An Investigation into the Human/Computer Interface from a Security Perspective

by

Daniel J. Cross

A Proposal Submitted to the Honors Council

For Honors in Computer Science and Engineering

15 October, 2004

Approved By: _____

Luiz Felipe Perrone
Thesis Advisor

_____

Garry Haggard
Chair, Department of Computer Science

# 1 Introduction

It can be argued that users have long viewed computer security as necessary only for governments and major corporations. (Computer security, in the context of this thesis, will be defined as the hardware, software, and rules implemented to restrict access to a computer system.) However, the rapid increase in the number of information sensitive transactions has forced this idea to become antiquated. Social security numbers, credit card numbers, and confidential documents have crisscrossed the Internet by the billions over the past year. Many computer software companies have bore the brunt of the outcry for more security and have responded to it with varying results. While software engineering, encryption, authentication, and OS support have improved, little has been done to change how users interact with their systems. Computer users in various institutions ranging from corporations to small businesses do not have a complete understanding of the security software provided to them and the number of these uneducated users continues grow [9]. As a result, many users disregard, ignore, and even act against the very security measures that are built to protect them. The greatest threat to a network is its own users. Their inefficient use of security, with either malicious or benign intent, threatens and breaks down the company's defenses. An investigation needs to be conducted regarding the behavior of the user. Computer experts such as Ross Anderson, Bruce Schneier, and Kevin Mitnick have proclaimed that the user creates risk in various areas of computer security. These areas range from poor password selection to social engineering to the intentional bypassing of protection software. While these areas have been discussed individually, they have not yet been combined to produce a comprehensive risk analysis of user behavior. Such an analysis would cast light upon the

weaknesses introduced by the user and enable the creation of a systematic solution to them. In my thesis, I will provide steps towards the analysis of how user's behavior interacts with the system and propose a policy through which these faults are addressed.

# 2 Background

Computer security can be implemented using a vast number of hardware and software combinations. Unfortunately, users some unknowingly circumvent and defeat these protections, regardless of which combination is implemented. Bruce Schneier asks us to imagine where the hardware, software, and networks are all completely secure and then tells us that a user will have to interact with the system, "And this interaction is the biggest security risk of them all [2]." In other words, it is impossible to "user-proof" a computer system. One of the most common ways users compromise security systems is through a method called social engineering. In a social engineering attack, "the attacker will extract it [the confidential information] directly, from people who are authorized to access it, by telling some plausible untruth [1]." For example, an attacker may phone an employee of a company, insist that there is an imminent problem, and request a password that gives broad access to the system to remedy the situation. Most employees are not willing to take the blame for the problem in case it worsens and are thus willing to compromise the system and give out the password [3].

The user's refusal and perhaps inability to make intelligent security decisions creates risk. Security is best accomplished when the user accepts responsibility for it. Unfortunately, many see it as a burden and do not wish to see it all [2]. Users seldom read a warning when it appears on their computer and simply click on it. Some users try

to read it only to get frustrated, because they do not understand it. In nearly all cases, the user clicks “Ok,” “Cancel,” “Abort,” or anything else in an effort to get the window off the screen and continue with whatever they’re attempting to do. Bruce Schneier elaborates that most users will ignore windows that display warnings, click “OK” to get the warning off the screen, and will promptly forget that a warning ever appeared [2].

A user’s password selection can also compromise a system. Most users select a password easy to guess, write down the password, or do both [1]. Unfortunately, this problem is compounded by the fact that many people find it simply too difficult to memorize a bunch of different passwords for the ever-increasing number of applications in which we use them. As a result, many people reuse the same password in a variety of systems. This enables an attacker to access far more information than would have been possible if different passwords were used. As a result, a sort of domino effect occurs. When dominos are set-up within reach of one another, toppling the first domino causes the others to follow. Similarly, using the same password across various systems establishes a close connection between all of the systems, thus if one system is compromised, the others will be as well.

A computer user with malicious intent is one of the hardest security issues to prevent. Since users already possess passwords and can thus enter their own restricted access systems without arousing suspicion, they are some of the most dangerous attackers. “The person who writes a security program can put a back door in it. The person who installs a firewall can leave a secret opening. The person whose job it is to audit a security system can deliberately overlook a few things [2].”

# 3 Project Description and Methodology

This project will focus on identifying the human modes of failure and risk relative to computer security. This will be accomplished in two parts. A comprehensive investigation will be undertaken to find and understand the various ways users can circumvent computer security systems. There will be a focus on network users; however, considering the rampant popularity of online shopping, banking, and other activities that are requiring home users to send out an ever-increasing amount of personal information, many of the security problems discussed will apply to home users as well. This project will investigate instances of malicious and benign intent alike. Benign intent is defined as intentionally circumventing the system's security mechanisms without the intent to put the system at increased risk. A user with malicious intent is someone who deliberately compromises the system with the purpose of doing harm to the system, the users, or the institution. These initial findings will give an understanding of user behavior that will be explored in the second part to generate a plan that addresses the flaws in the human/computer interface. This plan will include how users can help themselves without putting the system at risk and how managers and system administrators can educate their users and minimize their chances to expose the system. Incorporated in this will be a discussion on the paradoxical co-existence of privacy and security and the role they play in developing institutional security policy. The plan developed in the second part will approach computer security by working to make the user's behavior more secure.

The concept of users interfering with computer security is not a new concept. To the contrary, a number of authors have written about the subject. However, in nearly all of these cases, the author focused upon a specific method by which the user can

compromise a system. There is little or no literature that addresses the problem from a unified perspective; the information is scattered in a plethora of sources [12]. My plan is to survey these references and compile a comprehensive list of the ways that computer users can compromise a system and discuss how these risks might best be confronted. My work will interrelate cases from these multiple sources in the literature with case studies and statistical information supplied by ISR regarding our own network. For instance, the number of computers plagued by an email virus in a given year will reinforce the need to better educate users about the threats posed by email attachments. Statistics for security exposures such as this are generally easier to obtain than statistics regarding malicious intent. However, several studies, including the Insider Threat Study [10], highlight specific instances in which a user maliciously attacked a system. I will also explain the technical details of how particular security measures work, such as firewalls and passwords, and the best policies to adopt for them. The policies developed will be created from a variety of existing policies and the recommendations of the aforementioned experts. ISR's policy will be analyzed and compared with others readily available on the Internet [11]. Ultimately, my main contribution will be a consolidation of policies and technical solutions that attempt to minimize the security risks associated with the interface between humans and computers from a holistic approach.

# 4 Conclusion

The primary goal of this project is to illuminate the weaknesses in computer security created by user behavior and establish a coherent plan of attack that will address these

weaknesses. While this plan will be most applicable to corporate computer users, many of the conclusions and proposed solutions will also be applicable to home users.

The project will serve as a fitting complement to my Bucknell education. After three years of focusing on the technical aspects of software development and hardware design, this project will enable me to get an in-depth look of the typical user. The knowledge gained from this project will enable me to understand both sides, to see both sides of the coin simultaneously. This ability to understand the human component of the human/computer interface will enable me to design more secure systems and to develop policies that keep these systems secure, thus serving as a culminating experience in my education.

# References


[1] Anderson, Ross. *Security Engineering.* New York: Wiley Computer Publishing. © 2001

[2] Schneier, Bruce. *Secrets and Lies*. New York: Wiley Computer Publishing. © 2000

[3] Mitnick, Kevin D. and Simon, William L. *The Art of Deception*. Indianapolis: Wiley Publishing, Inc. © 2002

[4] Skoudis, Edward. *Malware.* Upper Saddle River, NJ: Prentice Hall Publishing © 2004.

[5] IEEE Cipher: Newsletter of the IEEE Computer Society Technical Committee on Security and Privacy. http://www.ieee-security.org/cipher.html

[6] The Institute of Electric and Electronics Engineers. http://www.ieee.org

[7] ACM: Association for Computing Machinery. http://www.acm.org

[8] Cert Coordination Center. http://www.cert.org

[9] Institute for Security Technology Studies (ISTS) - Dartmouth College. http://www.ists.dartmouth.edu

[10] Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. U.S. Secret Service and CERT® Coordination Center. August 2004

[11] Private conversation with Eric Smith, Network Administration, Bucknell University.

[12] Professor Sean Smith. Assistant Professor, Department of Computer Science, Dartmouth College. Departmental editor of IEEE Security and Privacy Magazine. Director of the Cyber Security and Trust Research Center at the Institute of Security Technology Studies.