001 (Fontana, 2001). Email communication will only continue to grow, and with that growth, new vulnerabilities and threats to email and its users will grow as well. People will not only be able to *hear* a person's voice with clarity through voice-email and instant voice over internet protocol (VOIP), but also through internet video conferencing where they will be able to *see* the individual they are speaking with, as if the person were standing in front of them. This type of communication technology brings many opportunities and services that have not been available in the past. It also brings many opportunities for deceit and manipulation of these new communication methods. Criminals of the future will find

new ways to deceive, steal, destroy, and manipulate in order to accomplish their criminal activities. We must look at these new communication tools and find new ways to defend them from such forms of illicit activity. The United States' dependence on information systems prompted former President Clinton to issue an Executive Order establishing a commission on critical information protection. This commission was charged with the responsibility of finding vulnerabilities that lie within the U.S.'s critical information systems infrastructure. The study found increasing reliance on critical information systems and decreased awareness to vulnerabilities within these systems. This study also found the number of threats and vulnerabilities to these systems to be increasing (Denning,1999). These new threats and vulnerabilities to our computers and communications systems must be made secure by those who protect these systems to prevent criminals from exploiting them.

As the U.S. and the world become more technologically advanced and information systems become more commonplace in society, the level of trust in those systems and technology will increase (Wickens, 1999). This increasing reliance or trust in automated systems has led researchers to study the many aspects of human-machine interaction (Parasuraman, 1987; Murray and Caldwell, 1999; Wickens, 1999). These studies found the more an individual works with a system and experiences successful use with that system, their level of system trust increases. System trust defined for the purposes of this research is "the level of trust a user places in a computer system to perform the task it was designed to perform." System awareness is defined then "as the level of attentiveness a user has in the computer system to identify when the computer system does not perform as it should." This research focuses on human-machine trust in

government email communication systems and attempts to determine if system trust increases with successful uses of that system. It also attempts to determine if there is a relationship between an individual's system awareness and system trust. The final and most important focus of this research is to determine if email forgery, a form of identity theft, is a vulnerability the U.S. military needs to be aware of. If government email systems are vulnerable to email forgery, then terrorists and criminals have a means to manipulate military members.

Research Applicability to the United States Air Force

Computer users have depended on email communication since its advent. This dependency has created an increased level of system trust within email systems. Individuals can verify where an email came from and who sent the email by simply looking at the sender's email address. The sender's email address can be hidden from unsuspecting individuals who do not know how to verify an email address and from individuals too hurried to pay close enough attention to the email address. This system trust relationship can be broken when the senders deceive receivers into believing senders are someone they are not. Identity theft is a rapidly growing crime within the U.S. with over 900,000 new victims each year (Frank, 1998). Computers and the Internet have given this form of crime an area in which to operate. With the increase in this type of crime and the dependency on email communication, we need to ask how do stolen identities and false orders affect the U.S. Air Force and DoD?

The Air Force and DoD rely heavily on email. Air Force commanders send orders for their troops to carry out through email. Air Force instructors use email as a

primary means of communication to issue assignments or inform students of class and course changes. Stealing an individual's identity is not difficult (Frank, 1998). Getting the receiver to trust the information the sender is sending is also not difficult. In face-to-face communication, a sender communicates a message by using a number of verbal and non-verbal cues. The receiver must interpret these cues in order to determine if the message has any truth to it. With email and any form of non-face-to-face communication, the receiver has to interpret the truth with only verbal cues. Those verbal cues are reduced even further because there is no actual voice communication. Email is primarily text-based. As such, it reduces the number of processes the receiver must interpret and allows less opportunity to detect false messages. An email sender can potentially gain the necessary communication (verbal) cues needed to defraud the receiver with only one email from an account/individual from which they have stolen an identity. If this is true and false orders are given and followed through with, what can prevent this type of deception? Can warnings about this type of deception increase a receiver's awareness and improve their ability to identify this type of deception? The Air Force Office of Scientific Research has funded deception detection research to answer the following questions: "1) How can receivers be assured of the reliability and accuracy of information and its source? 2) How can they know when to trust the information? 3) Are personnel likely to question the accuracy before relying on information to make decisions vital to our national interest?" (Research Consortium, 2001) This thesis research seeks to provide information on how these questions can be answered in the realm of email communication systems. It also seeks to add to the body of knowledge to further the research in deception detection using information systems.

Problem Statement and Purpose of Research

This thesis research looks at this new form of computer communication deception called e-mail forgery and attempts to show how easy it can be to deceive and manipulate individuals with only a small amount of information about the sender. E-mail forgery is a form of electronic identity theft in which the sender attempts to deceive the receiver into believing the sender is someone other than the person the receiver believes them to be. One of the purposes of this research is to determine if warnings about possible email forgeries are an appropriate method of raising an individual's awareness in detecting electronic types of deception through text-based communication methods. Biros, George, & Zmud (2002) found warnings increased an individual's ability to detect deception, but that it also increased his/her sensitivity to false alarms (judging true messages as deceptive). The scope of this research is to determine; 1) if warnings in deception detection improve an individual's ability to identify email forgeries, 2) ways to improve awareness in deception detection, and 3) if email forgery is a significant vulnerability the U.S. Air Force and DoD need to be concerned about.

Summary

The information age has provided an array of exciting opportunities in technology and communication. These opportunities are not without their negative impacts, such as the number of viruses spreading across the World Wide Web and email systems (Denning, 1999). The increase in frauds and crimes are in direct connection to these technological advances (Robb, 2002). The U.S. Air Force and DoD must not become complacent and allow these vulnerabilities to jeopardize our information superiority over

our foes. The U.S. must stay on the cutting edge of technology, but remember that with this technology come new vulnerabilities our enemies are more than willing and ready to exploit. Therefore, the U.S. must stay vigilant and determine what these vulnerabilities are before our adversaries have an opportunity to exploit them. The U.S. cannot allow new types of vulnerabilities to go undefended or unprotected in the future. Therefore, we must look at these new communication tools and find new ways to detect and defend our information infrastructure from all forms of illicit activity. Leaders and military organizations need to know what their computer vulnerabilities are. This research identifies a new vulnerability, email forgery, that leaders and military organizations need to be made aware of. This research will provide empirical evidence that military users are susceptible to email forgery and attempts to determine if warnings provide a way to increase users' awareness and ability to detect this form of deception. If military email is susceptible to email forgery is it possible false orders could be issued and acted upon in a battlefield environment?

Thesis Organization

The following chapters present support for a conceptual framework that will be used to observe: 1) an individual's trust and awareness in an information systems automation environment, 2) if warnings increase an individual's ability to detect deception, and 3) if email forgery is a significant vulnerability to government email systems.

Chapter II presents a literature review of the body of knowledge on deception, trust, information warfare, identity theft, and email forgery. Chapter III presents the

experimental and methodological framework for the experiment used to test the hypothesis. Chapter IV presents the statistical analysis of the data collected from the experiment. Finally, Chapter V presents the research findings and conclusions.

II. Literature Review

The Nature of Deception

Deceit has existed since the first man walked on the earth. "The man said 'the woman you put here with me she gave me some fruit from the tree, and I ate it.' Then the Lord God said to the woman, 'What is this you have done?' The woman said, 'the serpent deceived me and I ate'" (Genesis 3:12-13, Quest Study Bible, NIV, 1994). Ever since, deceit has driven men and women to manipulate others to attain their desires. Miriam-Webster's Collegiate Dictionary (Webster's) definition of deceit is "to cause to accept as true or valid what is false or invalid" (Webster's, 2002). "Mislead," a common synonym for "deceive," is defined as "to lead in a wrong direction or into a mistaken action or belief often by deliberate deceit" (Webster's, 2002). It can be presumed that the "detection" (defined as "to discover the true character of" (Webster's, 2002)) of deceit came into existence shortly after Adam and Eve's first deception, and that since then a struggle has ensued to perfect means and methods of both deception and detection.

Defining deception is difficult because people interpret deception in many different ways. For example, Buller and Burgoon (1996:205) state that deception "occurs when communicators control the information contained in their messages to convey a meaning that departs from the truth as they know it." They claim that this interpretation rules out any form of mistaken or unintended lies. Although their definition closely follows Webster's definition, the difference lies in "intent to deceive." Buller and Burgoon (1996:209) argue that deception occurs only when the sender *purposely* tries to deceive the receiver; therefore, deception can take place only on the part of the sender. The receiver is a mere victim of the sender's deception. They also argue that suspicion

occurs when a receiver holds a belief without evidence that the sender's actions are dubious. Another definition of deception is "a lie or deceit when one person intends to mislead another, doing so deliberately, without prior notification of this purpose and without having been explicitly asked to do so by the target" (Ekman, 1985:28). O'Hair and Cody (1994:182), describe deception as "the conscious attempt to create or perpetuate false impressions among other communicators." Their definition focuses more on the communication strategy rather than changing of the receiver's understanding or beliefs. Further, they view the mere *attempt* of deception, whether successful or not, as deception. Again, however, the focus is on the intent to deceive or mislead another person and appears to be most researchers' central theme when defining deceit or deception.

Types of Deception

This section will provide a sampling of the deception etiology which is intended to illustrate the complexity of both the subject and scope of *deception detection*. Ekman (1985:44) identified two types of deception: *falsification* and *concealment*. He defines falsification as "masking true information by transmitting false information," and concealment as "one person keeping the truth from another person or groups of people in an attempt to cause them to believe something that is not true." Turner, Edgley, and Olmstead (1975:75) defined five types of deception: *lies*, *exaggerations*, *half-truths*, *secrets*, and *diversionary responses*. Lies are acts that falsify the truth by providing false information to what the receiver believes to be true. Exaggerations are acts that afford more information or go beyond what the truth calls for. Half-truths occur when the

sender withholds parts of the information from the receiver in an attempt to minimize the effect of the whole truth. Secrets are a form of withholding or keeping silent about information the receiver wants or may need. Diversionary responses occur when the sender redirects the discussion to another topic area to avoid telling the truth or a lie. However, O'Hair and Cody (1994:185) claim their five categories of deception allow for greater latitude in behavioral and moralistic features than Turner et al.'s five deception types. Their categories are *lies*, *evasion*, *overstatement*, *concealment*, and *collusion*. Lies represent direct acts of fabrication intending to create a belief by the receiver that is not the truth. Evasion is defined as behavior intended to redirect communication away from certain topics. Overstatements are acts intended to exaggerate what is known to be true. Concealment is an attempt to hide true feelings or emotions from the receiver. Collusion is a form of deception where the sender and the receiver cooperate, at least initially, in allowing the deception to take place. Even though O'Hair and Cody claim their categories offer "greater latitude," from the Turner et al. (1975) types, we observe little or no difference in their respective definitions; it appears the differences are in name alone. Metts' (1989:165) research on "the form and function of deception in close relationships" found three basic lie types: *falsifications, distortions,* and *omissions*. A falsification is stating information that is not true and clearly refuting the legitimacy of the true information. Distortion is manipulation of the true information through exaggeration, minimization, and equivocation, so that the receiver would not know all the facets of the truth or would misconstrue the information provided. Omission is keeping all information from the receiver. However, this research does not intend to take issue the various deception nomenclatures and subdivided definitions found in the literature; the

intent is simply to show the numerous forms of deception which are believed to exist within the body of knowledge on deception. The complexity of the deception area of research was summed up well by McCornack who stated, "Messages involving fundamentally different types of information manipulation cannot be conceptualized as similar and treated methodologically as identical" (1992:2). The above discussion on the deception etiology allows this research to infer that deception involves messages and information intentionally communicated to produce a false conclusion. The etiology can be seen in Figure 1.

Falsification (Ekman, 1985)	Masking true information by transmitting false information
Concealment (Ekman, 1985)	One person keeping the truth from another person or groups of people in an attempt to cause them to believe something that is not true.
Lies (Turner et al., 1975)	Acts that falsify the truth by providing false information to what the receiver believes to be true.
Exaggerations (Turner et al., 1975)	Acts that afford more information or go beyond what the truth calls for.
Half-truths (Turner et al., 1975)	When the sender withholds parts of the information from the receiver in an attempt to minimize the effect of the whole truth.
Secrets (Turner et al., 1975)	A form of withholding or keeping silent about information the receiver wants or may need.
Diversionary responses (Turner et al., 1975)	When the sender redirects the discussion to another topic area to avoid telling the truth or a lie.
Evasion (O'Hair and Cody, 1994)	The behavior intended to redirect communication away from certain topics. from certain topics.
Overstatements (O'Hair and Cody, 1994)	Acts intended to exaggerate what is known to be true.
Collusion (O'Hair and Cody, 1994)	A form of deception where the sender and the receiver cooperate, at least initially, in allowing the deception to take place.
Distortion (Metts, 1989)	The manipulation of the true information through exaggeration, minimization, and equivocation, so that the receiver would not know all the facets of the truth or would misconstrue the information provided.
Omission (Metts, 1989)	Keeping all information from the receiver.

Figure 1: Deception Etiology

Interpersonal Deception Theory

Buller and Burgoon (1996:205) define interpersonal deception theory (IDT) "as a merger of interpersonal communication and deception principles designed to better account for deception in interactive contexts." To understand IDT, the terms "interpersonal" and "interactive" must be defined. Deception and suspicion are defined previously. Interpersonal communication is the exchange of communication, which takes place between two or more people. Interactive communication is the synchronous communication exchange in which immediate feedback is necessary. So IDT is a "theory of deception and reactions to actual or perceived deceptions" (Buller and Burgoon, 1996:212). IDT is a dynamic communication activity between the sender and the receiver or a face-to-face communication exchange. IDT involves verbal and non-verbal communication. It involves strategic and non-strategic behaviors. It is goal-oriented and egotistic. O'Hair and Cody (1994:195) believe that egoism is the root of why people are deceptive. They define egoism "as a self-directed motive employing deceptive strategies intended to protect, preserve, or promote the self-concept or self-esteem of the deceiver (sender)" (O'Hair and Cody, 1994:195). Egoism implies that deception is strategic. Strategic interpersonal communication is a highly conscious, planned activity. Non-strategic interpersonal communication is unintentional and often unconscious behavior. Neither the sender nor the receiver is a passive observer of the other's actions. What IDT claims is deception can be detected by looking at strategic and non-strategic behaviors. For example, senders, when lying, might be nervous or they might roll their hair with their finger. These would be non-verbal deceptive cues associated with the sender trying to provide a false statement. Although IDT is primarily associated with the receiver's

ability to identify non-verbal cues, IDT applies to this research in a non-interactive, strategic way. This research will look at a planned (strategic) attempt to deceive the receiver in a non-interactive way using an automated text-based communication method. There is no immediate feedback (non-interactive) rather it is a delayed feedback approach with the use of computer-mediated communication – email.

Associated with the cognitive demands of IDT are norms or expectations, which are held by both the sender and receiver. Truth-bias (discussed in detail later in this chapter) is present when two people engage in interpersonal communication and what is said is believed or expected to be true (McCornack and Parks, 1986). Buller and Burgoon (1996:209) claim, "Trust is the foundation on which enduring relationships are built, and trust grows with the belief that another is communicating in an honest, straightforward manner." Here is where deception becomes apparent. When participants recognize that a violation of this truth-biased expectation occurs, when the common bond of truth-bias is broken, deception begins.

Information Manipulation Theory

Since the time we were children, we have devised ways to divert from the truth to avoid trouble or confrontation. It is human nature to want to avoid trouble or confrontation whether it is intentional or unintentional. "Individuals frequently are confronted with situations in which they must reconcile the competing goals of conveying information that their conversational partners are entitled to have and minimizing the damage that conveying that information might cause" (McCornack, 1992:6). One way to merge these competing goals is to change the information presented

or withhold key information from the communication exchange. For example, when a parent or guardian asks a teenager, "Did you go to school today?" The teenager responds, "Why yes of course." The teenager did in fact go to the school. At the same time, the teenager may havewithheld the fact they did not stay. Another example of withholding information in order to deceive and avoid confrontation occurs when a spouse asks, "How do I look? I don't look fat in this do I?" The other spouse replies, "No you look great!" The spouse in reality thinks the other spouse looks very corpulent in the outfit. Many other examples of deception or manipulation exist. Information Manipulation Theory (IMT) is rooted in the situations described above. Deceptive messages mislead receivers through covertly breaching the ideologies that steer and direct conversational comprehension (Bowers, Elliot, & Desmond, 1977:237). Deceptiveness takes many forms. IMT focuses on the varying amount of information that is presented, the distortion of the information, the use of typically vague and unclear phrases, and/or varying the relevance of the information presented (McCornack, 1992:4). IMT is rooted in the conversational maxims of Grice's (1975) Cooperative Principle (CP). The CP claims that during conversations, people usually hold to unwritten conversational maxims. Truth bias ascertains that individuals enter into a trust relationship when communication takes place and that all pertinent information will be presented in a truthful manner (McCornack and Parks, 1986). Only when this trust relationship is broken does deception occur. According to Grice (1975:45), communication is made possible by these maxims where the communicators mutually agree to general principles of cooperation and rationality. Grice offers four conversational maxims, which exist within the CP. These maxims are *quantity, quality,*

relation, and *manner*. IMT builds on these maxims and claims that when these maxims are violated this can be considered a deviation from the rational and cooperative behavior (Biros, 1998).

Quantity. Refers to the amount of information required to communicate between the sender and the receiver. The amount of information presented should be no more than is required for the situation. A violation of this maxim would be to leave out information, which is necessary or add information, which is unnecessary.

Quality. Refers to the genuineness of the information presented within a message. This is a fundamental aspect of "truth bias." "To call on speakers to avoid falsehood and to have support for what they say" (Jacobs, Dawson, & Brashers, 1996:71). "Participants are expected not to present information they know to be false, nor make claims for which they lack adequate evidence" (McCornack, 1992:5). To provide false information knowingly, would be a violation of this maxim.

Relation. Refers to the relevance of information within communication contexts. A violation of this maxim would be to redirect the communication to another subject. This would be the ability to step around a subject without discussing it. An example of this is what is coined "tap-dancing." One is said to be a tap-dancing when one is trying to portray knowledge of a subject when none exists; the speaker steps around a subject. "Avoidance" is the key to the violation of this maxim.

Manner. Refers to how the information is presented or clarity. "Manner refers to how things should be said rather than to what should be said--avoid obscurity and ambiguity; be brief and orderly" (Jacobs et al., 1996:71). In one word, "clear." The previous three maxims existed because of what information is said or provided. This

maxim exists because of how information is said or provided. If information is presented in a sarcastic or jokingly manner it can shape how an individual perceives that information.

Given that individuals have certain expectations concerning information quality, quantity, relevance, and manner, it is a possibility for senders to abuse one or more of these maxims when trying to deceive receivers (McCornack, 1992:5). IMT and deception are founded in the violation of one or more of these CP maxims. "Messages that are commonly thought of as deceptive derive from covert violations of the conversational maxims" (McCornack, 1992:5). So IMT is, "Given that conversational interactants possess assumptions regarding the quantity, quality, manner, and relevance of information that should be presented, it is possible for speakers to exploit any or all of these assumptions by manipulating the information that they possess so as to mislead listeners" (McCornack, 1992:5). IMT focuses on the verbal context of communication, whereas IDT has a heavy emphasis on non-verbal communication methods. They are both critical to the research in deception and its detection. Deception takes many forms as can be seen from both of these theories and the numerous types of deception defined previously. This research will focus on information systems as the platform for communication, which have a heavy reliance on text-based communication. Therefore non-verbal communication does not have a role in this research other then to present the theory and show its importance on deception and deception detection in the communication process. IMT will play a significant role, since it is rooted in verbal and text-based communication.

Trust and Truth-bias

In order to understand deception thoroughly, one must understand the concept of *trust* and the theory of *truth-bias*. Webster's (2002) defines trust as "[an] assured reliance on the character, ability, strength, or truth of someone or something; one in which confidence is placed." If the Bible is viewed as historical reference, then trust has existed since the beginning of time, even before deception. According to the Book of Genesis, God trusted Adam and Eve to care for the Garden of Eden and to not eat from the Tree of Life. That trust was broken when the serpent deceived Eve and caused both Adam and Eve to eat the forbidden fruit (Genesis 3, Quest Study Bible, NIV, 1994). Hence, for deception to take place, trust must first be established. Trust is based on *credibility*, or how believable a person or system is, and is the fundamental basis on which long-lasting relationships are constructed (Stiff, Kim, & Ramesh, 1992:328). Aristotle, the ancient Greek philosopher, termed this concept *ethos*. Credibility refers to a collection of judgments that receivers make about the believability of a sender (Buller and Burgoon, 1996:207). Trust grows with time and the basic belief that others are communicating in an honest, straightforward manner (Buller and Burgoon, 1996:208). The truth-bias theory states it is in people's nature to trust their fellow humans unless they have information that negates that trust (McCornack and Parks, 1986; Levine and McCornack, 1992; Stiff et al., 1992; Buller and Burgoon, 1996; Burgoon, Buller, Guerrero, Afifi, & Feldman, 1996). Stated another way, truth bias is a social interaction expectation stemming from the norm of reciprocity (Gouldner, 1960:167). Researchers have concluded that our social relationships rely on the exchange of aid, help, and rewards to satisfy one another's needs (Buller and Burgoon, 1996; Greenburg, 1980;

Roloff, 1987), and that we embrace the social norm expectation that others are decent, pleasant, and worthy of positive regard (Kellerman, 1984:44). The concept of truth bias was extended by Muir to encompass not only human-to-human interaction, but also human-to-machine and human-to-system interactions (Muir, 1994:1912). She concludes further that truth bias, like trust, matures and is made significantly stronger over time. For example, in today's society of seemingly instant computer-based communication to almost anyplace in the world, individuals have a certain level of trust in the systems they use. The level of trust depends on length of experience with the system and system performance over periods of time (Moray, Hiskes, Lee, & Muir, 1995:185).

While trust may or may not be an endogenous trait (the question of which is beyond the scope of this paper), there is little doubt that the *level* of trust is learned or developed. For instance, a new computer user using electronic mail (email) may be dubious of the email process; although they would seem to exhibit some level of trust (as evidenced by simply using email to begin with), they may doubt the delivery will take place in a secure and timely manner. In fact, the doubter might even call the intended recipient to verify delivery. Veteran email-users have probably developed trust in their email system. Why? Likely, their trust level has built up over time with repeated successful experiences—they have faith in the system because it worked in the past. For example, when we turn on a light switch, we expect the light to come on. We do not think about the electrical-mechanical process when the switch is turned on; we simply know through experience that, in the past, the light came on, so we expect it to come on again each time we turn on the switch. Hence, trust level is based on performance or experience over time, and leads to development of truth bias. Levine and McCornack

(1992:144) empirically tested truth bias and determined it to be a significant social norm in deception research. The truth bias proved by McCornack and Parks (1986:388), Levine and McCornack (1992:144), and Stiff et al., (1992:327) was based on human-to-human interaction, but Muir (1994:1912) makes the point that this model holds true for human-to-machine or human-to-system trust as well. If this same email system failed to deliver the message to the sender, perhaps only once or even repeatedly, then the user's trust in the email system would decrease. At a higher level, computer system use should also decrease if the computer system becomes an unreliable system. This research does not attempt to define what a user might perceive as an "unreliable system" except that in some manner the computer system fails to meet the user's expectations. As for the human-to-machine interface, a *machine* can be just about anything from a watch to a microwave to a computer system. Muir (1994:1913) stated that human trust in machines would grow with their experience with usage of the machine over time. This concept or model is derived from McCornack and Parks' (1986:388) human-to-human trust relationships. Buller, Strzyzewski, & Comstock (1991a), Buller, Strzyzewski, & Hunsaker (1991b), and Stiff et al. (1992) present the view that as relationships develop, trust in those relationships becomes stronger; over time, people tend to move toward the simple decision heuristic that it is easier to trust than it is to perceive deceit in the communication. This same heuristic can be applied to human-to-system and human-to-machine trust (Moray et al., 1995:191). Hence, because a user's level of trust (or faith) has been established and grown through successful past uses, it is easier for the user to trust that continued successful communications will occur in the present than it is to attempt to detect deception.

Aroused Suspicion

Suspicion is one dynamic that may serve to offset this truth bias heuristic and decrease trust in the situation. Stiff et al. (1992) state that relationships of trust with well-developed truth bias, whether human-to-human or human-to-system, are not likely to become suspicious on their own. A third party (i.e., person, message, or signal) must introduce some form of deception to cause suspicion in those well-developed trust relationships. This information would increase awareness and impact these judgments of truthfulness. For example, a professor and student have a certain level of trust expectation in their relationship. The professor expects the student to do their own work. The student trusts the professor to present honest and correct information. This trust relationship is established until some third party information is introduced (i.e., cheating on a test by the student or incorrect information presented by the professor) that causes the professor or student to no longer place trust in that relationship. This trust in something or someone is what causes an individual to miss a deceptive message from a sender where a truth bias exists. Another example is email received from a trusted sender. Presumably, the user opens and reads the email with little or no suspicion of deceptive activity. The receiver trusts the sender not to deceive them or send them an email with malicious logic inserted (i.e., a virus). Now suppose a third-party warning is introduced. For example, information is received alerting all users that any email with a certain subject line introduces a damaging virus. This warning email should arouse suspicion in the receiver, causing him or her to be aware of this particular form of deceptive message, even if received from a trusted sender using a trusted email address. Hence, since suspicion is now introduced (or perhaps awareness heightened to an

unacceptable level from a previous minimally acceptable level), there is cause for the truth bias norm to be questioned. This is in direct agreement with what Stiff et al. (1992:330) found in their research. They claim the truth bias heuristic serves to increase judgments of truthfulness, unless aroused suspicion by a third party to the receiver, offsets this bias, producing greater judgments of deceptiveness.

Human Trust in Computer Systems (Artifacts)

Deception of computer- and communications-based information systems is a major security concern for the Air Force. Zmud describes information transiting these types of systems "artifact-based communication" (Zmud, 1990:97). Since 1990, artifact-based communication has grown exponentially in concert with the rapid growth of use of the Internet and the World Wide Web. In fact, we speculate that artifact-based communication (via Information Systems (IS) or Information Technology (IT)) is expanding more rapidly than any other form of communication method ever has before. Zmud appears prophetic as he claimed in 1990 the following would occur as artifact-based communications developed:

- People would become increasingly dependent upon IS.
- People's confidence in information received from IS would increase.
- Deceptive manipulation would increase via IS communication channels.
- Perpetrators of deceptive behavior would be more difficult to identify (Zmud 1990:109-111).

Zmud also presented the idea that information manipulation can occur beyond human-to-human interaction; it can exist in human-to-machine (artifact) interaction just as easily. This research will look at how a person, group, or company can be manipulated using artifact (email) based manipulation. As this technology grows, so

does the reliance we place on these systems to provide accurate information. This reliance is a trust relationship and must be nurtured over time. Since trust exists in this human-to-artifact model, new forms of electronic mediated deception are likely to take place.

Throughout history people have created machines to simplify their work. These machines not only simplified their tasks, but they also reduced the opportunity for human error in relatively mundane tasks. These automated machines increase proficiency, reliability, and speed of the tasks being completed. In short, they are supposed to make man's life simpler and easier. Is this always a good thing though? Parasuraman (1987:705) says that the goal of automation should not be to necessarily reduce workload but to optimize it. Parasuraman points out, "To much automation may lead to complacency, boredom, and poor monitoring behavior" (1984:705). In short, these claims suggest that too much trust in automation can lead to poor performance or too much reliance on the automation. An individual in this state will lack the vigilance to detect this poor performance. His/her level of awareness to deception will decrease. Parasuraman (1994:702) claims the best scenario is a combination of human-computer monitoring. This is in direct line with the focus of this research. The best tool to detect deception is through the use of the latest automated tools, computer systems, and human training. These tools combined together will give an individual the greatest opportunity to detect deception

With the use of machines to do our work, certain levels of trust are built. Muir (1984:1912-1914) claims that trust is a dynamic expectation, which follows a certain developmental progression as the relationship grows. It has a set hierarchical

development order based on *predictability*, *dependability*, and *faith*. Predictability is the consistency and desirability of its recurrent behavior over a certain period of time. Dependability is described as a process of pushing a system beyond its usual limits into unknown scenarios to see how dependable it is. Faith is the belief that a system can do what it is designed to do without knowing specifically how it does something (Muir 1994). For instance, a pilot need not know how the autopilot works down to every mundane task it performs; he just needs to know that it will fly the aircraft when engaged. Computer systems are part of everyday life for most of the modernized world. People who use them rely on them. It is reasonable to speculate that as dependence upon computers continues to grow, we can no longer imagine life without them. The trust we place in our technology leads to faith that it will function reliably, and faith leads to what some would term an unhealthy reliance or dependence on something or someone. Deception exploits this reliance. In order for people to continue trusting these systems, security measures must be raised. Detection of deception and intrusion of these systems must be a high priority in order for this trust to remain intact. Numerous researchers have studied *observed behavior* as a measure of trust in aircrew's reliance on automation (Mosier, Skitka, & Heers, 2000; Mosier, Skitka, & Burdick 2000). In their studies, participants were subjected to experiments using the aid of an auto pilot system to control an aircraft. The purpose of this research was to show that, "Air crews have a tendency to over-rely on automation to perform tasks and make decisions for them rather than using the aids as one component of thorough monitoring and decision-making processes" (Mosier, Skitka, & Heers, 2000: n. pag.). This trust dependence becomes a characteristic an enemy can exploit. A study accomplished on Air Force Officers in the grades of 2nd

Lieutenant through Captain at the Air Force Institute of Technology using the Air Battle Space Management System showed similar results (Daly, 2002). Officers trusted the automation to pick out targets and decide when to fire upon them. This over-reliance or trust in the system caused numerous friendly aircraft to be targeted and shot down. The only drawback of this study was the officers tested were not Air Battle Space managers and had no prior training in Air Battle Space management. This demonstrates when a person is put an unfamiliar situation he/she may tend to place a high level of trust in the system. Another study performed by Zuboff (1988) on experienced airline pilots examined two types of critical flight errors, automation omission and commision errors. Automation omission errors occurred when the pilot failed to take appropriate action when the autopilot system did not provide the information needed. Automation commission errors were caused when the pilot miscalculated the aircraft's position based on incorrect information presented by the autopilot system. The study by Zuboff (1988) showed that automation bias can exist in experience-trained personnel who are considered experts in their field.

Information Warfare

Information has long been considered a crucial resource to winning victories on and off the battlefield. The great military strategist Sun Tzu (6th Century B.C.) said, "Attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence." With the advancement in computer information systems and the Internet, vast amounts of information are readily available from just about anywhere in the world. The goal of

information warfare is to deny our enemy critical information and communication needed for victory and to capitalize on this same information and communication to be successful in our missions. Information warfare has many different variations of definitions. For the purpose of this research (IW) is defined as the following:

> The offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries. (Goldburg, 1996)

In the past, information gathering within a military context required the placement of personnel within an enemy's borders. This was costly from both human and monetary perspectives. Individuals often gave their lives to relay critical information about their enemies. Although this type of information gathering is still critical today, it is used less frequently. Instead, technologies such as satellite imaging, advances in transportation, and advanced communication capabilities have allowed countries to close the geographic gap that existed even ten years ago. Also, advancements in communications and the connectivity via the Internet have increased countries' dependencies upon one another. Consider, for example, a modern country's economic dependence on another in the form of trade and commerce—essentially, the two countries' economies are linked by import/export agreements, tariff structures, multinational enterprises, etc. If country A suffers economically, country B likely suffers as well (e.g., a "domino effect"). Economic dependence on other countries is becoming more common as the world conceptually "shrinks" due to ever-advancing technology. And, because of the intricacies of a globally-networked economy, the protection once afforded to economic,

social, and military infrastructures by geographic distance is becoming progressively more vulnerable *because* of the complexity of the Internet and our reliance upon information systems controlling our infrastructures (Van Cleave, 1997:22). An adversary can now easily, swiftly, and stealthily attack critical information systems using a wide variety of methods. Military commanders must understand the capabilities of their systems as well as the vulnerabilities. The key to any military victory is to never underestimate your opponent. Our military must never rely on its technology advancements to the degree that we believe superior technology is impervious from deception or attack, for to do so could be the first step to downfall. Thus, research in information systems and their vulnerabilities is critical to sustaining the sharpness of the military's sword. If we can find vulnerabilities in our information systems before our enemies do, then we can develop ways to mitigate or eliminate them—which exactly describes the mission of the Air Force Information Warfare Center (AFIWC). AFIWC is charged with developing, maintaining, and deploying Information Warfare/Command and Control Warfare (IW/C2W) capabilities in support of operations, campaign planning, acquisition, and testing. They act as a time-sensitive, single focal point for intelligence data and C2W services, providing technical expertise for computer and communications security. Further, AFIWC is the Air Force's focal point for tactical deception and operations security training, and they continuously monitor the service's information systems to assure and ensure a high posture of IS security.

The adaptable, unstructured, ever-present nature of the Internet, combined with its near indispensability as a force enhancer, has fostered an arsenal of IW weapons and strategies. One of those strategies, *hacking*, occurs when an unauthorized person or

persons attempt to gain access to information systems, whether legally or illegally, state-sponsored or rogue. Hackers attempt IS access for numerous reasons: information theft, information manipulation, or plain curiosity. Hackers desire information, a commodity that can be viewed as a form of power. In fact, that power is probably the single most influential reason why hackers hack (Denning, 1999:188). Another strategy is *direct launch*, the use of viruses and logic bombs. This strategy can wreak havoc on users because a direct launch can be deployed in a number of different forms. Presently, the most prevalent are email-based viruses since the virus can be sent to anyone merely by typing in an intended target's email address (Robb, 2002:2). In most cases, this virus (of which the recipient is probably completely unaware) requires a recipient to initiate the virus by opening an attachment of some type. Once opened, the virus may self-propagate with no action required of the (current) recipient and email itself out to everyone in the recipient's email address book and then drop its payload on the initial recipient's system (e.g., delete files, etc.). Another IW strategy is *forward basing* (Denning, 1999:188). This type of virus lies dormant in the system for a period of time until a specific action launches it; for example, it might be a single node in a massive pre-planned denial of service (DoS) attack. Once propagated, and at a predetermined moment in time, the virus can self-launch from each of its many victim computer systems (called "zombies") and send a flood of email to a targeted server or servers for any set length of time. The targeted computer is often unable to deal with the DoS attack; even if the targeted server can screen out the zombie emails, it may become so unbearably slow as to be functionally unavailable to legitimate users. More likely, the server will simply crash. Once this virus cycle is started, it can be difficult to detect and harder to stop or eradicate. Another

method an attacker can misuse IS, one that is simplistic and requires little knowledge of networks or how computer systems operate, is electronic *identity theft*, discussed in the next section. Related to electronic identity theft is *assumption of false identity*. For example, recently, a teenager in a major United States metropolitan area, somehow in possession of a police radio, was able to falsely assume the identity of a police dispatcher. This miscreant sent out false commands and alarms, effectively tying up the city's 911 emergency assets for a period of hours until he was finally apprehended (Gunsch, 2002). Because the teenager had the radio, unrestricted access (i.e., no code access or encryption of the radio signal), and motive to misuse a system in which high trust existed, he was able to easily violate the trust model that 911 responders had in their dispatch system. Similarly, false commands or orders could be issued to military personnel via email, and once discovered to be false, could result in a violation of the trust relationship.

One way to protect information systems from these types of exploitations is a Defense in Depth strategy (DiD). DiD combine the capabilities of people, operations, and security technologies to establish layers of protection, and is analogous to a home protection strategy (e.g., fenced property, motion-activated lighting, door locks, burglar alarm, firearm, etc.) (Paul, 2001). DiD for IS security may include protective layers such as physical protection, user vigilance, access controls, user-level privileges, firewalls, intrusion detection system, virus protection software, and other computer-based forms of protection (e.g., screen locks, timeouts, audits, etc.). The purpose of a DiD strategy is to implement a multi-layered defense so that critical information systems are protected and will continue to operate should one or more of the safeguards be thwarted. The Common

Access Card (CAC) employed by the U.S. Air Force is one form of that Defense in Depth strategy. One of the security features of the CAC card is it allows users to authenticate their email when sending it to other email users. The email receiver can then verify this authentication to know for certain that the email originated from a trusted source. This security feature not only provides for human authentication by the email recipient, but also provides system authentication by the email servers. The computer system can authenticate the email message when it is received therefore removing the possibility that the user might not verify the sender is a trusted source. The best security measure though is when both the system and the user verify the authentication. Parasuraman (1987) points this out in his claim that the most potent protection component, is when both human and system vigilance is combined to ensure information integrity.

Identity Theft

Identity theft occurs without the victim's knowledge, when an individual steals or assumes a victim's identity for the purpose of committing a crime (Arnold, 2000). Denning (1999:193) adds,

> Identity theft is the misuse of another person's identity, such as a name, social security number, driver's license, credit card numbers, and bank account numbers. The objective is to take actions permitted to the owner of the identity, such as withdraw funds, transfer money, charge purchases, get access to information, or issue documents and letters under the victim's identity.

Through the use of information systems and the World Wide Web, identity theft is a crime that is growing exponentially. In 2001 alone, more than eighty-five thousand people reported some form of identity theft (Robb, 2002:2). Information systems make it

easier for one to steal another's identity because customers no longer need to be physically present to purchase something. Purchases can be made over the Internet just by knowing a person's name and credit card number.

A criminal can use many methods to steal an individual's identity. They range from high-tech Internet snooping to low-tech dumpster diving. The Federal Trade Commission lists on their Internet site numerous ways the crime is committed (FTC-1, 2002). Mail theft is a common method of identity theft, and can be committed in several different ways. The thief can go to the post office, fill out a change of address form, and have the victim's mail forwarded to his or her address. Another form of mail theft is to steal the victim's mail from his/her mailbox. Mail theft would be an easy way to steal a new credit card application. For instance, suppose an individual receives a pre-approved credit application. The thief steals the application, fills it out, and mails it to the credit card company, except with the thief's mailing address. The thief has just successfully stolen the victim's credit card, and the victim has no idea the theft has taken place. Vigilance would certainly pay off in this instance; if the victim periodically monitored his or her credit, chances are that a newly issued credit card would be noticed. It is conceivable that, if noticed early enough, the victim could alert authorities before an unauthorized purchase even takes place, and could even lead to apprehension of the thief. Other forms of identity theft include stealing information by looking over someone's shoulder ("shoulder surfing"), illegally obtaining credit records, and stealing personal data records. The Internet is a potential identity thief's delight: it provides a nameless, faceless, anonymous interface, and makes identity theft easier and more difficult to

defend against. An identity thief can devastate a victim's life with just a few keystrokes of a keyboard.

However, this research notes a second form of identity theft: *electronic identity theft*, which is committed via some type of electronic communication such as computers, cell phones, or PDAs. Some examples include hackers stealing passwords or other personal information, software Trojans, web page spoofing, email relay eavesdropping, spam-mail forgeries, and email forgery (Denning, 1999:195). *Software Trojans* are programs that are downloaded to a user's computer with the intent of stealing personal information such as names, passwords, credit card numbers, birth dates, email addresses, and other forms of personal information. For example, the Chaos Computer Club demonstrated how a web-delivered Trojan could siphon money out of a person's bank account. Their program used *ActiveX*, an application that downloads a document or application and runs it on the user's computer. This *ActiveX* application scanned the user's computer for *Quicken*, a financial application with a built-in funds transfer capability; if it was found, the Trojan extracted details about the user's bank accounts and created a phony transaction to move money from the user's account(s) to a Chaos account (Denning, 1999:197). *Web page spoofing*, traditionally viewed as hackers exploiting IS vulnerabilities to insert their own illegitimate web pages, can also occur from the web server direction. For example, Princeton researchers demonstrated that, after enticing someone to their web site, they were able to keep the person within their site when the user tried to go elsewhere by presenting counterfeit non-Princeton web pages to them, all done without the user ever knowing the spoof had taken place (Denning, 1999:199). *Email relays* provide a service to users that allow them to have a permanent email

address while another email provider hosts the actual email service. One such email relay company is bigfoot.com. A user can obtain a permanent email address from bigfoot.com (e.g., yourname@bigfoot.com), while another company (e.g., AOL) serves as the person's actual email host interface; bigfoot.com simply forwards all email received for that user to their current email host server. If a user changes their email service, they provided bigfoot.com with the new host server information, and bigfoot.com can then forward their email (still directed to yourname@bigfoot.com) to their new email host without the user having to change their actual email address. The drawback with this type of service is that the email relay service can eavesdrop on all email going through their servers. Nevertheless, this type of service might appear attractive to anyone who frequently changes email services, such as PCSing military members. *Milmail*, one such provider based in the Netherlands, targets email relay specifically to military members; however, a significant concern is that *Milmail* could theoretically collect information on military personnel, movements, and operations, and sell it to our enemies. *Spam-mail forgeries* occur when bulk email is sent out with a bogus return email address. For example, a denial of service (DoS) attack utilizing a spam-mail forgery took down 1-800-flowers' servers. A spammer sent out a bogus email using flowers.com as the return email address advertising a non-existent flower sale. Flowers.com, flooded with more emails than they could handle, was forced to shut down their email servers. The final type of electronic identity theft is *email forgery*. Email forgery is defined as someone changing the outgoing email address to appear to originate from someone or some organization other than it actually did; essentially, the email forger assumes someone else's position or identity through the use of email. For

example, at Dartmouth College, a student sent an email message from a department secretary that claimed an examination was canceled (Denning, 1999:202). Email forgeries are relatively easy and do not require a vast amount of technical knowledge to commit; forgers can steal an individual's or organization's email identity through several methods. One method that does require a substantial amount of technical ability is hacking into the victim's computer account/email account. This method would probably exceed most users' abilities. However, much easier is simply changing the return address to something other then the actual email origination; curiously, some email services allow the sender to change the outgoing email address to anything they want. Another form of email forgery is to create a bogus *hotmail*, *yahoo* or some other commercial source email account with the individual's name as the address. All of these are forms of electronic identity theft.

The federal government is trying to prevent this type of criminal activity. For example, in 1998 Congress passed the Federal Identity Theft and Assumption Deterrence Act, which established identity theft as a felony and defined it as the following:

> "Any individual who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law" (FTC-2, 2002).

Additionally, the act calls for violators to be investigated by the U.S. Secret Service, the FBI, the U.S. Postal Service and calls for the Department of Justice to prosecute any form of this criminal activity. The final provision in this act allows victims

to receive financial restitution from the individual who committed the crime against them.

This research will conduct a study on Air Force personnel to determine if email forgery is a vulnerability to which they are susceptible. The study will involve creating a forged email address from some commercial source to duplicate a military email address. It will involve sending emails to participants to see if they can determine which of the emails came from a forged source. If it is determined that the majority of participants respond to the email forgery, then a new vulnerability the Air Force needs to be aware of will have been identified.

Research Hypotheses and Model

Studies done on whether humans are good detectors of deception have shown that humans are not good at detecting deception and in most cases are no better than chance. Studies show that lie detection accuracy falls in the range of 45%-60% (Zuckerman et al., 1984; DePaula et al., 1985). Many research in the arena of deception detection focuses on interpersonal forms of deception, which is face-to-face communication. IDT as stated previously involves verbal and non-verbal communication with both strategic and non-strategic behaviors. Non-verbal and verbal cues are given by the sender and processed and interpreted by the receiver. In text-based communication, there are no non-verbal cues only verbal cues. These verbal cues are text-based, so no noise takes place. The receiver only sees words written on a document or software system. This narrows the number of cues a receiver has to detect, but it also lowers the number of ways a person can deceive. Studies in interpersonal communication reveal that there are two results that

can increase a persons' sensitivity to deception, they are: 1) training on deception detection (DePaulo et al., 1983; Zuckerman et al., 1984; deTurck et al., 1990) and 2) receiving explicit alerts about the possibility of deception within a text-based medium (Biros et al., 2002; Miller and Stiff, 1993; Parasuraman, 1984; Stiff et al., 1992). DeTurck et al. (1990) found that formal training for observers to detect deception improved their judgmental precision. Biros et al. (2002) found that training in a text based or artifact-based environment does not necessarily increase an individual's ability to detect deception. This study also found that user experience and awareness or suspicion significantly improved a person's ability to detect deception in text-based medium. The model for this research began with the construct defined in the research by Biros et al. (2002) that warnings will increase an individual's ability to detect deception. In their research, they were looking at whether traditional training would increase an individual's ability to detect deception in computer based data. Although they found that traditional training did not increase an individual's ability to detect deception, they did find that by issuing a warning prior to the deception the participants' ability to detect deception was increased. Therefore, we would expect this construct to apply to the research in electronic identity theft – email forgery.

> *H1: Warnings about possible deception via electronic identity theft will be positively associated with detection success.*

Since warnings decrease an individual's level of trust, it should also be positively associated with a heightened level of awareness. Existing research points out that individuals are generally not good at detecting deception, but if an individual's awareness

is aroused, their ability to detect deception increases (Stiff et al., 1992; Miller and Stiff, 1993; Parasuraman, 1984; Biros et al., 2002). Therefore, we expect:

> *H2: Warnings about possible electronic identity theft will be positively associated with an individual's level of awareness.*

Buller and Burgoon (1996:209) say, "trust is the foundation on which enduring relationships are built, and trust grows with the belief that another is communicating in a honest, straightforward manner." If a warning suggests someone is not communicating in a straight forward manner, this warning arouses suspicion and causes a receiver not to necessarily believe what the sender is communicating. Stiff et al. (1992) suggests that in relationships with well-developed truth biases, warnings from a third party will decrease the receiver's levels of trust in the relationship. Information from a third party may be sufficient to provoke suspicion and affect truth bias judgments. Stiff et al. (1992) further suggests that the truth bias heuristic serves to increase judgments of truthfulness, therefore aroused suspicion by a third party to the receiver will offset this bias, producing greater judgments of deceptiveness. For instance, when an individual places a high level of trust in a system and that trust has been established over time, the individual will be less susceptible to detecting deception unless some form of warning provokes suspicion, therefore decreasing levels of trust. Warnings will place an individual in a heightened state of alert (Stiff et al., 1992; Biros et al., 2002). Therefore, we expect:

> *H3: Warnings about possible electronic identity theft will be negatively associated with system trust.*

Lee (1992) found that when trust is low, self-confidence is high. He found that as trust declines, self-confidence rises (Lee, 1992; Lee and Moray, 1992). We would expect

as this heightened state of alert or awareness increases, levels of system trust would decrease. It is thought that if a participant's level of system trust is high, (i.e., they have a high level of trust that the system will identify the deceptive messages,) then he or she will be less likely to identify deceptive messages themselves. In regards to awareness, it is thought that if the participant's awareness is high, then the participant will be more likely to identify deceptive messages because he or she will be more alert. It is hypothesized that system trust and awareness are inversely correlated. That is, if system trust is high, awareness will be low. Also, if awareness is high, system trust will be low. Therefore, we expect:

H4a: System trust will be negatively associated with awareness.

Muir (1992) suggests that trust in machines will increase with experience over time. The longer an individual works with a reliable system, the greater the level of trust. Lee (1992) found that as self-confidence declines, levels of trust are increased. Stiff et al. (1992) says that well-established trust relationships (truth bias) are not likely to become suspicious on their own. Increased levels of trust are established unless a third party introduces some form of suspicion. Egan et al. (1961) showed that an observer's sensitivity in detecting a signal declines over time. This decline in sensitivity is in direct relationship with the decision heuristic that it is easier to trust than it is to perceive deceit in communication (Buller et al., 1991a; Buller et al., 1991b; Stiff et al., 1992; McCornack and Parks, 1986). This increase in levels of trust has a direct effect on an individual's ability to detect deception in communication – sensitivity to deception is likely to decline over time (Parasuraman, 1984). Because a user's level of trust (or faith) has been

established and grown through successful past uses, it is easier for the user to trust that continued successful communications will occur in the present than it is to attempt to detect deception. Therefore, we expect:

H4b: System trust will be negatively associated with deception detection.

Warnings will cause an individual to place a lower level of trust in a system (Stiff et al., 1992). Awareness is that heightened state of alert caused by the third party suspicion introduction (warning). This warning induced awareness was shown to increase an individual's ability to detect deception correctly in the Biros et al. (2002) study. Hence, since suspicion is now introduced (or perhaps awareness heightened to an unacceptable level from a previous minimally acceptable level), there is cause for the truth bias norm to be questioned. Therefore we expect:

H5: Awareness about possible electronic identity theft will be positively associated with deception detection.

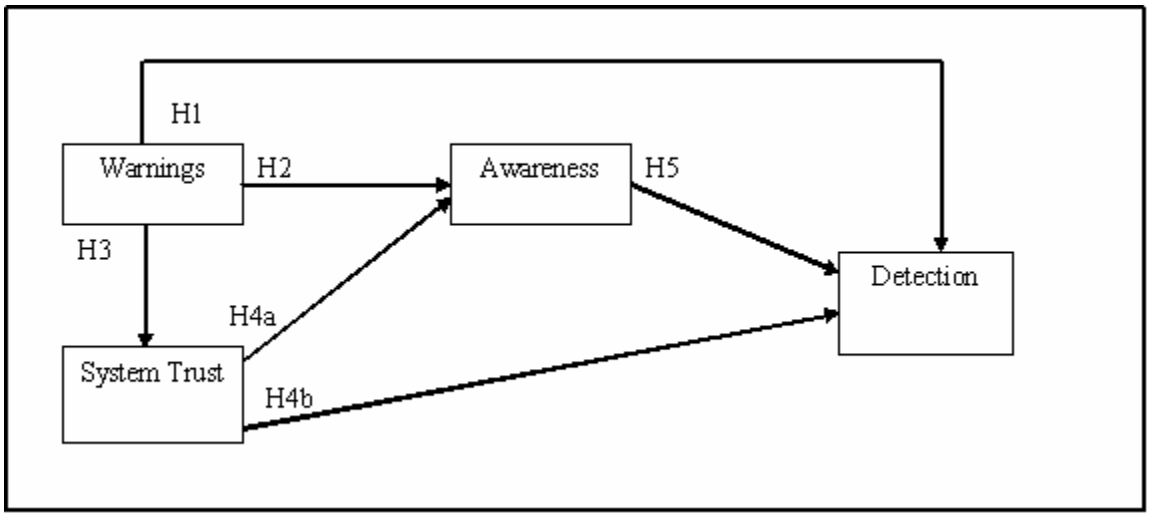

Figure 2: Theoretical Research Model for Research in Electronic Identity Theft

Summary

This chapter provided a literature review of the body of knowledge on deception, trust, information warfare, identity theft, and email forgery. In addition, it presented a theoretical framework from which the research problem could be explored. Finally, a set of hypotheses were presented to predict the type of relationships between each of the defined constructs. The research model can be seen in Figure 2 on the previous page. Chapter III describes a research method to investigate the theorized relationship between warnings, system trust, awareness, and detection of information manipulation. Chapter IV presents the analysis of the data collected, statistical methods used, and inferences made about the data. Chapter V presents the research findings, conclusions and recommendations for future research efforts.

III. Methodology

Study Summary

In order to study a person's trust, awareness, and ability to detect manipulation in an information system, a two stage process was developed consisting of a questionnaire, and an information system manipulation experiment. This allowed analysis of the constructs defined in Chapter II of this research. The questionnaire was used to study the relationships between warnings and participants' levels of system trust and awareness. An experiment phase was used to provide a manipulation of an information system to determine how participants who receive a warning perform against those who do not receive a warning. The information system used was the Air Force Institute of Technology (AFIT) email system. Two experiments were conducted to allow this research to compare and confirm the findings from each of the experiments.

Participants

The participants in Experiment 1 were 80 officers at AFIT's Graduate School of Engineering and Management, between the ranks of 2Lt and Maj (grades O1 – O4). Each participant had a Bachelor's degree and was a student working towards a Master of Science or Doctorate of Science Degree at AFIT. Seventy-six of the participants in the Experiment 1 were officers in the U.S. Air Force. There was one participant each from the U.S. Marine Corps, the Turkish Air Force, the Australian Air Force, and the South Korean Air Force. The participants' mean age was 29.7 years old. The participants included 68 males and 12 females. The level of email experience ranged from three years

to more than 10 years experience. Seven participants had some level of experience with computer security. The participants in Experiment 2 were 67 Air Force officers, two Air Force enlisted, two Marine enlisted, and one Air Force civil service personnel at AFIT's Graduate School of Engineering and Management. Experiment 2's military participants' ranks ranged from SSgt to Capt (grades E6 – O3). Each participant had a Bachelor's degree and was a student working towards a Master of Science or Doctorate of Science Degree at AFIT. The participants' mean age was 30.3 years old. The participants included 61 males and 11 females. The level of email experience ranged from two years to more than 10 years experience. Fifteen participants had some level of experience with computer security. In this research each participant participated in both the questionnaire and experiment.

Procedures

Due to the nature of the manipulation during both experiment phases of this study, the Air Force Research Laboratory Human Subjects Committee required all participants to read and sign a consent form. This was accomplished by meeting with the participants. Each participant was given time to read, review, and ask any questions concerning his or her participation in this research project. Participants were told to review the consent form, sign it, and return it no later than one week from the day they received it. The consent form and Human Subjects Review Board application can be seen in Appendix A.

Questionnaire

The questionnaire consisted of 15 questions and was administered electronically. Ten questions were tailored to identify system trust. Five questions were tailored to identify awareness. On all items, participants indicated their level of agreement with each item using a five point Likert scale: *5 = Strongly Agree, 4 = Agree, 3 = No Opinion, 2 = Disagree, and 1 = Strongly Disagree*. The questionnaire used to identify trust and awareness was developed and empirically tested by researchers at the Center for Multi-source Information Fusion (CMIF) (Jian, Bisantz, & Drury, 1998). The original set of items was tailored to specifically measure system trust and awareness relative to the AFIT email system. Jian et al. (2000) anticipated this type of manipulation and designed the questions to be generic and adaptable to specific information systems. An example from the CMIF questionnaire item measuring trust is, "I can trust the system." For this study, this item was tailored to read, "I can trust the AFIT Network Operations and Security Center to protect me from attacks to the local area network and email." For awareness, an example from the CMIF questionnaire is, "I am wary of the system." For this study, this item was tailored to read, "I feel I am always aware of information warfare threats and computer system vulnerabilities. Schmit, Ryan, Stierwalt, and Powell found that items measuring context-specific personalities had higher validities then items measuring general personality (1995). Based on this finding, it is believed that the items used in this research are more context specific; therefore, they will be more valid.

The objective of the questionnaire was to show how system trust and awareness were related to warnings and participants' deception detection ability. This analysis was

compared with the experiment to determine the overall success of this study. This can be seen in Chapter IV on Analysis.

Pilot Study

A pilot study was conducted on the questionnaire to ensure the survey proved reliable for this study. The questionnaire was sent to all AFIT, School of Systems and Logistics, faculty, and staff. Twenty-eight personnel responded by completing the questionnaire. The participants' mean age was 43 years old. The participants included 19 males and nine females. The level of email experience ranged from two years to more than 10 years experience. In the pilot study, none of the participants had any experience with computer security. The participants in the pilot study provided a good comparison to the actual sample used in the study because experience with government email systems was roughly the same. The largest difference between participants in the pilot study and the actual study was participants were students, not faculty and staff. All participants, both in the pilot study and in the final experiment were daily users of the AFIT email system. In order to ensure reliability of the questionnaire during the pilot study a reliability analysis was performed and recorded. The Cronbach's alpha reported for the 10 items dealing with systems trust was .86 and the Cronbach's alpha recorded for the five items dealing with awareness was .70. A reliability level above .70 indicates the measure is sufficiently reliable for studies using Likert scale items (Nunnally, 1978).

Experiment

The research design for the first experiment used five emails sent at five different times, with four of those emails coming from a legitimate source and one coming from a fraudulent source (i.e., an email forgery) (See Table 1). For the second experiment a three email design was used, with two of those emails coming from a legitimate source and one coming from a fraudulent source (See Table 2). For the purposes of this study, an email forgery is defined as a case where the source of the email address has been manipulated. It was determined during Experiment 1 that four legitimate emails may have conditioned the participants to the legitimate source, thus reducing their awareness and ability to discover the email forgery. The Experiment 2 was designed with that finding in mind. The AFIT Network Operations and Security Center (AFIT.NOSC@afit.edu) was the legitimate source used to send the four legitimate emails during Experiment 1 and the two legitimate emails during Experiment 2. Permission was granted to duplicate the AFIT NOSC email address with a commercial source email address. The commercial source email address was used for the fraudulent source. The commercial source used to send the email forgery was afit_network_operations_and_security_center@ (commercialsource).net. (The source has been withheld to protect the rights of the corporation.) This email account was created temporarily to execute these experiments. Once the experiments concluded, the account was terminated.

The consent form mentioned the possibility of email manipulation increasing the participants' awareness to email manipulation. Due to this increased awareness of the participants, an environment had to be created that reduced the participants' awareness to

information manipulation. This increased awareness was a problem and the reason behind the five email design during Experiment 1. This five email design was used to create a trusted environment in which the participants' suspicion to email manipulation was decreased. It was determined after Experiment 1 that the five emails may have conditioned the participants causing their awareness to be decreased; therefore Experiment 2 reduced the number of emails to a total of three. The emails were sent every other day during a two week time-period. For example, during Experiment 1, at time 1, the legitimate email was sent to five groups and the fraudulent email was sent to one group. During the Experiment 2, the legitimate email was sent to three groups and the fraudulent email was sent to one group.

Table 1: Experiment 1 - Research Design

	*WG1	WG2	WG3	**NWG1	NWG2	NWG3
Legitimate Source	4 emails	4 emails	4 emails	4 emails	4 emails	4 emails
Fraudulent Source	1 email	1 email	1 email	1 email	1 email	1 email

* WG = Warning Group

**NWG = Non-Warning Group

Table 2: Experiment 2 - Research Design

	*WG1	WG2	**NWG1	NWG2
Legitimate Source	2 emails	2 emails	2 emails	2 emails
Fraudulent Source	1 email	1 email	1 email	1 email

In addition, during both experiments participants were randomly assigned to one of two groups. The groups were named Warning Group and Non-Warning Group. The Warning group received a message prior to the start of the experiment warning the participants of a possible email forgery. This message explained to the participants what an email forgery was and that the AFIT NOSC had seen an increase in this type of fraudulent activity (See Appendix B for the actual warning email). The Non-Warning Group did not receive this email. Next during Experiment 1, those two groups were broken down into three sub-groups each. This brought the total number of groups for Experiment 1 to six. The Warning Group was broken down into: Warning Group 1, Warning Group 2, and Warning Group 3. The Non-Warning Group was accomplished the same way: Non-Warning Group 1, Non-Warning Group 2, and Non-Warning Group 3. The six sub-groups were created to allow this research to determine if email forgeries were more susceptible to detection early in the process or late in the process. During Experiment 2, these two groups were broken down into two sub-groups each, two Warning groups and two Non-Warning groups. This brought the total number of groups for Experiment 2 to four.

To determine how each sub-group performed over time, a timeline was devised to specify when each sub-group would receive the email forgery from the fraudulent source and when each sub-group would receive the four emails from the legitimate source (See Tables 3 and 4). Non-Warning Group 1 was chosen to receive the email forgery at Time 1 for both experiments. The reason a non-warning group was chosen over a warning group was to allow a certain amount of time to pass between the warning the warning groups received and the actual email forgery. Warning Group 1 was chosen to receive the email forgery at Time 2 for both experiments. Each of the six sub-groups in Experiment 1 and four sub-groups in Experiment 2 were alternated until each sub-group had received an email forgery at one of the five different times during Experiment 1 and three different times during Experiment 2 (See Tables 3 and 4).

Table 3: Experiment 1 - Timeline for email forgery for each sub-group (Total time interval was two weeks).

	*NWG1	**WG1	NWG2	WG2	NWG3	WG3
Time 1 - Monday Week 1	**Email Forgery**	True Email	True Email	True Email	True Email	True Email
Time 2 - Wednesday Week 1	True Email	**Email Forgery**	True Email	True Email	True Email	True Email
Time 3 - Friday Week 1	True Email	True Email	**Email Forgery**	True Email	True Email	True Email
Time 4 - Tuesday Week 2	True Email	True Email	True Email	**Email Forgery**	True Email	True Email
Time 5 - Thursday Week 2	True Email	True Email	True Email	True Email	**Email Forgery**	**Email Forgery**

* NWG = Non warning Group
**WG = Warning Group

Table 4: Experiment 1 - Questions asked at each of the different time frames.

	*NWG1	**WG1	NWG2	WG2
Time 1 - Monday Week 1	**Email Forgery**	True Email	True Email	True Email
Time 2 - Wednesday Week 1	True Email	**Email Forgery**	True Email	True Email
Time 3 - Friday Week 1	True Email	True Email	**Email Forgery**	**Email Forgery**

Each sub-group received one email forgery from the fraudulent source at one of the five determined times described in Table 3 for Experiment 1 and three different times described in Table 4 for Experiment 2. The other sub-groups, when not receiving an email forgery, received an email from the legitimate source. The six sub-groups in Experiment 1 and the four sub-groups in Experiment 2 all received the same five and three questions, respectively. There were five questions asked at the five different time intervals during Experiment 1 and three questions ask at three different time intervals during Experiment 2 (see Tables 5 and 6). For Experiment 1, at each time interval, five of the six sub-groups received an email from the legitimate source and one of the six sub-groups received an email forgery from a fraudulent source. For Experiment 2, at each time interval, two of the three sub-groups received an email from the legitimate source and one of the three sub-groups received an email forgery from a fraudulent source. Questions asked at each specific time were the same regardless of where the email originated. Participants received the email in their official email box and were asked to reply to the email with a "yes" or "no" answer. All responses were sent to the researchers email address for data collection purposes. "Yes" response was used if they were satisfied with the support and a "no" response if they were not satisfied with the support. The questions can be seen in tables 5 and 6. The five emails for Experiment 1 and three emails for Experiment 2 were set to expire using Microsoft Outlook's "expire on certain date feature." This feature automatically removed the email from the participant's inbox, and placed it in the participant's deleted items folder. This was done to prevent the participants from going back after the experiment to verify which email was a forgery. The intent of the experiment was for the participant to identify the email forgery when it

occurred, not at the end of the experiment. All efforts were made to prevent the participants from identifying the email forgery at the end of the experiment verses when it actually occurred.

Table 5: Experiment 1 - Questions asked at each of the different time frames.

Time	*Questions*	*Answer*
Time 1 Question	Are you satisfied with the Internet browsing capabilities at AFIT?	Yes/No
Time 2 Question	Are you satisfied with the E-mail capabilities at AFIT?	Yes/No
Time 3 Question	Are you satisfied with AFIT's Computer Support Help Desk?	Yes/No
Time 4 Question	Are you satisfied with AFIT's remote login procedures?	Yes/No
Time 5 Question	Are you satisfied with the overall support the Network Operations and Security Center provides?	Yes/No

Table 6: Experiment 2 - Questions asked at each of the different time frames.

Time	*Questions*	*Answer*
Time 1 Question	Are you satisfied with the E-mail capabilities at AFIT?	Yes/No
Time 2 Question	Are you satisfied with AFIT's Computer Support Help Desk?	Yes/No
Time 3 Question	Are you satisfied with the overall support the Network Operations and Security Center provides?	Yes/No

The questions were designed to be benign in nature. The questions did not ask the participants any personal information. This was done to determine whether people paid attention to the email address they were responding to. It was thought that if the questions had asked the participants personal information it may have heightened their awareness. This heightened awareness due to the context of the message was not a desired result for this research. This research wanted to establish if participants paid attention to the email address they responded to. The questions were designed to be simple in nature (not suspicion arousing) to determine if they would respond to the forged email based on the environment created from the experiment. It was hypothesized that the warning sent to the Warning Group would raise suspicion, therefore causing a heightened sense of awareness in the Warning Group. During Experiment 1, the only way the participant could determine whether the message was from the legitimate source or the fraudulent source was by looking at the sender's address line on the email message. During Experiment 2, a manipulation was made in the senders signature block to see if cues in the message would help add to the participants' ability to better identify the email forgery (See Appendix C for this manipulation). In both experiments, when the participants selected the reply to button from the forged email, the forged email address afit_network_operations_and_security_center@commercialsource.net was displayed directly in front of them in the To: address line. Each participant had an equal opportunity to identify it. AFIT students and therefore these participants know from previous computer security training during their in-processing to AFIT to be aware of the sender's address when replying to an email requesting any information. This includes yes and no responses to emails. For the purposes of this study, the names and ranks of

the participants were known. In a real world scenario, a criminal might have been trying to establish if someone was a military member and where they worked. It is public knowledge that U.S. Air Force email addresses are designed using a generic first name.last name @ AirForceBase.af.mil procedure. For example, john.doe@wpafb.af.mil. Criminals can use this to their advantage and send emails to a list of names in the attempt that someone might reply. If someone does happen to reply, the criminals have just verified the individual's name, email address, and rank. Criminals or terrorists who want to infiltrate our networks will do so patiently collecting information in small pieces until they have what they need. The point of these experiments was to determine if people paid attention to the email address they were responding to, not necessarily to raise their awareness by asking for personal information.

The experiments concluded with an email asking the participants if they identified any counterfeit emails during the two-week time period for these two research experiments and to explain what they identified. This email was used to increase the response rate to 100% from the participants because not all participants responded to the five email questions during the experiment. The participants were asked to identify this email forgery from memory and not to go back through their email folders to determine if they could figure out which email was from a fraudulent source. The participants were asked to be honest in their responses, as being deceived by the email forgery was part of this research. The participants who did not identify the email forgery were asked to respond to this email with a "no" reply. If the response was "yes", the participant did identify the email forgery when it occurred, and they correctly described what the counterfeit email was, the participant received a second email asking them to identify

which question was an email forgery. In this email, it listed each of the five questions and had the participants identify which email was from a counterfeit source. If the response was “no”, the participant did not receive a second email.

Summary

This chapter described a research method to investigate the theorized relationship between warnings, system trust, awareness, and detection of information manipulation. It described an experimental methodology and how each construct was operationalized and measured. Chapter IV presents the analysis of the data collected. In this chapter each stage of the research will be examined individually and then cross compared with the other stages. For example, the results from the questionnaire will be examined individually and than cross-analyzed with the results from the experiment. Chapter V presents the research findings, conclusions and recommendations for future research efforts.

IV. Analysis

Overview of Questionnaire

The questionnaire was designed to show how system trust and awareness were related to warnings and participants' deception detection ability. It established a starting point from which further research could determine the participants' ability to detect deceptive messages. It was thought that if a participant's level of system trust was high, (i.e., they had a high level of trust that the system would identify the deceptive messages,) then he or she would be less likely to identify deceptive messages themselves. In regards to awareness, it was thought that if the participant's awareness was high, then the participant would be more likely to identify deceptive messages because he or she would be more alert. Therefore, it was hypothesized that system trust and awareness are inversely correlated. That is, if system trust is high, awareness will be low. Also, if awareness is high, system trust will be low. The questionnaire consisted of 15 items and was administered electronically. As noted in the preliminary analysis, ten items were tailored to identify levels of system trust. Five items were tailored to identify levels of awareness. Participants indicated their level of agreement with each item using a five-point Likert response format where *5 = Strongly Agree, 4 = Agree, 3 = No Opinion, 2 = Disagree, and 1 = Strongly Disagree*.

Factor Analysis of Questionnaire

A factor analysis was performed on both experiments separately and combined to establish the construct validity of the measure. However, before this analysis was

conducted, the data were examined to assess its suitability for this analysis. For Experiment 1, the Bartlett's test of spericity revealed the data was suitable for factor analysis with a $\chi^2 = 504.6$, $p < .01$. The Kaiser-Meyer-Olkin measure of sampling adequacy was .74 this exceeds the stated level for suitability of .70 (Hair, 1995). For Experiment 2, the Bartlett's test of spericity revealed the data was also suitable for factor analysis with a $\chi^2 = 282.1$, $p < .01$. The Kaiser-Meyer-Olkin measure of sampling adequacy was .79. The combined Bartlett's test of spericity revealed the data was suitable for factor analysis with a $\chi^2 = 680.1$, $p < .01$. The Kaiser-Meyer-Olkin measure of sampling adequacy was .76. These tests of assumption reveal the data is suitable for exploratory factor analysis. The factor analysis was performed on system trust and awareness separately. For the 10 items used to measure system trust one factor was expected, but the factor analysis revealed two factors with eigenvalues greater then 1.0. Eigenvalues that are less then 1.0 usually account for less variance. Kachigan states "the rule of thumb is to retain factors with eigenvalues greater then 1.0" (1991, pp. 246). Two items showed a significant cross loading between the two factors in both the analysis of experiments individually and combined. Experiment 1 analysis revealed the item measuring a participant's belief in the system showed a loading of 0.61 for Factor 1 and 0.41 for Factor 2. The item measuring a participant's comfort level in the system showed a loading of 0.69 for Factor 1 and 0.36 for Factor 2. Experiment 2 analysis revealed the item measuring a participant's belief in the system showed a loading of 0.43 for Factor 1 and 0.69 for Factor 2. The item measuring a participant's comfort level in the system showed a loading of 0.55 for Factor 1 and 0.31 for Factor 2. The combined analysis revealed the item measuring a participant's belief in the system showed a loading of 0.53

for Factor 1 and 0.57 for Factor 2. The item measuring a participant's comfort level in the system showed a loading of 0.61 for Factor 1 and 0.38 for Factor 2. These items were removed and the factor analysis was performed a second time resulting in eight items loading on a single factor in each of the three separate factor analysis termed "system trust" (see Table 7). The final Experiment 1 factor analysis for system trust revealed a single eigenvalue of 4.1 and loadings on a single factor captured 50% of the total variance. The final Experiment 2 factor analysis for system trust revealed a single eigenvalue of 4.2 and loadings on a single factor captured 52% of the total variance. The final combined factor analysis for system trust revealed a single eigenvalue of 4.2 and loadings on a single factor captured 52% of the total variance. The new combined Cronbach's alpha was .85. Experiment 1 Cronbach's alpha was .82. Experiment 2 Cronbach's alpha was .86.

Table 7: Combined Experiment Factor Loadings of System Trust

Trust Items	Factor Loading
6. I feel the Web email system AFIT/SC provides is a trusted environment.	0.83
15. What level of trust do you place in the email system here at AFIT?	0.83
5. I feel secure about the Web email system AFIT/SC provides.	0.81
13. In your own opinion, do you feel the AFIT email system is secure from information warfare threats?	0.72
11. In your own opinion, how effective do you feel the government email system here at AFIT is?	0.67
10. The government email system AFIT/SC provides has enough safeguards to make me feel comfortable using it to send and receive messages to perform real-world missions.	0.67
1. I feel assured the AFIT Network Operations and Security Center adequately protects me from attacks to the local area network and email.	0.67
3. My typical approach is to trust the government email system until it proves I should not trust it.	0.51

For the five items used to measure awareness one factor was expected, but the factor analysis revealed two factors with eigenvalues greater then 1.0 in the individual analysis of Experiment 1 and 2, and the combined analysis. For Experiment 1 and the combined analysis it was revealed that one item showed a significant cross loading between the two factors and the other item loaded on the second factor. For Experiment 2 the analysis revealed two items with significant cross loadings. For Experiment 1, the item measuring if a participant feels they are always aware of threats and vulnerabilities

loaded on Factor 2 completely. The item asking the participant to state in their own opinion what level of awareness do they feel they have against threats showed a loading of 0.53 for Factor 1 and 0.63 for Factor 2. For Experiment 2, the item measuring if a participant feels they are always aware of threats and vulnerabilities showed a loading of 0.65 on Factor 1 and 0.35 on Factor 2. The item asking the participant to state in their own opinion what level of awareness do they feel they have against threats showed a loading of 0.30 for Factor 1 and 0.79 for Factor 2. For the combined analysis, the item measuring if a participant feels they are always aware of threats and vulnerabilities loaded on Factor 2 completely. The item asking the participant to state in their own opinion what level of awareness do they feel they have against threats showed a loading of 0.68 for Factor 1 and 0.44 for Factor 2. After those two items were removed, each of the three separate factor analysis yielded three items loading on a single factor, awareness (see Table 8). The final Experiment 1 factor analysis for awareness revealed a single eigenvalue of 1.7 and loadings on a single factor captured 57% of the total variance. The final Experiment 2 factor analysis revealed a single eigenvalue of 1.6 and loadings on a single factor captured 52% of the total variance. The combined factor analysis showed a single factor with an eigenvalue of 1.7, accounting for 55% of the total variance. The combined Cronbach's alpha was .56. Experiment 1 Cronbach's alpha was .62. Experiment 2 Cronbach's alpha was .41. However, since the item asking if the user thinks warnings increase awareness loads at 0.54 whereas the other two items load at 0.84 and 0.82 this item was deleted and the combined Cronbach's alpha improves to .68. Therefore, awareness was measured using a two-item scale.

Table 8: Combined Factor Loadings of Awareness

Awareness Items	Factor Loading
3. I feel it is my duty to be aware of information warfare threats and report them to the AFIT Network Operations and Security Center.	0.84
8. I feel the only one responsible to be aware of information warfare threats or computer system vulnerabilities is the AFIT Network Operations and Security Center.	0.82
12. In your own opinion, do you feel your level of awareness is increased if the AFIT Network Operations and Security Center sends out a warning about possible information warfare threats?	0.54

The next phase of analysis was to test for whether the curves for system trust and awareness were normally distributed. This can be seen in the skewness and kurtosis reported in Table 9. The skewness is -0.48 and the kurtosis is 0.52 for system trust. This shows the curve for systems trust was slightly skewed to the left because of its negative skewness and the kurtosis was leptokurtic (thin bulging) since it has a positive value. The skewness is -.99 and the kurtosis is 1.34 for awareness. The skewness for awareness was skewed to a higher degree to the left then system trust and the kurtosis was even more leptokurtic since it has a fairly high positive value. The skewness and kurtosis values for both system trust and awareness are within the accepted range for the assumption of normality (SPSS, 1999).

The next phase of the analysis for the questionnaire was to check the reliability of the questionnaire. The combined Cronbach's alpha reported for the eight-item system trust scale decreased slightly from .86 to .85 after the factor analysis, but this is still considered a high estimate of reliability (Nunnelly, 1978). This reliability analysis

showed that the eight items used to measure system trust are reliable. The combined Cronbach's alpha reported for the three-item scale measuring awareness also slightly decreased from .59 to .56 after the factor analysis. This is below normally accepted levels of reliability and may be a weakness for this study. However, the Cronbach's alpha for the two-item scale increases from .59 to .68. This is slightly below the normally accepted level of .7, but would be considered significant in statistical research (Nunnelly, 1978). Therefore, the reliability analysis for the two-items used to measure awareness is reliable. The Pearson correlation reflects that system trust and awareness have no correlation (see Table 9 for values). This finding does not support hypothesis 4a (i.e., system trust will be negatively associated with awareness). However, Nunnelly says, "One should be extremely cautious in applying the deduction that there is no correlation in samples of less than several hundred" (1978; p.128). Further analysis of hypothesis 4a can be seen in the following section.

Table 9: Descriptive Statistics for System Trust and Awareness

Variable	*M*	*SD*	*S*	*K*	α	*Pearson Correlation*
System Trust	3.99	0.56	-0.48	0.52	0.85	
Awareness	4.25	0.56	-.99	1.34	0.56	-0.02

Note *N*=152. S = Skewness, K = Kurtosis

Analysis of Variance for Warning and Non-Warning Groups

The participants from Experiment 2 were divided into two randomly selected groups of 36 participants each called Warning Group and Non-Warning Group. The Warning Group received an email prior to the start of the questionnaire warning the participants of a possible email forgery. This email explained to the participants what an email forgery was and that the AFIT NOSC had seen an increase in this type of fraudulent activity (see Appendix B for warning email). In Experiment 1, the warning email was sent to the Warning Group after the questionnaire was administered and not before. Therefore, one-way ANOVAs were not conducted. The results between groups in Experiment 1 would have shown no difference, because neither the Warning Group nor the Non-Warning Group had received anything that would have heightened their awareness or lowered their system trust. During Experiment 2, the warning was sent to the Warning Group before the questionnaire was administered. Therefore, a difference in the system trust and awareness of the Warning and Non-Warning groups should have been observed.

One-way ANOVAs were conducted to determine if there was a significant difference in the Warning and Non-Warning groups of Experiment 2. The Warning Group was coded with a 1 and the Non-Warning Group was coded with a 0. This is the independent variable of this study. The result of the ANOVA comparing the means for system trust revealed an F-statistic 0.082, which showed that the difference was insignificant ($p>.05$) (SPSS, 1999). The result for awareness was 0.007, which also showed that the differences were insignificant ($p>.05$) (SPSS, 1999). Therefore, the results showed that system trust and awareness did not have a negative relationship. The

results reveal that no relationship exists between system trust and awareness. This could mean several things, it could mean system trust and awareness have no relationship as reported by this study or it could mean the items used to measure system trust and awareness do not fully depict those constructs. This finding does not support hypothesis 2 (i.e., warnings about possible electronic identity theft will be positively associated with an individual's awareness), hypothesis 3 (i.e., warnings about possible electronic identity theft will be negatively associated with system trust), or hypothesis 4a (i.e., system trust will be negatively associated with awareness). Table 10 presents the results for the ANOVA.

Table 10: Experiment 2 ANOVA Results for Warning and Non-Warning Groups

	Warning Group		Non-Warning Group		ANOVA		
Variable	*M*	*SD*	*M*	*SD*	*df*	*F*	*p*
System Trust	4.07	0.5	4.03	0.62	1,71	0.082	0.775
Awareness	4.35	0.43	4.36	0.48	1,71	0.007	0.932

Note N=72

Further analysis of the questionnaire revealed that system trust in well established systems does not decrease when a warning suggesting manipulation of the system is issued. This provides additional support to the finding from the ANOVA that revealed hypothesis 3 was not supported. System trust in email systems remains almost the same

(i.e., a person's trust in the system does not decrease). This can be seen in the comparisons of the distributions between the Warning Group and the Non-Warning Group (see Figure 3). The mean system trust for Warning Group was 4.03 and for the Non-Warning Group was 4.06. Standard deviation for the Warning Group was 0.5 and for the Non-Warning Group was .61. The plot reveals that each distribution is extremely similar, leading this research to conclude, that system trust does not decrease if a warning suggesting manipulation is issued.

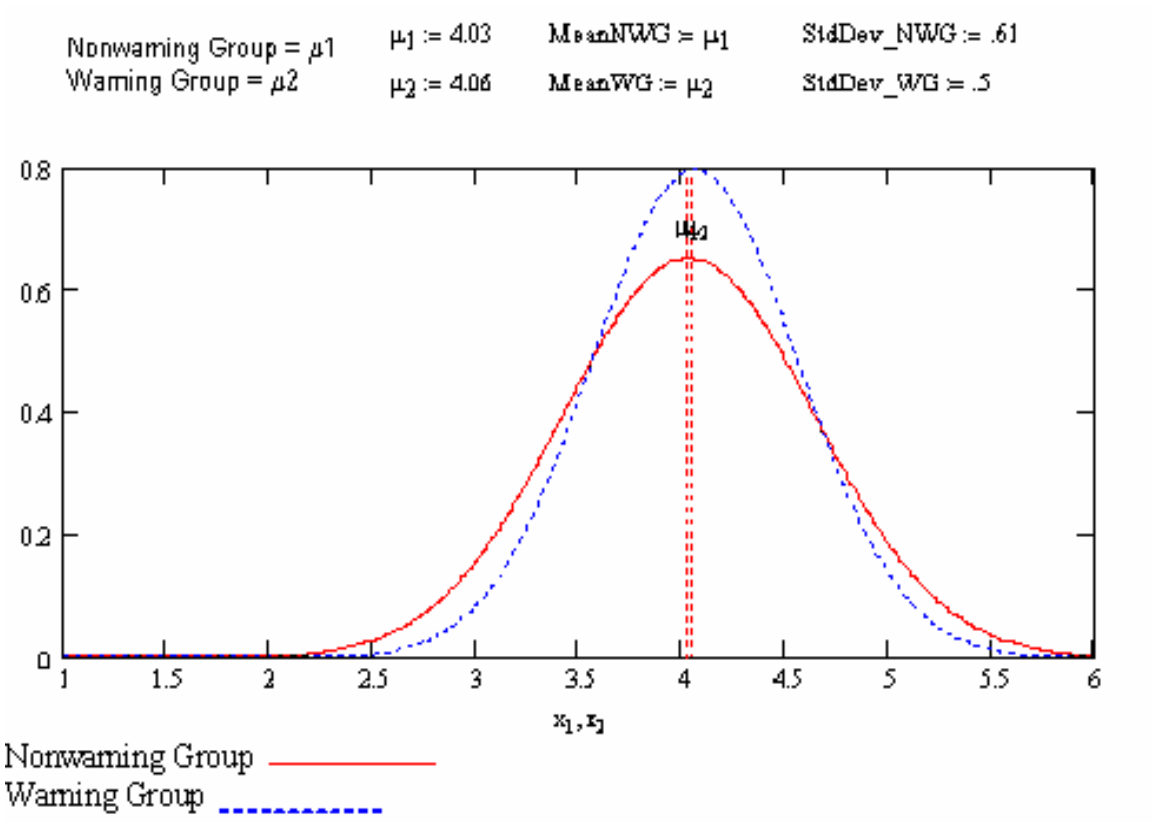

Figure 3: Distribution Plot for System Trust of Warning and Non-Warning Groups

Further analysis of the questionnaire also revealed that warnings do not appear to increase a participant's awareness level. This provides additional support to the finding

from the ANOVA that revealed hypothesis 2 was not supported. Awareness is not heightened from a previous level (i.e., a person's awareness is not increased). This can be seen in the comparisons of the distributions between the Warning Group and the Non-Warning Group (see Figure 4). The mean awareness for Warning Group was 4.35 and for the Non-Warning Group was 4.36. Standard deviation for the Warning Group was 0.43 and for the Non-Warning Group was .48. The plot reveals that each distribution is extremely similar, leading this research to conclude, that awareness does not increase if a warning suggesting manipulation is issued.

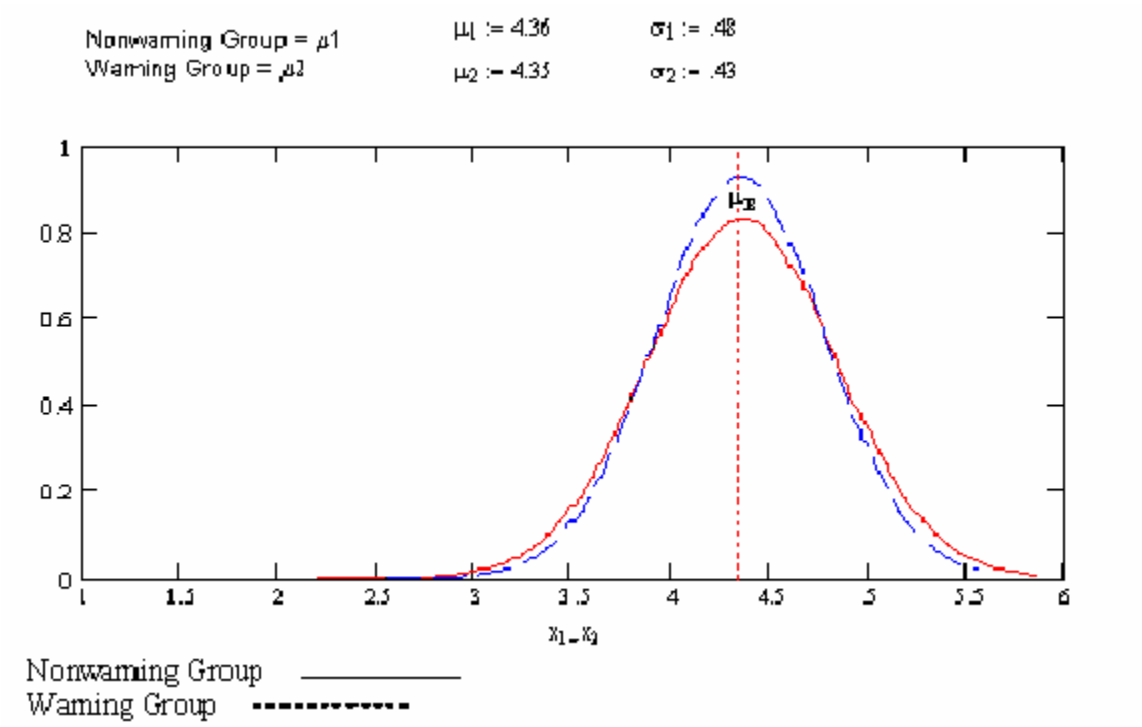

Figure 4: Distribution Plot for Awareness of Warning and Non-Warning Groups

Experiment Analysis

Two separate experiments were conducted. Experiment 1 consisted of 80 participants while Experiment 2 consisted of 72 participants. The experiments were designed to show whether warnings had any affect on a participant's ability to detect email forgery. Thirty-three out of 80 participants responded to the email forgery in Experiment 1 for a 41% response rate. Thirty-two out of 72 participants responded to the email forgery in Experiment 2 for a 44% response rate. Both experiments concluded with an email asking the participants if they identified any counterfeit emails during the two-week experimental time period. Based on the participants' responses to this email in Experiment 1, 63 participants reported not identifying the email forgery when it occurred, 7 participants reported correctly identifying the email forgery when it occurred, and 10 participants did not respond to any of the emails. The responses from this final email for Experiment 2 were 53 participants reported not identifying the email forgery when it occurred, 8 participants reported correctly identifying the email forgery when it occurred, and 11 participants did not respond to any of the emails. Therefore, the 10 participants in Experiment 1 and the 11 participants in Experiment 2 were not used in the final analysis of this experiment. The analysis of the experiments can be seen in Table 11 for Experiment 1 and Table 12 for Experiment 2. The two experiments revealed that warnings do not have a positive effect on a participant's ability to detect deception. This finding does not support hypothesis 1 (i.e., warnings about possible deception in electronic identity theft will be positively associated with detection success).

Table 11: Experiment 1 Results

Experiment 1		
Actual Responses to Email Forgery		After Experiment Analysis
15 Responses From Non-Warning Groups		63 - Did Not Identify Email Forgery
18 Responses From Warning Groups		7 - Identified Email Forgery Correctly
		10 - Stopped Responding to All Emails
41% Response Rate to Email Forgery		90% Failure to Identify Email Forgery

Table 12: Experiment 2 Results

Experiment 2		
Actual Responses to Email Forgery		After Experiment Analysis
17 Responses From Non-Warning Groups		52 - Did Not Identify Email Forgery
15 Responses From Warning Groups		8 - Identified Email Forgery Correctly
		12 - Stopped Responding to All Emails
44% Response Rate to Email Forgery		87% Failure to Identify Email Forgery

In order to determine if participants in the warning groups were able to identify the email forgery earlier or later during the experiments the warning groups were split into three groups for Experiment 1 and two groups for Experiment 2. It was thought that the warning groups who received the email forgery earlier would be able to identify the email forgery more accurately then those groups who received the email forgery at later times. This did not occur. The warning groups who received the email forgery at time 2 and were deceived were comparable to those warning groups who received the email forgery at later times. The results revealed that the interval between the warning email and the email forgery had no effect. The results can be seen in Tables 13 and 14.

Table 13: Experiment 1 Responses to Forged Email Address

	WG1	WG2	WG3
Time 1			
Time 2	**7 Deceived**		
Time 3			
Time 4		**1 Deceived**	
Time 5			**10 Deceived**

*NWG = Non warning Group
**WG = Warning Group

Table 14: Experiment 1 Responses to Forged Email Address

	WG1	WG2
Time 1		
Time 2	**10 Deceived**	
Time 3		**5 Deceived**

*NWG = Non warning Group
**WG = Warning Group

Analysis of Variance for Deceived and Not Deceived Participants

One-way ANOVAs were conducted to determine if there was a significant difference in the system trust and awareness of those participants who were deceived and those who were not deceived. The deceived participants were coded with a 0 and the participants not deceived were coded with a 1. This is the independent variable of this study. The result of the ANOVA comparing the means for the system trust revealed an F-statistic 0.569, which showed that the difference was insignificant ($p>.05$) (SPSS, 1999). The F-statistic result for awareness was 5.4, which showed a significant difference ($p<.05$) (SPSS, 1999). Therefore, the results for system trust do not support hypothesis 4b (i.e., System trust will be negatively associated with deception detection). However, the results for awareness do support hypothesis 5 (i.e., Awareness about possible electronic identity theft will be positively associated with deception detection). Table 15 presents the results for the ANOVA.

Table 15: ANOVA for Deceived and Not Deceived Participants

	Deceived		Not Deceived				
Variable	*M*	*SD*	*M*	*SD*	*df*	*F*	*p*
System Trust	3.99	0.55	3.88	0.67	1,151	0.569	0.452
Awareness	4.2	0.56	4.55	0.35	1,151	5.4	0.021
N=152							

Summary

This chapter presented the analysis of the data collected. In this chapter the questionnaire and the experiment were examined individually and then compared with the each other. For example, the results from the questionnaire were examined individually and than cross-analyzed with the results from the experiment. Chapter V presents the research findings, conclusions, and recommendations for future research efforts.

V. Findings and Recommendations

Research Findings and Implications

The results of this research contain important implications for the U.S. Military and other governmental agencies that depend on email for disseminating information. The overarching question for this research was threefold: 1) to determine if email forgery is a significant vulnerability in U.S. Air Force and DoD email systems, 2) to determine what affect warnings have on human system trust, human awareness, and an individual's ability to detect deception, and 3) to research the relationship between human system trust and human awareness in information systems. This research effort supports the finding that U.S. Air Force personnel at the Air Force Institute of Technology appear to be extremely vulnerable to email forgery manipulation. This finding is based on the results of two experiments performed at two separate times with different personnel. The two experiments revealed that 90% (137 out of 152) of the participants failed to identify the email forgery when it occurred and 42% (65 out of 152) actually responded to the email forgery. Therefore, this research supports the finding that email forgery is a significant vulnerability U.S. Military organizations need to be aware of.

Biros et al. (2002) found in their deception detection research that the issuance of a warning prior to the deception increased detection performance in those individuals. This research attempted to confirm that finding. On the contrary, the finding of this research was exactly the opposite. The findings from this research revealed that warnings do not increase a participant's ability to correctly identify email forgeries. Therefore, this finding does not support hypothesis 1. This finding along with the finding of Biros et al.

(2002) does demonstrate that warnings affect people differently. The findings lead this research to theorize about what types of warnings are sufficient enough to increase suspicion to an acceptable level. Therefore, a recommendation for future research is to examine at what level warnings increase suspicion in order to demonstrate behaviors in trust and awareness or other behaviors which affect an individual's ability to detect deception.

Past research (Stiff et al., 1992; Miller and Stiff, 1993; Parasuraman, 1984; Biros et al., 2002) found that if an individual's suspicion is aroused, their ability to detect deception increases. The findings from this research suggest that awareness did not increase in those individuals who were issued a warning. Therefore the finding from this research does not support hypothesis 2. This finding could mean that the instrument used to measure awareness did not effectively measure this behavior, but the statistical analysis of the instrument does not support this. The finding could mean that the warning issued did not increase suspicion to an acceptable level to cause an increase in an individual's awareness. I feel the findings of this research, along with the findings of previous research on warnings (Biros et al. 2002), support the second meaning (i.e., the warning issued did not increase suspicion to an acceptable level to cause an increase in awareness). Both of these results suggest future research to confirm the effectiveness of the instrument used to measure awareness and to determine the effectiveness of warnings used in computer system alerts.

Stiff et al. (1992) suggests that in relationships with well-developed truth biases, warnings from a third party will decrease the receiver's level of trust in the relationship. Information from a third party may be sufficient to provoke suspicion and affect truth

bias judgments. Therefore, it was thought that warnings would decrease an individual's level of trust in a specific system. This research supports the generalization that system trust, in well established systems, does not decrease, when a warning suggesting possible manipulation of the system is issued. This supports what Daly (2002) found. System trust is developed and strengthened over time and it is difficult to reduce system trust levels in relationships (human-computer) with well established truth biases. Therefore, this finding does not support hypothesis 3. This could be a result of the warning issued. It is possible the warning was too generic or not assertive enough to increase suspicion to an acceptable level which would not have caused a decrease in the individual's system trust. Future research should experiment with the use of several variations of warnings to determine how warnings affect individuals differently.

It was thought that if a participant's level of system trust is high, (i.e., they have a high level of trust in the system to identify the deceptive messages,) then he or she will be less likely to identify deceptive messages themselves. In regards to awareness, it is thought that if the participant's awareness is high, then the participant will be more likely to identify deceptive messages because he or she will be more alert. The finding from this research did not support the idea that system trust and awareness are inversely correlated. In addition, it was determined by this research that no relationship exists between system trust and awareness. Therefore, hypothesis 4a was not supported. This could have to do with the possibility that the warning was not specific enough to have generated enough suspicion to induce an increase in awareness and a decrease in system trust. The other possibility is that the questionnaire did not properly measure the desired behaviors of system trust and awareness.

The comparison analysis of the questionnaire and the experiment of those who were deceived and not deceived revealed that hypothesis 4b was not supported. The results revealed that the system trust in those individuals who received a warning and those who did not was very similar. Therefore leading this research to conclude that system trust was not negatively associated with deception detected. This again, as mentioned previously, could have to do with the warning that was issued or the effectiveness of the questionnaire in measuring the desired constructs.

The comparison analysis of the questionnaire and the experiment revealed that hypothesis 5 was supported. The finding for hypothesis 5 revealed that the awareness of those who identified the email forgery was higher than those who did not identify the email forgery. The breakdown of the 15 individuals who identified the email forgery was nine individuals from the Warning Group and six from the Non-Warning Group. The analysis of the data revealed no reasons as to why their awareness was higher, only that it was higher. There were no demographic correlations which revealed why these individuals had a heightened sense of awareness. There were no correlations to the warning that was issued based on the fact that six from the Non-Warning Group discovered the email forgery. A correlation was found between eight of the 15 individuals. This correlation revealed that these eight individuals at some time in the past had been a victim of some type of information system attack. Therefore, their awareness was in a constant-heightened state because of a past experience. This finding does support the use of the Air Forces computer security awareness training which could have also been a reason why these individuals awareness was heightened. A complete summary of the findings can be seen in Table 16.

Table 16: Summary of Findings

H1	Warnings about possible deception in electronic identity theft will be positively associated with detection success.	Not Supported
H2	Warnings about possible electronic identity theft will be positively associated with an individual's awareness.	Not Supported
H3	Warnings about possible electronic identity theft will be negatively associated with system trust.	Not Supported
H4a	System trust will be negatively associated with awareness.	Not Supported
H4b	System trust will be negatively associated with deception detection.	Not Supported
H5	Awareness about possible electronic identity theft will be positively associated with deception detected.	Supported

Limitations

The participants for the two experiments were active duty U.S. military personnel at the Air Force Institute of Technology. Future research efforts need to be expanded to other random units across the U.S. Air Force, U.S. Military, and other DoD organizations to determine if other email systems are vulnerable to the threat of email forgery. These research efforts should include a higher ratio of officer/enlisted personnel to determine if there is a significant difference between these groups' ability to detect email forgeries.

The participants were required to sign a consent form which posed another limitation for this research. The consent form mentioned the possibility of an email manipulation. This statement in the consent form could have raised the awareness levels of the participants beyond an acceptable level for this study. This could have been a

reason for the heightened level of awareness in the participants who detected the email forgery. A heightened level of awareness due to the consent form was not a desired result for this study. The study may have been more beneficial and may have provided better results had the participants' not had to provide a consent form. This would have allowed for use of the original research design of one email versus the five-email package developed for Experiment 1 and the three-email package developed for Experiment 2. The original protocol designed for this study was to send out one email forgery and no legitimate emails to the entire AFIT student body and then evaluate whether a participant was deceived by measuring the number of responses to the email forgery account. This would have provided a more natural setting for this experiment therefore, possibly providing better overall results. The Air Force Research Laboratories Human Subject Review board denied this protocol because the Air Force does not allow manipulation protocols without the participants' consent. The one-email protocol may have provided a more accurate measure of participants' ability to detect this form of email manipulation. The amount of time between the administration of the consent form and the email manipulation was another limitation of this research. Future studies should lengthen this time; the results may improve.

A limitation on the application of the questionnaire during Experiment 1 was it should have been sent to the Warning group after the warning email. This would have provided a better statistical evaluation between the Warning Group and the Non-Warning Group in an ANOVA. However, this was accomplished in Experiment 2 and results between the two experiments appeared to be relatively the same. This again suggests that the warning issued may not have increased suspicion to an acceptable level or could

suggest that the questionnaire used may not have appropriately measured the desired constructs. It was thought that the Warning Group's system trust would be lower and their awareness would be higher than the Non-Warning group. This was not supported by the responses from the questionnaire items. This suggests that future research is needed to determine at what level warnings increase suspicion to an acceptable state, which would induce a change in an individual's system trust and awareness. It also appears from the results that several of the items used to measure awareness did not provide strong indicators for this behavior. The overall findings from the questionnaire may suggest that better indicators for awareness need to be developed to effectively evaluate a system trust and awareness relationship. Because no other instruments existed at the time of this study, it was determined to be the best instrument available.

A final limitation was the use of very benign questions in the email messages. The email questions did not ask the participants any personal information. This research was concerned with whether people paid attention to the actual email address they respond to and not how they would respond to personal-type questions. Future studies should experiment with the use of more personal type questions to determine if the types of questions asked could be used as deceptive cues.

Recommendations for Future Research

The findings from this study are encouraging enough to continue this line of research. The findings from the questionnaire led this researcher to recommend that a new instrument be developed to study the behavior between system trust and awareness in information systems. Additional studies are needed to determine if other systems are

vulnerable to an email forgery information attack. Additional studies are needed to study what type of relationship warnings (i.e., about possible deception) has on an individual's ability to detect deception. These studies could determine how different types of warnings (i.e., verbal or text) relate to participant's ability to detect deception. These studies could look at the delivery or presentation of the message. For example, in text-based warning messages, future research could examine how people respond to bold colored text messages vs. an ordinary black text message to determine which of these messages increase suspicion more effectively. Additional studies are also needed to determine if people deceived by an email forgery show improvement in identifying these forms of deceptive messages during future manipulations. This would determine if individuals learn from their past experiences and are better at detecting this form of manipulation. Future studies could be used to determine how the nature of the questions asked (i.e., personal questions vs. generic questions) in email forgeries affect a person's ability to detect email manipulation. Finally, a longitudinal study is recommended to determine what affects email forgery has on a person over prolonged periods of time.

Another possible area of research would be to determine how training affects identity theft in email forgery. This training could be done in several ways. It could be added to the annual computer security training (COMPUSEC) U.S. Air Force personnel receive or it could be a separate computer security training package. This opens up two future research issues to be explored. The first research issue would be to see how individuals with annual COMPUSEC training, which includes training on identity theft and email forgery, perform in a similar scenario as used by this experiment. The second research issue would be to determine how a separate training format devised solely to

train individuals on identity theft and email forgery performs in a similar scenario as used by this research. These areas of training should be explored as a possible way of raising email users' awareness to the possibility of email forgery.

A final future area of study would be to determine how effective the Common Access Card's (i.e., Smart Card or CAC) authentication capability is. In this study, individuals with authentication capability could be measured against those without authentication capability. This would determine whether the authentication capability of the CAC is a solution to the email forgery vulnerability.

Summary

The information age has provided an array of exciting opportunities in technology and communication. This new computer technology has produced advancement in the areas of communication, increased productivity, increased efficiency and increased information processing. However, these benefits are not without their negative impacts, such as the number of viruses spreading across the World Wide Web and email systems (Denning, 1999). The increase in frauds and crimes are in direct connection to these technological advances (Robb, 2002). Email is one of those technological advances in communication. We have seen email communication grow from less than 100 million mailboxes before 1996 to over 800 million mailboxes in 2001 (Fontana, 2001). Email communication will only continue to grow, and with that growth, new vulnerabilities and threats to email and its users will grow as well. The U.S. Air Force, U.S. Military and DoD rely heavily on email. U.S. Air Force commanders send orders for their troops to carry out through email. U.S. Air Force instructors use email as a primary means of

communication to issue assignments or inform students of class and course changes. This research looked at a new vulnerability to email systems and showed how easy it can be to deceive and manipulate individuals with only a small amount of information about them. The U.S. Air Force and DoD must not become complacent and allow these vulnerabilities to jeopardize our information superiority over our foes. The U.S. must stay on the cutting edge of technology, but must also remember that with this technology, come new vulnerabilities our enemies are more than willing and ready to exploit. This research identifies one of those new vulnerabilities. Research efforts like this one, which are designed to seek out new vulnerabilities to our information systems, need to be continued. The U.S. cannot allow new types of vulnerabilities to go undefended or unprotected in the future. The use of authentication will reduce the threat of email forgery. However, people have to be taught to authenticate the email address of the sender or email forgery will continue to be a vulnerability our enemies will exploit. Leaders and military organizations need to be aware of what their computer vulnerabilities are. This research provides empirical evidence that military users are susceptible to email manipulation.

Appendix A: Human Subjects Review Board Application

1. Title: Information Manipulation in Electronic Means of Communication
F-WR-2002-0038-H

2. Principal Investigator: Capt Roy V. Rockwell, AFIT/ENV GIR03M, 371-8184, roy.rockwell@afit.edu

3. AFIT Thesis Advisor: Lt. Col David P. Biros, AF-CIO, DSN: 329-3555 Comm: (703) 601-3555, david.biros@pentagon.af.mil

4. Medical Monitor: N/A

5. Contractor and/or Facility: N/A

6. Objective: This research will add to the body of knowledge in the computer systems information assurance research field. It will study the correlations between email system trust and levels of awareness. It will determine if identity theft through email forgery is a significant vulnerability the Air Force should be aware of.

a. **Hypothesis**:

H1: Warnings about possible electronic identity theft will be positively associated with decreased levels of trust.
H2: Warnings about possible electronic identity theft will be positively associated with increased levels of awareness.
H3a: Decreased levels of trust will be positively associated with increased levels of awareness.
H3b: Increased levels of trust will be positively associated with information manipulation not detected.
H4: Awareness about possible electronic identity theft will be positively associated with information manipulation detected.

b. Given that identity theft and email forgery is a growing concern in electronic computer communication, research in this area is needed by the Air Force to determine the magnitude of this potential computer vulnerability.

7. Impact: It will determine if email forgery is a viable threat to government email systems and if Air Force personnel are susceptible to this type of vulnerability.

8. Experimental Plan:

This experiment will measure levels of system trust and awareness of the AFIT/EN student body using email forgery. The experiment will last a total of 5 weeks. The proposed experiment will consist of several stages:

a. Stage 1 will consist of email sent to the AFIT/EN student body asking 80 students to voluntarily participate in a study regarding information manipulation in electronic means of communication. I will ask them to reply to the email if they wish to participate. Once 80 participants agree, I will set up a designated time for them to meet with me, review, and sign the informed consent form.
b. Stage 2 will begin once all 80 participants have signed their informed consent forms. This stage will consist of a survey sent out to the participants, which will measure levels of system trust and awareness levels to deception. It will also measure computer security and email experience. This survey will be done via email from the AFIT Network Operations and Security Center.
c. Stage 3 will consist of splitting the responses at random into two groups. Group 1 will not receive any type of warning regarding identity theft or possible computer system vulnerabilities. Group 2 will receive a warning email from the AFIT Network Operations and Security Center regarding possible computer system vulnerabilities, which involves identity theft and email forgery.
d. Stage 4 will take place approximately one week after Group 2 receives the warning email. This will consist of five emails from the AFIT Network Operations and Security Center and one email forgery from what appears to be the AFIT Network Operations and Security Center, sent to both Groups 1 and 2. This email forgery will be from a commercial source such as yahoo, hotmail, att.net or some other commercial resource and disguised to look as if it originated from the AFIT Network Operations and Security Center. The email forgery will consist of a question, which requires a response. The question used for the email forgery will ask the participants to vote yes or no if they think AFIT should incorporate a wireless Local Area Network when building 640 is renovated. This would allow students to connect their personal or government issued laptops to the AFIT network at anytime within the AFIT campus.
e. Stage 6 will be five to ten days after all data has been collected. This email will originate from the AFIT Network Operations and Security Center and will be a post-survey, which will measure system trust and awareness levels to be compared and correlated with the first survey taken. This post survey will ask the same questions used in the pre-survey with the addition of several questions to determine if the participants were able to successfully tell which email was a forgery.

9. Medical Risk Analysis: There are minimal risks to student participants. Participants who receive these emails from the AFIT Network Operations and Security Center may feel anxiety from the increased number of emails they receive. The participants may feel embarrassed by failing to identify the email forgery. One possible benefit to the participants would be an increased awareness of this type of vulnerability and way to identify other possible email forgeries in the future.

INFORMED CONSENT DOCUMENT
Information Manipulation in Electronic Means of Communication

1. **Purpose of Study**

This research is being conducted by Roy V. Rockwell, Captain, USAF, and a graduate student in Information Resource Management at the Air Force Institute of Technology (AFIT). Lt Col David P. Biros is overseeing this research for the Air Force Office of Scientific Research. I understand the purpose of the research project is to better understand information manipulation in electronic means of communication. I understand that if I participate in the project, I may be asked questions about my levels of trust and awareness placed in government computer systems. There will be approximately 80 Subjects.

2. **Procedures**

a. This experiment will measure levels of system trust and awareness of subjects using an email system. The experiment will last a total of 5 weeks. The experiment will consist of six to nine stages, each of which is an email form requesting information. Some messages may originate from outside military channels and should be handled according to applicable regulations. I will also take two surveys, consisting of 15-20 questions. At the conclusion of the research, I will be debriefed on the results of the experiment by the investigator.

3. **Risks and Inconveniences**

a. There are no known risks to me. All my answers to the survey questions will be kept confidential and identified by a subject code number. My name will not appear on any of the results. I understand there will be no retribution of any form from the Air Force, AFIT, or any other agencies involved in this study concerning the responses made by the participants. No individual responses will be reported. Only aggregate findings will be reported.

4. **Benefits**

a. There is no direct benefit to me for participation in this research.

b. I understand that the Air Force may gain valuable information on the vulnerabilities of government computer systems.

5. **Alternatives**

Choosing not to participate is an alternative to participating in this study.

6. **Entitlements and Confidentiality**

I understand that this consent may be withdrawn at any time without prejudice, penalty or loss of benefits to which I am otherwise entitled. The decision to participate in this research is completely voluntary on my part. No one has coerced or intimidated me into participating in this program. I am participating because I want to. Capt. Roy V. Rockwell, (AFIT, School of Engineering and Management, Phone: (937) 255-3636 ext 6459, Email: roy.rockwell@afit.edu, Cell Phone: 937-371-8184) has adequately answered any and all questions I have about this study, my participation, and the procedures involved. Capt Rockwell will be available to answer questions during the study.

_____

(Investigator)

_____

(Subject)

_____

(Witness)

Privacy Act Statement

Authority: We are requesting disclosure of personal information, to include your Social Security Number. Researchers are authorized to collect personal information (including social security numbers) on research subjects under The Privacy Act-5 USC 552a, 10 USC 55, 10 USC 8013, 32 CFR Part 219, 45 CFR Part 46, and EO 9397, November 1943 (SSN).

Purpose: It is possible that latent risks or injuries inherent in this experiment will not be discovered until some time in the future. The purpose of collecting this information is to aid researchers in locating you at a future date if further disclosures are appropriate.

Routine Uses: Information (including name and SSN) may be furnished to Federal, State and local agencies for any uses published by the Air Force in the Federal Register, 52 FR 16431, to include, furtherance of the research involved with this study and to provide medical care.

Disclosure: Disclosure of the requested information is voluntary. No adverse action whatsoever will be taken against you, and no privilege will be denied you based on the fact you do not disclose this information. However, your participation in this study may be impacted by a refusal to provide this information.

Appendix B: Warning Email

Subject
Stay alert for fraudulent email messages.

Message
During the past several weeks the AFIT Network Operations and Security Center has seen an increase in the attempt to gather information on military individuals. The process has been to disguise the email address so that it looks like it has come from a legitimate source when it is really coming from some fraudulent source. AFIT students need to be aware of this type of fraudulent activity and be alert to these types of threats. These attempts for information cannot be filtered out by the Network Operations and Security Center until they are brought to our attention, by someone such as you. So please be alert!!!

An example of one such attempt was sent to you by Capt. Lacey several weeks ago. It is attached below.

```
Attention All:

The following message appears to be an attempt to gather HUMINT from
unsuspecting users.  Two things make this message suspicious, the TO
field is not visible and the FROM address is a yahoo.com address... not
one a business like SAIC should be using.

DO NOT respond to this e-mail.  We have no confirmation that it is a
hoax, but be safe.

Be vigilant!

Maj(s) Tim Lacey
Deputy Director
AFIT/SCB

-----Original Message-----
From: SAIC_Korea@yahoo.com
Sent: 7/16/2002 10:19 AM
Subject: Cleared Opportunities in South Korea with SAIC

Cleared Opportunities in South Korea with SAIC

Company: SAIC
Website: www.saic.com
Overview: A diversified high-technology research and engineering
company based in San Diego, California, Science Applications
International Corporation (SAIC) offers a broad range of
expertise in technology development and analysis, computer system
development and integration, technical support services, and
computer hardware and software products. SAIC engineers and
scientists work to solve complex technical problems in national
security, homeland defense, energy, the environment,
telecommunications, health care and transportation.
```

FOR ALL POSITIONS:

-------This Message Ends for space savings----------

Tim Fox

AFIT/SCBY
Chief, Support Branch
Information Systems Division
Communications and Information Directorate
Air Force Institute of Technology
(937-255-6565 x4265)
(DSN 785-6565 x4265)
Tim.Fox@afit.edu

Appendix C: In-Text Message Manipulation for Experiment 2

Signature block used in legitimate email messages:

Tim Fox

AFIT/SCBY
Chief, Support Branch
Information Systems Division
Communications and Information Directorate
Air Force Institute of Technology
(937-255-6565 x4265)
(DSN 785-6565 x4265)
Tim.Fox@afit.edu

Signature block used manipulation in email forgeries:

Tim Fox
AFIT Network Operations and Security Center
Chief, Support Branch
Information Systems Division

Bibliography

Air Force Information Warfare Center. Common Intrusion Detection Director System Installation, Administration, and User's Guide. April 2000a. FOUO

Air Force Information Warfare Center. Automated Security Incident Measurement Tools: Sensor System Installation, Administration, and User's Guide. April 2000b. FOUO.

Arnold, Tom. "Internet Identity Theft: A Tragedy for Victims," Software & Information Industry Association White Paper, June 2000.

Biros, David. The Effects of Truth Bias on Artifact-User Relationships: An Investigation of Factors for Improving Deception Detection in Artifact Produced Information. Dissertation. Florida State University at Tallahassee, 1998.

Biros, D.P., George, J.F., and Zmud, R.W. "Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study," MIS Quarterly, 26(2): 1-26, June 2002.

Bowers, J.W., Elliott, N.D., and Desmond, R.J. "Exploring Pragmatic Rules: Devious Messages," Human Communication Research, 3: 235-242, 1977.

Buller, David B., K.D. Strzyzewski, and J. Comstock. "Interpersonal Deception: I. Deceivers' Reactions to Receivers' Suspicions and Probing," Communication Mongraphs, 58: 1-24, 1991a.

Buller, David B., K.D. Strzyzewski, and F.G. Hunsaker. "Interpersonal Deception: II. The Inferiority of Conversational Participants as Deception Detectors," Communication Mongraphs, 58: 25-40, 1991b.

Buller, David B. and J. K. Burgoon. "Another Look at Information Management: A Rejoinder to McCornack, Levine, Morrison, and Lapinski," Communication Monographs, 63(1): 92-103, March 1996.

Buller, David B. and J. K. Burgoon. "Interpersonal Deception Theory," Communication Theory, 6(3): 203-242, August 1996.

Burgoon, Judee K. and David B. Buller. "Interpersonal Deception III.: Effects of Deceit on Perceived Communication and Nonverbal Behavior Dynamics," Journal of Nonverbal Behavior, 18(2): 155-184, Summer 1994.

Burgoon, J.K., Buller, D.B., Eresu, A.S., and Rockwell, P. "Interpersonal Deception: Accuracy in Deception Detection," Communication Monographs, 51, 303-325, 1994.

Burgoon, J.K., Buller, D.B., and Guerrero, L.K. "Interpersonal Deception: Effects of Social Skills and Nonverbal Communication on Deception Success and Detection Accuracy," Journal of Language and Social Psychology, 14(3): 289-311, 1995.

Burgoon, J.K., Buller, D.B., and Guerrero, L.K., Afifi, W.A., and Feldman, C.A. "Interpersonal Deception XII.: Information Management Dimensions Underlying Deceptive and Truthful Messages," Communication Monographs, 63: 50-69, March 1996.

Daly, Mark A. Task Load and Automation Use in an Uncertain Environment. MS Thesis, AFIT/GAQ/ENV/02M-05. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2002.

Denning, Dorothy E. Information Warfare and Security. Reading, MA: Addison Wesley Longman, Inc. 1999.

Department of the Air Force. Information Operations. AFDD 2-5. Washington: HQ USAF, 22 January 2002.

DePaulo, B. M., K. Lanier, and T. Davis. "Detecting Deceit of the Motivated Liar," Journal of Personality and Social Psychology, 45: 1096-1103, 1983.

DePaulo, B. M., J.I. Stone, and G.D. Lassiter. "Deceiving and Detecting Deceit," in The Self and Social Life. Ed. B.R. Schlenker. New York: McGraw Hill, 1985.

deTurck, M.A., J.J. Harszlak, R.J. Bodhorn, and L.A. Texter. "The Effects of Training Social Perceivers to Detect Deception From Behavioral Cues," Communication Quarterly, 38: 189-199, 1990.

Dillon, A. and M.G. Morris. "User Acceptance of Information Technology: Theories and Models" in Annual Review of Information Science and Technology (ARIST). Ed. Williams, Martha E. Medford NJ: Information Today, 31: 3-32, 1996.

Egan, J.P., Greenburg, G.Z., and Schulman, A.I. Interval of Time Uncertainty in auditory detection. Journal of the Acoustical Society of America, 33: 771-778, 1961.

Ekman, Paul. Telling Lies. New York, NY: W.W. Norton & Company, 1985.

Ekman, Paul. Why kids lie: How parents can encourage truthfulness. New York: Charles Scribner's Sons, 1989.

Federal Trade Commission (FTC-1). "ID Theft: When Bad Things Happen to Your Good Name." Article. http://www.ftc.gov. 18 January 2002.

Federal Trade Commission (FTC-2). "Identity Theft: If You're a Victim." Article. http://www.consumer.gov/idtheft/victim.htm. 12 February 2002.

Fields, Gregory S. The Effect of External Safeguards on Human-Information System Trust in an Information Warfare Environment. MS Thesis, AFIT/ENV/GIR/01M-07. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2001.

Fontana, J. "Email Continues Explosive Growth," Network World Fusion. www.nwfusion.com/news/2001/0308email.htm March 2001.

Frank, M. Identity theft Prevention and Survival. www.identitytheft.org/index.htm. 1998.

Grice, Paul H. "Logic and Conversation," in Syntax and Semantics: Speech Acts. Eds. P. Cole and J.L. Morgan. Academic Press, 1975.

Gouldner, A.W. "The Norm of Reciprocity: A Preliminary Statement," American Sociological Review, 25: 161-178, 1960.

Greenburg, M.S. "A Theory of Indebtedness," in Social Exchange: Advances in Theory and Research. Eds. K. Gergan, M. Greenberg, and R. Willis. New York: Plenum, pp. 3-26, 1980.

Goldburg, Ivan. "Information Warfare," Institute for the Advanced Study of Information Warfare. www.psycom.net/iwar.1.html 1996.

Gunsch, Gregg H. Class Lecture, CSCE 625, Information Systems Security Assurance and Analysis I. School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB OH, April 2002.

Hair, J.F. Multivariate Data Analysis. NJ: Prentice Hall. 1995.

Jacobs, S; Dawson, E.J.; and Brashers, D. "Information Manipulation Theory: A Replication and Assessment," Communication Monographs, 63(1), 70-82, 1996.

Jian, J., Bisantz A., and Drury C. "Foundations for an empirically determined scale of trusting automated systems." International Journal of Cognitive Ergonomics, 4(1): 53-71, 2000.

Johnson, P.E; Grazioli, S.; and Jamal, K. "Fraud Detection: Intentionality and Deception in Cognition," Accouting, Organizations, and Society, 18(5), 467-488, 1993.

Kachigan, S.K. Multivariate Statistical Analysis. New York: Radius Press, 1991.

Kellermann, K. "The Negativity Effect and Its Implications for Intial Interaction,"` Communication Monographs, 51: 37-55, 1984.

Klein, B.D., Goodhue, D.L., and Davis, G.B. "Can Humans Detect Error in Data? Impact of Base Rates, Incentives, and Goals," MIS Quarterly, 21(2): 169-194, June 1997.

Klein, B.D., Goodhue, D.L., and Davis, G.B. "Conditions for the Detection of Data Errors in Organizational Settings: Preliminary Results from a Field Study." Unpublished manuscript, 1997.

Klein, B.D. "Perceptions of Information Quality: A Study of Internet and Traditional Text Sources," Proceedings of the Fifth Americas Conference on Information Systems, 99: 618-620, August 1999.

Laudon, K.C. "Data Quality and Due Process in Large Interorganizational Systems," Communications of the ACM, 29(1), 4-11, 1986.

Lee, J.D. Trust, Self Confidence, and Operators' Adaptation to Automation. Dissertation. University of Illinois at Urbana-Champaign, 1992.

Lee, J.D. and Moray, N. Trust and the Allocation of Function in Human-Machine Systems. Ergonomics, 35: 1243-1270.

Levine, T.R. and McCornack, S.A. "Linking Love and Lies: A Formal Test of the McCornack and Parks Model of Deception Detection," *Journal of Social and* Personal Relationships, 9, 143-154,1 1992.

McCornack, S.A. and Parks, M.R. "Deception Detection and Relationship Development: The Other Side of Trust". In Mclaughlin (ed.), Communications Yearbook 9, Beverly Hills CA: Sage, 1986.

McCornack, Stephen A. "Information Manipulation Theory," Communication Monographs, 59: 1-15 March 1992.

McCornack, S.A., Levine, T.R., Solowczuk, K.A., Torres, H.I., and Campbell, D.M. "When the Alteration of Information is Viewed as Deception: An Empirical Test of Information Manipulation Theory," Communication Monographs, 59: March 1992.

McCornack, S.A., Levine, T.R., Morrison, K., and Lapinski, M. "Speaking of Information Manipulation: A Critical Rejoinder," Communication Monographs, 63(1): 83-91, March 1996.

Metts, S. "An exploratory investigation of deception in close relationships," Journal of Social and Personal Relationships, 6: 159-179, 1989.

Millar, Murray G. and Karen U. Millar. "The Effects of Cognitive Capacity and Suspicion on Truth Bias," Communication Research 24(5): 556-570, October 1997.

Miller, Gerald R. and James B. Stiff. Deceptive Communication. Newberry Park, CA: Sage Publications, 1993.

Miriam-Webster's Collegiate Dictionary. Springfield, MA: Miriam-Webster Inc. www.m-w.com. 2002.

Moore, Gordon. "Moore's Law," Web article. Webopedia, http://www.webopedia.com/TERM/M/Moores_Law.html, 8 May 2002.

Moray, Neville, Douglas Hiskes, John Lee, and Bonnie Muir. "Trust and Human Intervention in Automated Systems," in Expertise and Technology: Cognition and Human-Computer Cooperation. Eds. Jean-Michel Hoc and Pietro Carlo Cacciabue. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc., 1995.

Moray R. C. "Estimating and Improving the Quality of Information in a MIS," Communications of the ACM. 25: 337-342, 1982.

Mosier, Kathleen L., Linda J. Skitka, and M. D. Burdick, "Accountability and Automation Bias," International Journal of Human-Computer Studies, 52(4): 701, 2000.

Mosier, Kathleen L, Linda J. Skitka, and Susan T. Heers, "Automation and Acountability for Performance," Ames Research Center and NASA Human Factors Research and Technology Division, human-factors.arc.nasa.gov/Ihpublications/mosier/OSU95/OSU_Mosier.html. 21 July 2000.

Muir, Bonnie M. "Trust Between Humans and Machines, and the Design of Decision Aids," International Journal of Man-Machine Studies, 27: 527-539, 1987.

Muir, Bonnie M. "Trust in Automation: Part I. Theoretical Issues in the Study of Trust and Human Intervention in Automated Systems," Ergonomics, 37(11): 1905-1922, 1994.

Murray, S. A. and B. S. Caldwell. "Operator Alertness and Human-Machine System Performance During Supervisory Control Tasks," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah NJ:Lawrence Erlbaum Associates, 1999.

Nunally, J. Psychometric Theory. (2nd Edition.) New York: McGraw Hill Company, 1978.

O'Hair, Dan H. and Michael J. Cody, "Deception," in The Dark Side of Interpersonal Communication. Eds. William R. Cupach and Brian H. Spitzberg. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc., 1994.

Parasuraman, Raja. "Human-Computer Monitoring," Human Factors, 29(6): 695-706 December 1987.

Parasuraman, Raja. "Sustained Attention in Detection and Discrimination," in Varieties of Attention, Eds. R. Parasuraman and D. R. Davies. Academic Press Inc., London, pp 243-266, 1984.

Paul, Brooke. "Building an In-Depth Defense," Network Computing. http://www.networkcomputing.com/1214/1214ws1.html 2001

Quest Study Bible New International Version. Eds. Marshall Shelley, Richard Doebler, Paul Woods, and John Gundan. Zondervan Publishing House, Grand Rapids, MI, 1994.

Research Consortium (University of Arizona, Michigan State University, Florida State University and the Air Force Institute of Technology). "Detecting Deception in the Military Infosphere," Research Proposal to Air Force Office of Scientific Research. May 2001.

Redman, T. C. Data Quality: Management and Technology. New York: Bantam Books 1992.

Ricketts, J.A. "Powers-of-Ten Information Biases," MIS Quarterly, 14(1), 62-77, 1990.

Robb, Drew. "Protecting Sensitive Data Requires Vigilance," HR Magazine, 47(4), 91-96, April 2002.

Roloff, M.E. "Communication and Reciprocity Within Intimate Relationships," in Interpersonal Process: New Directions in Communication Research. Eds. M.E. Roloff and G.R. Miller. Newbury Park, CA: Sage. pp. 11-38, 1987.

Schmit, M.J., Ryan, A.M., Stierwalt, S.L., and Powell, A.B. "Frame-of-Reference Effects on Personality Scale Scores and Criterion-Related Validity." Journal of Applied Psychology 80(5): 607-620, 1995.

SPSS©base 10.0 applications guide [software manual]. Chicago, IL: SPSS, Inc. 1999.

Stiff, J.B., Kim, H.J. and Ramesh, C.N. "Truth Biases and Aroused Suspicion in Relational Deception," Communications Research, 19(3): 326-345 June 1992.

Sun Tzu 6th cent B.C. The Art of War / by Sun Tzu. Ed. Clavell, James. New York: Delecorte Press, 1983.

Turner, R., C. Edgley, and G. Olmstead, "Information control in conversations: Honesty is not always the best policy," Kansas Journal of Sociology, 11(1), 69-89, 1975.

Wickens, C. D. "Automation in Air Traffic Control: The Human Performance Issue," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah NJ: Lawrence Erlbaum Associates, 1999.

Wiener, E.L. "Application of Vigilance Research: Rare, Medium, or Well Done?," Human Factors, 29(6), 725-736, 1987.

Van Cleave, John. "Critical Factors in Cyberspace," Research paper submitted to the Department of Joint Military Operations, Naval War College, Newport, RI. February, 1997.

Venkatesh, Viswanath and Fred D. Davis. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," Management Science (46:2), pp. 186-204, February 2000.

Zuboff, Shoshana. In the Age of the Smart Machine: The Future of Work and Power. Oxford: Heinemann Professional, 1988

Zuckerman, M., R.E.Koestner, and A. Alton. "Learning to Detect Deception," Journal of Personality and Social Psychology. 46: 519-528. 1984.

Zmud, R.W. "Opportunities for Strategic Information Manipulation through New Information Technology," in Fulk & Steinfield (Eds.), Organizations and Communication Technology, Sage, 1990.

Vita

Captain Roy Rockwell graduated from Santa Fe High School in Alachua, Florida in June 1990. After two years attendance at Florida Baptist Theological College in Graceville, Florida Captain Rockwell enlisted in the U.S. Army as a Finance Specialist. After a 3 year assignment to Ft. Sill Oklahoma, he separated from the Army and enlisted in the Air Force Reserve Officer Training Corps at East Carolina University in Greenville, North Carolina. Capt Rockwell graduated from East Carolina University with a Bachelor of Science in Business Administration degree in Information Systems Management and was commissioned in the Air Force.

His first assignment was to Peterson AFB, Colorado where he was trained as a Communications/Computer Programmer Specialist. He served in this assignment for two years as Chief of the Intercontinental Ballistic Missile Systems Support Section. In 1999, he was assigned to Detachment 1, 533rd Training Support Squadron at Schriever, AFB, Colorado, where he served as the Chief of the Computer and Financial Support Branch. In August 2001, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to Headquarters, Air Force Reserve Command, Warner Robbins AFB, Georgia.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
25-03-2003	**Master's Thesis**	Aug 2001 – Mar 2003

4. TITLE AND SUBTITLE

DECEPTION DETECTION: STUDY OF INFORMATION MANIPULATION THROUGH ELECTRONIC IDENTITY THEFT – EMAIL FORGERY IN THE U.S. MILITARY

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Rockwell, Roy V., Captain, USAF

5d. PROJECT NUMBER
2002-093

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/03-16

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/PIF
Attn: Ms. Danielle Lindsey
801 N. Randolph St., Rm #732 DSN: 426-9562
Arlington, VA 22203-1977 e-mail: Danielle.Lindsey@afosr.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research describes the results of a field experiment which examines the effects of warnings on system trust and individual awareness in government computer systems through the use of email forgery. The experiment consisted of forging a trusted government email account and trying to get government computer users to reply to a forged email address. The results revealed that warning individuals about possible email forgery did not increase their awareness or reduce their level of system trust in the email system nor did it increase their ability to detect email forgery. The results did determine that government computer users are extremely vulnerable to email forgery and that new security measures need to be adapted to protect these systems from this type of threat.

The culmination of this effort was to support the use of email authentication through the use of the new common access card (i.e., smart card or CAC) by the military. Recommendations to implement effective email authentication and encryption capabilities.

15. SUBJECT TERMS

E-Mail, E-Mail Forgery, Encryption, Authentication, System Trust, User Awareness, Warnings, Electronic Identity Theft, Deception Detection, Information Manipulation,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David P Biros, Lt Col, USAF (ENV)
U	U	U	UU	106	19b. TELEPHONE NUMBER *(Include area code)* (703) 601-3555; e-mail: david.biros@pentagon.af.mil

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18