## VITA

John D. Enamait

## EDUCATION

| 2012 | Indiana State University, Terre Haute, Indiana <br> Ph. D. in Technology Management, Digital Communication Systems <br> Specialization |
| :--- | :--- |
| 2001 | Gardner-Webb University, Boiling Spring, NC <br> Masters in Business Administration |
| 1999 | Gardner-Webb University, Boiling Spring, NC <br> Bachelor of Science |
| 1997 | Caldwell Community College, Hudson, NC <br> Associate in Applied Science |
| PROFESSIONAL EXPERIENCE |  |

2007-Present Catawba Valley Community College, Hickory, NC
Dean, School of Business, Industry, and Technology
2003-2007 Caldwell Community College, Hudson, NC
Instructor of Information Systems / Electronic Commerce
1994-2003 NACCO MHG, Inc., Lenoir, NC
Manufacturing Engineer

# THE EFFECT OF PASSWORD MANAGEMENT PROCEDURES ON THE ENTROPY OF USER SELECTED PASSWORDS 

A Dissertation
Presented to
The College of Graduate and Professional Studies
Ph.D. in Technology Management Program
College of Technology
Indiana State University
Terre Haute, Indiana

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
$\qquad$
by
John D. Enamait
May 2012
© John D. Enamait 2012
Keywords: Entropy, password management, information security, digital communication, technology management

## COMMITTEE MEMBERS

Committee Co-chair: Yuetong Lin, Ph. D.
Assistant Professor, Electronics \& Computer Engineering Technology Indiana State University

Committee Co-chair: David Beach, Ph. D. Professor Emeritus, Electronics \& Computer Engineering Technology Indiana State University

Committee Member: Terry Lee Herman, Ed. D.
Associate Professor, Learning Design
Bowling Green State University
Committee Member: Troy Ollison, Ph. D.
Associate Professor, Industrial Management \& Engineering Technology University of Central Missouri

Committee Member: Jeff Ulmer, Ph. D.
Associate Professor, Industrial Management \& Engineering Technology
University of Central Missouri


#### Abstract

Maintaining the security of information contained within computer systems poses challenges for users and administrators. Attacks on information systems continue to rise. Specifically, attacks that target user authentication are increasingly popular. These attacks are based on the common perception that traditional alphanumeric passwords are weak and susceptible to attack. As a result of attacks targeting alphanumeric passwords, different authentication methods have been proposed. Nonetheless, traditional alphanumeric-based passwords remain the most common form of user authentication and are expected to remain so for the foreseeable future.

This study provided empirical data to determine if the entropy of user-selected passwords was affected by the use of password management software. This research also provided data to determine if efforts to increase user-awareness of password strength affected the selection of passwords. The research results revealed that the use of a password management application resulted in an increase in average password entropy, but at a level that was not significant. The research results also indicated that the use of a password management application when coupled with electronic secondary information awareness efforts did result in a significant increase in average password entropy. The research results further illustrated that the use of a password management application when coupled with verbal secondary information awareness efforts also resulted in a significant increase in average password entropy. Finally, this investigation


determined that the use of password management software together with electronic and verbal secondary information user-awareness efforts resulted in an increase in password entropy.

## DEDICATION

Completing this degree will rank among my most significant accomplishments for many years to come. However, I dare not revel in this accomplishment alone for it was earned, in ways, by others as well.

Mark Twain once said "We are always too busy for our children; we never give them the time or interest they deserve. We lavish gifts upon them; but the most precious gift, our personal association, which means so much to them, we give grudgingly." I find the words of Mark Twain to be apropos for a doctoral student. In this case, however, the word family must be substituted for children.

To Anissa and Arielle: this dissertation is dedicated to you. Anissa, your support and determination was like a lighthouse beacon to a ship in the night. It kept me from straying too far off course. Arielle, I pray that this is an example of hard work that you can use throughout your life. May you always dream of butterflies (and fractions)...

## ACKNOWLEDGEMENTS

There are a number of people who provided valuable guidance and insight to me during this process.

First, I would like to thank the members of my committee, Dr. Terry Lee Herman, Dr. Troy Ollison, and Dr. Jeff Ulmer, for their time and efforts in this process. Your willingness to serve on my committee and your thoughtful comments greatly added to the quality of this project. Special recognition and appreciation goes to my committee co-chairs, Dr. David Beach and Dr. Yuetong Lin. My sincere gratitude goes to you both for challenging me to grow throughout this process. Your insight, patience, and support helped me through the process.

I would like to thank Dr. Mark Ciampa for his tremendous support. The many phone calls, emails, and various questions never went unanswered. Thanks for the help and friendship, Mark.

I would be remiss if I did not thank a number of my friends and colleagues at Catawba Valley Community College. I would like to thank Dr. Keith Mackie and Marvin Elliott for their support and willingness to listen when it was needed. I would also like to thank Daniel Clanton for his technical assistance. Gratitude goes to Ari Sigal for reading my countless drafts. I would like to thank Dr. Garrett Hinshaw, Dr. Kim Clark, and Dr. David Streater for their assistance.

I would like to thank my family and extended family for their support. Mom, thanks for the life skills that you instilled in me. They helped mold me into the person I am today. Dad, thanks for the support you gave to me during this process. I knew that you would help in any
way you could. Sharon, thanks providing support to Anissa while this project took me away from her. Everyone, you all have been supportive throughout this process. I thank you.

Each of you listed provided some level of help to me while I toiled away. I am forever in your debt. However, know that my gratitude runs deep and I am humbled by the support that was shown to me. To all of you listed, I thank almighty God for placing you in my life.

## TABLE OF CONTENTS

COMMITTEE MEMBERS ..... ii
ABSTRACT ..... iii
DEDICATION ..... v
ACKNOWLEDGEMENTS ..... vi
LIST OF TABLES ..... xi
LIST OF FIGURES ..... xii
CHAPTER 1 INTRODUCTION .....
Overview ..... 1
Statement of the problem ..... 3
Purpose of the Study ..... 4
Need for the Study ..... 5
Hypotheses ..... 5
Assumptions. ..... 7
Limitations ..... 7
Methodology ..... 8
Terminology ..... 9
CHAPTER 2 REVIEW OF RELATED LITERATURE AND RESEARCH ..... 11
Overview ..... 11
A Brief History of Information Security ..... 12
Attack Costs ..... 14
Types of Attacks ..... 15
Types of Authentication ..... 19
Password Selection Guidelines ..... 32
Alphanumeric Password Challenges ..... 33
Password Management ..... 41
CHAPTER 3 METHODOLOGY ..... 45
Experimental Design of the Study ..... 45
Ethical Considerations ..... 48
Research Participants ..... 48
Data Collection and Analysis ..... 49
CHAPTER 4 FINDINGS AND ANALYSIS OF DATA ..... 54
Overview ..... 54
Descriptive Statistics. ..... 54
Data Analysis ..... 61
Conclusion ..... 65
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS ..... 66
Discussion of Research Findings ..... 66
Implications ..... 68
Recommendations ..... 69
Summary ..... 70
REFERENCES ..... 72
APPENDIX A: INFORMED CONSENT PAGE ..... 83
APPENDIX B: IRB EXEMPT STATUS LETTER ..... 84
APPENDIX C: CVCC PERMISSION LETTER ..... 85
APPENDIX D: CCC PERMISSION LETTER ..... 86
APPENDIX E: VERBAL SECONDARY INFORMATION ..... 87
APPENDIX F: ELECTRONIC SECONDARY INFORMATION ..... 95
APPENDIX G: SURVEY INSTRUCTIONS FOR NON-KEEPASS PARTICIPANTS ..... 96
APPENDIX H: SURVEY INSTRUCTIONS FOR PARTICIPANTS USING KEEPASS ..... 99

## LIST OF TABLES

Table 1 Sample Password Cracking Times ..... 17
Table 2 Entropy Descriptive Statistics ..... 56
Table 3 Normalized Entropy Descriptive Statistics by Condition ..... 58
Table 4 College Major ..... 59
Table 5 Age of Respondents ..... 59
Table 6 Gender of Respondents ..... 60
Table 7 Employment Status of Respondents ..... 60
Table 8 Quiz Scores ANOVA ..... 61
Table 9 Test of Homogeneity of Variance ..... 62
Table 10 ANOVA for Entropy ..... 62
Table 11 ANOVA: Post-Hoc Comparisons of the Control Group (Tukey's HSD) ..... 63
Table 12 Non-Normalized Entropy Descriptive Statistics by Condition. ..... 63

## LIST OF FIGURES

Figure 1 Entropy Histogram .......................................................................................................... 55

Figure 2 Normalized Entropy Histogram ...................................................................................... 57

## CHAPTER 1

## INTRODUCTION

Overview

The security of information contained within computer systems poses challenges for users and administrators. The information contained within these computer systems is being targeted by attackers more frequently each year; when they do strike, attackers often target users of an information system.

The weakest link in an information system is considered to be the user (Kim \& Bzullak, 2008). Users in an information system have multiple deficiencies, but a primary weakness is the selection of weak passwords (Goldberg, Hagman, \& Sazawal, 2002). Although alternatives to alphanumeric passwords exist (Sasse, Brostoff, \& Weirich, 2001), text-based passwords remain the most prevalent form of user authentication (Chiasson \& Biddle, 2007). Consequently, the number of attacks on information systems continues to rise (PricewaterhouseCoopers, 2010). The rise in attacks on information systems is considered to be the cause of the increase in data breaches experienced by organizations. The subsequent costs of data breaches to organizations also continue to escalate. The average cost of a data breach in 2008 was $\$ 202$ per exposed record. This represented a marginal increase of $2.5 \%$ from $\$ 197$ per exposed record in 2007. The 2008 data breach cost represented an 11\% increase from 2006 ( $\$ 182$ per record), and a $46 \%$ increase since 2005 ( $\$ 138$ per record). The average total cost was in excess of $\$ 6.6$ million per
breach, which represented an increase over 2007 (\$6,355,132), 2006 (\$4,789,637), and 2005 $(\$ 4,541,429)$. As a result of these breaches, $53 \%$ of corporate victims have implemented preventative measures such as training and awareness programs, and $40 \%$ launched identity and access management solutions.(2008 Annual study: Cost of a Data Breach, 2008).

The cost of data breaches continues to rise as the information system user continues to be the weakest link. The probability that a brute force attack is successful is directly affected by the complexity of the password used to access the information system (Shay \& Bertino, 2009). The complexity of the password selected by a user is affected by various factors, including memorability and ease of use. As the number of passwords a user needs increases, the complexity of these passwords decrease due to memorability factors. However, Chiasson and Biddle (2007) state that password management software can result in an increase in usability and security since users are only responsible for one password. Furthermore, Kuo, Romanosky, \& Cranor (2006) state that awareness efforts affect user behavior. Users who have a greater awareness of how to create a strong passwords use this information when creating their passwords. Therefore, as users implement additional methodologies to create their passwords, these methodologies are expected to have a positive effect on the entropy of the user-selected passwords. This positive effect is expected to assist organizations limit the total number of data breaches annually as well as decrease the expense of data breaches.

The goals of this chapter are to formulate the problem of data security as it relates to abating data breaches, identify the purpose of the study, and to account for its need. This chapter will also define key terms and describe the methodology that was employed in the study.

## Statement of the problem

The most common form of user authentication is the password. Even though they are widely used, passwords represent a major challenge to information security. Some hurdles include memorability and lack of entropy, which is the amount of randomness associated with information. A password lacking entropy may be defined as an easily guessed password since the password is not random in nature.

The problem addressed by this study was to determine if individuals could employ certain methodologies in order to generate passwords that contain a higher entropy level than when those methodologies are not utilized. More specifically, this study determined if the use of a password management application resulted in an increase in the entropy of user-selected passwords. This study also determined if the entropy of user-selected passwords was increased by awareness efforts when combined with a password management application.

Strong passwords are increasingly more important as use of the Internet and other networks continues to grow (Henry, 2007). Passwords help prevent a breach of data the user is accessing on particular information system. In order for passwords to be resistant to attack, users must select passwords with high entropy. However, evidence shows that users do not select such passwords. This lack of entropy has been identified as a problem with user-selected passwords (St. Clair, Johansen, Enck, Traynor, McDaniel, \& Jaeger, 2006). Lack of entropy in passwords is a result of memory limitations, primarily the ability to recall information. Miller (1956) determined that human memory is constrained to around seven plus or minus two items. Though these constraints exist, computer system users today are required to use an increasing number of passwords (Chiasson \& Biddle, 2007). A recent study by Florencio and Herley (2007b) found that users have approximately 25 accounts that require passwords. In order to compensate for
having this high number of passwords, users generally perform one or two actions. They will either use the same password across different systems to help them remember (Chiasson, Forget, Biddle, \& van Oorschot, 2006), or will select passwords that are easy to remember (Gaw \& Felton, 2006).

Since user authentication is so vital to an information system, it has been studied by a number of researchers. Thorpe (2008) determined that even non-text based authentication schemes result in low entropy. These authentication schemes included graphical passwords. Chiasson and Biddle (2007) conducted studies related to password managers and graphical passwords. Another study found password problems were related to the number of passwords a user must remember, the number of systems requiring passwords, and the complexity of the passwords (Carstens, McCauley-Bell, Malone, \& DeMara, 2004). Thorpe (2008), Chiasson and Biddle (2007), and Carstens, et al. (2004) all make recommendations for further research into increasing the entropy of user-selected passwords.

## Purpose of the Study

The purpose of this study was intended to answer research questions regarding the way individuals within an organization, and thus the organization itself, can implement methodologies to create passwords that are higher in entropy and are therefore more resistant to attack. This research served to provide users, employers, and security administrators with tactics to increase the entropy of user-selected passwords.

This research specifically tested whether the use of particular password management techniques may be used to harden user-selected password strength. The research questions investigated as a part of this study were:

1. Do users who employ a password management application create passwords that are more difficult to decrypt than users that do not use such an application?
2. Do users who are provided information security material in addition to the use of a password management application create passwords that are more difficult to decrypt than users that do not receive such information or use such an application?

## Need for the Study

Predictable passwords are often selected by a user (Chiasson et al., 2007). In addition to predictable passwords, users select passwords that contain low entropy. The need for this research was to determine the influence that password management tactics have on the entropy of user-selected passwords.

## Hypotheses

This study sought to determine if the use of password management techniques result in an average increase in password entropy by testing four hypotheses.
$\mathrm{H}_{0} 1$ - The average password entropy of participants who use a password management application will not exceed the average password entropy of participants who do not use a password management application.
$\mathrm{H}_{1} 1$ - The average password entropy of participants who use a password management application will exceed the average password entropy of participants who do not use a password management application.
$\mathrm{H}_{0} 2$ - The average password entropy of participants who use a password management application and receive verbal secondary information will not exceed the average password
entropy of participants who do not use a password management application or receive verbal secondary information.
$\mathrm{H}_{1} 2$ - The average password entropy of participants who use a password management application and receive verbal secondary information will exceed the average password entropy of participants who do not use a password management application or receive verbal secondary information.
$\mathrm{H}_{0} 3$ - The average password entropy of participants who use a password management application and receive electronic secondary information will not exceed the average password entropy of participants who do not use a password management application or receive electronic secondary information.
$\mathrm{H}_{1} 3$ - The average password entropy of participants who use a password management application and receive electronic secondary information will exceed the average password entropy of participants who do not use a password management application or receive electronic secondary information.
$\mathrm{H}_{0} 4$ - The average password entropy of participants who use a password management application, receive verbal secondary information, and receive electronic secondary information will not exceed the average password entropy of participants who do not use a password management application, receive verbal secondary information, or receive electronic secondary information.
$\mathrm{H}_{1} 4$ - The average password entropy of participants who use a password management application, receive verbal secondary information, and receive electronic secondary information will exceed the average password entropy of participants who do not use a password
management application, receive verbal secondary information, or receive electronic secondary information.

## Assumptions

The following assumptions were made in this research:

1. Any potential bias was minimized by the random selection of participants.
2. The interaction between the researcher and participants was similar and consistent.
3. The time-limited nature of this research will not affect the long-term implications of password management utilization.
4. The participants possessed similar knowledge regarding password selection.
5. The participant's primary language did not affect their ability to participate in this study.
6. The participants realized no financial or grade benefit as a result of participating in this study.

## Limitations

The following limitations were made in this research:

1. Study participants were limited to undergraduate students enrolled in one computer course: CIS 110, "Introduction to Computers," at multiple community colleges in North Carolina.
2. The study was limited to the use of Keepass, an open-source password management application.
3. The study was not longitudinal in nature but assessed the state of participant ability at the date of data collection.

## Methodology

The methodology used in this study enabled the researcher to measure the average entropy of user-selected passwords. A 'posttest-only' control group design was utilized. This research study consisted of four steps:

- Subject were identified to participate in the study;
- The subjects were randomly assigned into a treatment group or the non-treatment group;
- The treatments were administered to all groups;
- The data were analyzed.

There were a total of four treatment groups and one control group in this study.
All subjects participating in this study established passwords to access seven different websites and completed a quiz that was consistent across all groups. The first treatment group only used the password management application and completed the quiz prior to the creation of all seven of their passwords. The data resulting from the treatment of this group allowed the researcher to reject or fail to reject null hypothesis $\mathrm{H}_{0} 1$. The second treatment group used the password management application and received verbal secondary information. The second treatment group completed the quiz after receiving verbal secondary information but before creating all seven of their passwords. The data resulting from the treatment of this group allowed the researcher to reject or fail to reject null hypothesis $\mathrm{H}_{0} 2$. The third treatment group used the password management application and received electronic secondary information. The third treatment group completed the quiz after receiving electronic secondary information but before creating all seven of their passwords. The data resulting from the treatment of this group allowed the researcher to reject or fail to reject null hypothesis $\mathrm{H}_{0} 3$. The fourth treatment group used the
password management application and received electronic secondary information and verbal secondary information. The fourth treatment group completed the quiz after receiving the electronic secondary information and the verbal secondary information but before creating all seven of their passwords. The data resulting from the treatment of this group allowed the researcher to reject or fail to reject null hypothesis $\mathrm{H}_{0} 4$. The control group neither utilized a password management application nor received electronic secondary training or verbal secondary training. The control group completed the quiz before creating all seven of their passwords. Once the participants established their passwords, the researcher recorded and saved these on a remote server. The researcher, using the standard established by the National Institute of Standards and Technology, then calculated the entropy of the passwords.

Terminology
For the purposes of this research, the following definitions apply:
Bit: The smallest unit of information on a computer. The term bit is also called a binary digit (Evans, Martin, \& Poatsy, 2007).

Entropy: The measure of uncertainty that an attacker faces when attempting to determine the value of a secret. Entropy was first introduced by Shannon (1949). Shannon's paper provided the foundation for information theory and represents the degree of randomness associated with information. Entropy is typically expressed in bits (NIST Special Publication 800-63, 2006).

Password management application: Software designed to allow users to use strong passwords (Chiasson, van Oorschot, \& Biddle, 2006).

KeePass: An open-source password management application.
Key logger: A software application or hardware device that records each keystroke made using a specific computer.

Secondary information: Data or information that has been gathered by other individuals or agencies (Crawford, 1997).

## CHAPTER 2

## REVIEW OF RELATED LITERATURE AND RESEARCH

Overview
Information security continues to be a problem for computer users and organizations. Information security has been defined as the confidential access to accurate information by those who need it (Carstens et al., 2004) and is an ever-increasing problem because the number of attacks on information systems continues to climb. Carnegie Mellon's Computer Emergency Response Team has shown that the number of computer security incidents has increased from six in 1988 to 137,529 in 2003 (Carstens et al., 2004). In addition, over 220 million data breaches occurred between January 10, 2005 and March 24, 2008. Approximately 160 million of these involved hacking (Garrison, 2008). Many of these attacks are the result of a weak link in information security.

Users of information systems are considered to be the weakest link in information security (Kim \&Bzullak, 2008) for a variety of reasons. The first is negligence, which causes computer systems to suffer (Dhamija \& Perrig, 2000). A second reason is that users have memory limitations (Forget, Chiasson, \& Biddle, 2007). A third reason users are a weak link is because users select predictable passwords (Goldberg, Hagman, \&Sazawal, 2002). Attacks on information systems therefore continue to grow.

## A Brief History of Information Security

Information security efforts from the 1960's to the mid- 1980's were concentrated on single computer systems. These computer systems were mostly mainframe computers and minicomputers (Canavan, 2001). Initially, these computer systems were not connected to a network. Instead of communicating with the computer systems via a network, users employed terminals for access. The computers were not available for public use; rather, they were accessible only to trained technicians (Bosworth \& Jacobson, 2002).

In 1969, the first major computer network was introduced. This system, the Advanced Research Projects Agency Network (ARPANET), was sponsored by the Department of Defense. It connected research computers at the University of California at Los Angeles, the University of California at Santa Barbara, the Stanford Research Institute, and the University of Utah. This network would ultimately be the predecessor to the Internet (Bosworth \& Jacobson, 2002).

In 1970, the earliest documented attack on a computer network was released. The Creeper virus was unleashed onto the ARPANET by an unnamed person (Elliott, Young, Collins, Frawley, \& Temares, 1991). The Creeper virus spread harmlessly from one computer to another through modems. The infected machine displayed the message 'I'M THE CREEPER: CATCH ME IF YOU CAN' (PricewaterhouseCoopers, 2010).

The development of the computer network, the introduction of personal computers, and the development of new applications resulted in a new age of information technology. These new technologies allowed computers to be linked to the outside world via computer networks. During this time, programs began to be executed on local computers and it became possible for the public to transfer data from one computer to another. Furthermore, portable devices such as
floppy disks began to store data and allow for the portability of that data (Bosworth \& Jacobson, 2002).

The first major attack on a computer network occurred in 1988 (Conklin, White, Cothren, Williams, \& Davis, 2004). The "Internet Worm" was created by Robert Morris, Jr. Morris was a graduate student at Cornell University and the son of the former chief scientist at the National Computer Center, a branch of the National Security Agency (Rosenberg, 2004). Morris' worm used automated password guessing techniques to crash more than 6,200 computers in the United States (Zviran \& Haga, 1999). Computers crashed as a result of the worm reproducing so rapidly that computers had no time left to do any useful work (Conklin et al., 2004).

Since the Morris incident, major attacks involving computer networks became more common. These have included attacks such as the Melissa virus, which caused an estimated $\$ 80$ million in damages. The Love Letter worm was another significant attack, which cost an estimated $\$ 10$ million. Another example is the 2003 Slammer worm (Conklin et al., 2004). This worm infected over 120,000 computers within the first 24 hours of its release. It caused computer networks to crash and created problems with ATMs and airline flights (Conklin et al., 2004). Other attacks continue to affect both organizations and individuals. User accounts at eBay fell victim to successful dictionary attacks. In these attacks, hackers broke into the accounts of sellers with positive ratings and set up fraudulent auctions (Pinkas \& Sander, 2002).

The number of attacks continues to rise. According to the Privacy Rights Clearinghouse, over 220 million data breaches occurred between January 10, 2005 and March 24, 2008. Approximately 160 million of these involved hacking (Garrison, 2008). Additionally, Carnegie Mellon's Computer Emergency Response Team discovered that the number of computer security incidents increased from 6 in 1988 to 137,529 in 2003(Carstens et al., 2004).

Initial attacks on computers and computer networks were the result of researchers learning about computers and networking. According to Ciampa (2008), however, attacks on information security shifted after 2001. At this time, a collective body of attackers began to become organized. This body of individuals included attackers and identity thieves. This collective body is referred to as cybercriminals and they have the attention of the United States government. President Barack Obama ordered a complete review of the United States' policies and structures regarding security in cyberspace shortly after assuming office. As a result of this review (Cyberspace Policy Review), the United States government has developed action plans that outline how the country will handle cyberterrorism (Executive Office of the President, 2009). A United States Senator has aptly said, "We live in a world where a terrorist can do as much damage with a keyboard and a modem as with a gun or a bomb" (Crowley, 2003).

## Attack Costs

The human error aspect of information security can have a negative impact on business (Carstens et al., 2004).The resulting costs of these errors continue to escalate. The 2008 average cost of a data breach was $\$ 202$ per exposed record. This represented a marginal increase of $2.5 \%$ from 2007, which was $\$ 197$ per exposed record. The 2008 data breach cost represented an 11\% increase from 2006 ( $\$ 182$ per record) and a $46 \%$ increase since 2005 ( $\$ 138$ per record). The average total cost was in excess of $\$ 6.6$ million per breach which represented an increase over 2007 (\$6,355,132), 2006 (\$4,789,637), and 2005 (\$4,541,429), respectively (2008 Annual study: Cost of a Data Breach, 2008). Costs associated with unauthorized access to information increased from $\$ 51,545$ in 2004 to $\$ 303,234$ in 2005(2005 CSI/FBI Computer Crime and Security Survey, 2005). The average loss was $\$ 288,618$, up from $\$ 167,713$ in 2006 (2008

CSI/FBI Computer Crime and Security Survey, 2008). Financial fraud accounted for the most expensive computer security incident in 2008. The average cost was $\$ 500,000$.

## Types of Attacks

The information contained within computer systems continues to be the target of attacks. This may be because information security has thus far been treated solely as a technical problem and has ignored the human element (Wiedenbeck, Waters, Birget, Brodskiy, \& Memon, 2005). Attacks are often the result of human negligence. Carstens et al. (2004) found that indirect or direct user action accounted for $70 \%$ of security breaches at businesses. Another study found that more than $88 \%$ of data breaches were the result of insider negligence (2008 Annual study: Cost of a Data Breach, 2008). Passwords are often the target of attacks and password issues pose a significant risk factor to an information system. The significance of this problem is magnified since passwords are the most common type of user authentication for the majority of users and organizations (Carstens et al., 2004). Kuo, Romanosky, \&Cranor (2006) found that passwords are generally compromised in several ways:

- Guessing the password based on knowledge of the user;
- Social engineering;
- Shoulder surfing;
- Using cracking software, such as John the Ripper.

Yan (2001) states that when a password is cracked by a hacker, one of two methods may be used. The first method is a dictionary attack, which tries a list of words and other weak passwords. The second method is a brute-force attack to analyze the entire key space.

A brute-force attack is a method that attackers may employ to identify the password of a user and consists of performing an exhaustive trial-and-error search of possible passwords (Network dictionary).

Brute-force attacks are used with varying degrees of success. Attackers are successful in part because default passwords are still being used. Systems are still vulnerable to brute-force and dictionary attacks (SANS Top-20 2007 Security Risks, 2007). The success of a brute-force attack depends on the entropy of the password being attacked. Florencio, Herley, and Coskun (2007a) stated that it is "common to assume that stronger passwords help against guessing and brute-force attacks." A number of studies have been conducted in an attempt to determine how vulnerable passwords are against brute-force attacks. Klein (1990) reported being able to crack approximately $25 \%$ of passwords using brute force. Belgers (1993) analyzed 521 passwords and was able to breach $11.1 \%$ in 25 hours. Windows alphanumeric passwords have been cracked in less than 14 seconds (Wagner, 2003). When conducting an analysis of conference attendee passwords, Garrison (2008) found that almost half of the passwords could be cracked in less than one week. Examples of password cracking times are found in Table 1 (Wakefield, 2004). Held and Bowers (2001) provide the following algorithm in order to estimate how long a password can withstand an attack:

$$
\mathrm{T}=\mathrm{m}^{\mathrm{n}} / 2 * \mathrm{i} * 1 / \mathrm{MIPS} \text { where: }
$$

T = Amount of time in seconds it takes to crack the password
$\mathrm{m}^{\mathrm{n}}=$ address space of password
$\mathrm{i}=$ number of instructions in the cracking algorithm
MIPS $=$ Machine speed of the machine executing the algorithm
A password that consists of a combination of seven upper- and lowercase letters and numbers 0 9 is used as an example. This password has an available password space of $62^{7}$ units. The example extrapolated is:

$$
\begin{aligned}
& \mathrm{T}=1,760,807,303,104 \text { passwords } * 100 \text { instructions/password } * 1 \text { second/500,000,000 } \\
& \text { instructions }=352,161 \text { seconds } \\
& \quad=5,869 \text { minutes }=4.08 \text { days }
\end{aligned}
$$

As seen in the algorithm, the time it takes to crack a password depends on three variables: The password itself, the cracking algorithm application, and the computer speed. As computational speed increases rapidly, the amount of time it takes to crack a password will decrease.

Table 1
Sample Password Cracking Times

| Number of <br> Characters | Possible Combinations | Person Attempt Time | Computer Attempt Time |
| :--- | :--- | :--- | :--- |
| 1 | 36 | 6 minutes | 0.000036 second |
| 2 | 1,300 | 4 hours | 0.00130 second |
| 3 | 47,000 | 6 days | 0.04 second |
| 4 | $1,700,000$ | 6 months | 2 seconds |
| 5 | $60,000,000$ | 20 years | 60 seconds |
| 10 | $3,700,000,000,000$ | $>999$ million years | 118 years |

One example of a brute-force attack is a dictionary attack. A dictionary attack is a method in which an attacker systematically searches for the correct password by using words in a collective list, such as a dictionary (Shirey, 2000). A dictionary attack method reduces the total password space by making assumptions about how the user selected his password (Yee \& Sitaker, 2006).

These types of attacks are used with some success. Klein (1990) concluded that $25 \%$ of all passwords are vulnerable to a small dictionary attack. Attackers know that weak passwords may be broken via a dictionary attack or by some knowledge of the user (Wiedenbeck et al., 2005). Attackers attempting to guess a password will "try the most likely chosen passwords first" (Burr, Dodson, \& Polk, 2006). One reason dictionary attacks are successful is the wide scope of the search list. Dictionaries used in password cracking software are available in multiple languages (Kuo et al., 2006).

There are a variety of brute-force cracking applications available. "Crack" is a popular password cracking software (Yan, 2001). "John the Ripper" is an open source password cracking application (Openwall Project). Cain and Abel is a Windows password recovery application (Oxid, n.d.).

Additional attacks on information systems include shoulder surfing, phishing, social engineering, and keyboard emanations. Many successful attacks are executed by means of social engineering techniques. This technique is defined as "psychological manipulation or other nontechnical means to detect information" (Henry, 2007). Hackers use these techniques to obtain passwords because they understand the weakest link in information security is the human factor (Adams \& Sasse, 1999). Shoulder surfing is considered a form of social engineering. This occurs when a person looks over a user's shoulder when the user is entering their password (Henry, 2007; Kyas, 1997). Shoulder surfing is a significant threat even though most people understand that they should not type their password when someone is watching (Florencio et al., 2007a). Keyboard emanations are another form of attack, albeit uncommon. Asonov and Agrawal (2004) were able to show that computers are vulnerable to attacks based on the sound of key input. Asonov and Agrawal's study was followed by a study conducted by Zhuang, Zhou, and Tygar
(2005). This groups study was done by recording a 10 -minute session of a user working on a computer. The researchers were able to recover up to $96 \%$ of the typed characters. Their conclusion was that passwords are recoverable using keyboard emanations.

Phishing is another form of attack. Phishing is a social engineering technique used to commit fraud. According to Henry (2007), a phishing attack is carried out by an attacker acting as a trustworthy source. According to Ciampa (2008), the act of phishing is executed in two ways. The first method is the social engineering method, in which an attacker sends an e-mail in an attempt to fool the user into giving personal information, which could include passwords. The second method is utilization of technology to steal personal information. For example, software applications such as key loggers are often used (Ciampa, 2008).

## Types of Authentication

Authentication mechanisms are the means by which how users prove their identity to the computer system. Authentication may also be defined as determining whether a person should or should not have access to a system (Wiedenbeck et al., 2005). Characteristics of authentication mechanisms should include being available to the user, being robust and reliable, being user friendly, and having a low cost to implement and operate (Pinkas \& Sander, 2002). The methods of authenticating a user may be categorized in different forms. These include knowledge-based systems, token-based systems, and systems based on biometrics (Dhamija \& Perrig, 2000). Also, authentication techniques for users include what the user knows, what the user possesses, and "what the user is" (Brostoff \& Sasse, 2000).

Text-based passwords are presently the most common form of user authentication (Chiasson \& Biddle, 2007). However, alternatives to text-based passwords do exist (Sasse, Brostoff, \& Weirich, 2001), or have been suggested (Renaud, 2005). Others are being researched
(Chiasson \& Biddle, 2007) and include biometrics, hardware tokens, and graphical authentication (Mulligan \& Elbirt, 2005). Other authentication tools include single sign-on, onetime use passwords, and recognition-based passwords. In some cases, federal regulations necessitate investigating alternative authentication methods. As a result of the Health Insurance Portability and Accounting Act of 1996 (HIPAA), IT managers are investigating alternative methods of authentication such as smart cards and biometrics (Heckle \& Lutters, 2007).

Another approach to authenticating users is by using biometrics. Biometric authentication systems have been investigated as an alternative to text-based passwords (Kim \& Bzullak, 2008; Narayanan \& Shmatikov, 2005). Biometric authentication uses a physical or behavioral characteristic to identify a user. This can be fingerprints, signatures, or voice (Brostoff \& Sasse, 2000).According to the 2008 CSI/FBI Computer Crime and Security Survey, $23 \%$ of surveyed organizations are using biometrics as one method of user authentication (2008 Annual study: Cost of a Data Breach, 2008).

Biometric authentication is not without its downside. One drawback is that the users cannot easily be changed. Therefore, the biometric identifier needs to be well protected. Another drawback of a biometric system is that analog copies of a biometric can be stolen and replicated. For example, a fingerprint that was left behind by an authenticated user may be stolen by an attacker and used to gain access to the system (Brostoff \& Sasse, 2000). Another disadvantage of employing biometric authentication is cost. Biometrics requires use of additional hardware, which can be expensive (Dhamija \& Perrig, 2000). The keystroke dynamics form of biometrics can be a less costly option, but users resist this form because it can be used to monitor productivity (Brostoff \& Sasse, 2000).Another drawback of biometric systems is they can be
"unpleasant to use" (Dhamija \& Perrig, 2000). Finally, biometrics raise privacy concerns (Wiedenbeck et al., 2005).

Biometrics is a relatively secure alternative to text-based passwords. However, financial constraints prevent smaller businesses from implementing this solution (Kim \& Bzullak, 2008). Bunnell, Podd, Henderson, Napier, and Kennedy-Moffat (1997) note that biometrics are usually expensive and most likely will not replace traditional passwords.

Another approach to authenticating users is that of hardware tokens. Hardware tokens have been investigated as an alternative to text-based passwords (Brostoff \& Sasse, 2000; Dhamija \& Perrig, 2000). Token-based authentication uses a physical device to authenticate a user of a computer system. An advantage of doing this is the difficulty of cloning the device (Brostoff \& Sasse, 2000). Such devices include smart cards or a USB token. According to the 2008 CSI/FBI Computer Crime and Security Survey, 36\% of surveyed organizations are using smart-cards or other hardware tokens as a form of user authentication (2008 Annual study: Cost of a Data Breach, 2008).

The use of hardware tokens creates some challenges. One weakness of such authentication systems is that tokens require additional hardware, which can be expensive because a token reader must be present at each location from which the user needs to be authenticated (Brostoff \& Sasse, 2000). A second drawback is that such systems also need knowledge-based authentication since the token can be lost by the user (Wiedenbeck et al., 2005). A third weakness is that possession of a token does not prove identity (Brostoff \& Sasse, 2000).

One-time passwords are a variation of hardware token authentication systems and are commonly used in conjunction with them. The token creates a new password at fixed time
intervals and is synchronized with a server generating the same new password at the same time interval. A one-time password has the advantage of providing security in the event the password becomes compromised. The compromised password will work only once, after which the system generates a new random password which renders the previous one obsolete (Summers \& Bosworth, 2004). In addition, one-time password authentication systems provide greater security than traditional text-based passwords (Florencio et al., 2007b).

One-time passwords are not, however, without drawbacks. One weakness is that users must keep the token with them when they need to be authenticated on computer systems (Summers \& Bosworth, 2004). There is also the additional cost associated with one-time passwords as a result of extra hardware and software as well as changes in infrastructure (Bigler, 2004).

Due to the problems associated with hardware tokens, their use is a not yet a viable alternative to text-based passwords (Florencio et al., 2007b). Instead, hardware tokens are being implemented as a complementary solution to text-based passwords (Brostoff \& Sasse, 2000; Dhamija \& Perrig, 2000).

Single sign-on is another method of authenticating users to a computer system. The use of single sign-on has been investigated as an alternative to text-based passwords (Sasse et al., 2001; see also Heckle \& Lutters, 2007). A single sign-on authentication system allows a user to gain access to multiple systems while logging in just once. An advantage of using single sign-on is that it reduces the number of passwords a user must remember for multiple systems. This approach to authentication is gaining popularity and seems to be emerging as the solution of choice in certain industries because of HIPAA guidelines (Bigler, 2004; Heckle \& Lutters, 2007, Kim \& Bzullak, 2008).

Single sign-on systems do pose challenges. One is cost (Sasse et al., 2001). The cost associated with single sign-on is the result of added hardware, extra software, and changes in infrastructure (Bigler, 2004). Another drawback of single sign-on is that some systems will not support it (Bigler, 2004). Heckle \& Lutters (2007) conducted a study on single sign-on systems. Based on their work, these researchers found that users express concerns over the use of single sign-on. Single sign-on systems are a viable authentication system, but their implementation cost is a barrier for small businesses.

Graphical passwords are another technique of authenticating users and have been investigated as an alternative to text-based passwords (Gaw \& Felton, 2006; Narayanan \& Shmatikov, 2005). Graphical passwords have been researched in an attempt to make authentication more secure (Wiedenbeck et al., 2005). PassPoints is one graphical password scheme that has garnered research attention. Using PassPoints requires users to click on a number of points on a single background image. Research has shown, however, that PassPoints passwords are not more secure than the text-based ones they were intended to replace (Thorpe \& van Oorschot, 2007).

Déjà Vu is another graphical password scheme that has been studied. Dhamija and Perrig (2000) proposed a recognition-based authentication system that allows users to be authenticated by recognizing images. The person first creates an image portfolio consisting of $p$ images. The system then presents the user with a challenge set of $n$ images. In order to be authenticated to the system, the user must correctly identify which images are part of their portfolio. Deja Vu therefore has three phases: creation of portfolios, user training, and user authentication. Their study concluded that the image portfolio took longer to create than passwords and the time required to login was also longer than for text-based passwords.

Another graphical password system that has been developed is Passdoodles. Goldberg et al. (2002) studied Passdoodles. Passdoodles are handwritten designs or text and are typically drawn using a stylus on a touch screen. The study asked users to create a passdoodle and an alphanumeric password. The alphanumeric passwords were at least six characters long. Users were then asked to create alphanumeric passwords that were not found in the dictionary. The researchers found that users were able to recall the alphanumeric passwords more accurately than passdoodles.

Passfaces is another graphical authentication system that has been proposed. This authentication system allows users to select four faces from a grid. The faces selected become the user's authentication method. Based on a study conducted by Brostoff and Sasse (2000), Passfaces took longer to execute than passwords. In addition, users logging in via passfaces started work later than those who used passwords and logged into the system less often.

PassPoints is still another graphical password scheme. This graphical system authenticates by multiple clicks on a single image. Users select where on the image they want to click for their password. After the user clicks a point on the image, the PassPoints system develops a tolerance around the click point. When authenticating, the user must click within the tolerance region. The size of the tolerance region may vary, but is not recommended to exceed 2 - 5 millimeters. The PassPoints can create a "very large password space." If a user selects five click points on an image $330 * 260 \mathrm{~mm}^{2}$, the system yields $590^{5}=7.15 * 10^{13}$ memorable passwords. With six click points, the system yields $4.22 * 10^{16}$ memorable passwords. Other recognition-based systems would require 14 or 15 rounds in order to provide a password space equal to that of PassPoints. The results of the authors study indicate that users remembered the image presented, but had trouble recalling where they clicked (Wiedenbeck et al., 2005).

There are graphical password alternatives to text-based ones, though studies show they have problems similar to text-based passwords. In addition to the problems cited above, some graphical password alternatives have disadvantages due to their increased use of bandwidth (Sasse, et al., 2001). Further, widespread adoption of graphical passwords would require significant changes in user behavior. Users would need training about how to make effective use of graphical passwords and service providers may be reluctant to implement a new technology (Pinkas \& Sander, 2002). Finally, a drawback to image-based authentication is the limit to the number of images that may be displayed during the authentication process. Wiedenbeck et al. (2005) write, "To obtain security similar to that of 8-character alphanumeric password (over an alphabet of 64 characters), 15 or 16 rounds with 9 faces each would be required. This could make the login process slow and tedious. Also, using faces as the images has been shown to lead to passwords with very low entropy because people choose faces in predictable ways." Based on these results, graphical passwords are not expected to replace traditional text-based passwords as a primary authentication mechanism.

Mnemonic passwords are another method of authenticating users to a computer system. Mnemonic passwords have been researched as a possible alternative to traditional text-based passwords. These are passwords selected by using a character from each word in a memorable phrase. The first character of each word in the phrase is often selected (Kuo et al., 2006). Mnemonic passwords are thought to be stronger than traditional text-based passwords for three reasons: (1) mnemonic passwords do not appear in the dictionary, (2) users may have a mix of different character classes and, (3) the space of possible phrases is almost infinite (Kuo et al., 2006). Kuo et al. (2006) conducted a study on mnemonic passwords and concluded that mnemonic passwords are not as strong as first thought. The mnemonic passwords did not
incorporate more character classes (upper- and lower-case) than the control group. The password length was roughly the same. Based on these results, mnemonic passwords are not expected to replace traditional text-based passwords.

The most common way to authenticate users currently is the alphanumeric password (Chiasson \& Biddle, 2007; Kim \& Bzullak, 2008). Alphanumeric passwords use information that the users know to prove their identity to the computer (Brostoff \& Sasse, 2000). Such passwords are still used by $80-95 \%$ of businesses to protect their information systems (Armstrong, 2003). This type of password is required by email providers, banks, dating, and social networking sites (Florencio et al., 2007b). More secure authentication mechanisms, such as smart cards and public key cryptography, have been proposed, but none have become widely used (Pinkas \& Sander, 2002). Alternatives are expensive to implement; passwords are still common because they are cheap and simple (Mulligan \& Elbirt, 2005).

Even though they are the most widespread form of authentication, alphanumeric passwords have limitations. A primary weakness of a knowledge-based authentication system is that it requires a precise recollection of some piece of information. If a user makes the slightest mistake when entering the secret, she is not authenticated to the computer system (Dhamija \& Perrig, 2000).Furthermore, Bunnell et al. (1997) state, "unless passwords are easy to remember, difficult to guess, and frequently changed, they will not reach their full potential as a security technique." Another negative aspect of alphanumeric passwords is that a weak password could result in a compromised computer system resulting in identity theft, data loss, or a large financial loss (Spafford, 1992).

Users of computer systems are a hindrance to a secure authentication process. This is due to the methods by which users select their passwords. The length of passwords selected by users
varies greatly, as does their composition. Furthermore, passwords are selected based on items or people that are familiar to users. This could be their own names, family names, phone numbers, or favorite movies (Dhamija \& Perrig, 2000).

Alphanumeric passwords have been the subject of a variety of research studies. Specifically, these studies have attempted to determine the content of user-selected passwords. In one study, CentralNic (2001) surveyed 1200 people and determined that user-selected passwords can be divided into one of four categories based on their way of selecting passwords. The first category is the family group. These users select passwords from the names of family. This group represented $47.5 \%$ of the population studied. The second category is the fan group who select passwords based on the names of sports stars or other famous people. The fan group represented $32 \%$ of the population. The third group is the fantasists who select passwords based selfobsession. They represented $11 \%$ of the population. The last category of users is the cryptics group. These users select passwords that include upper- and lower-case letters, numbers, and punctuation. This group represented just $9.5 \%$ of the population (CentralNic, 2001).

Other studies reinforce CentralNic's finding that users base their passwords on their names. Harada \& Kuroki (1996) found that $42 \%$ of respondents used their names in their passwords. In another study, Wu (1999) found that 283 out of 2045 passwords studied were based on the username or some derivation of the person's name. Brown, Bracken, Zoccoli, and Douglas (2004) completed a study in which 218 users participated. Their results indicated that $92.7 \%$ of participants used their name in the password. A relative's name was used in the password $27.7 \%$ of the time. A pet's name was used in $15.5 \%$ of the cases. They also discovered that $45 \%$ of participants used their name for at least one password.

When users do not use their name in the selected password, they often use words found in the dictionary. Riddle, Miron, and Semo (1989) found that $44 \%$ of a sample of 7000 passwords was English words. This is consistent with Morris and Thompson's (1979) finding that passwords were very weak because they were easily found in a dictionary. Morris and Thompson (1979) analyzed 3289 passwords and found that $86 \%$ of the passwords were words in the English dictionary, reverse spellings of words in the dictionary, first or last names, street names, cities, Social Security numbers or telephone numbers, making them very weak.

The literature attests to the fact that users select a password that includes their name. In addition to using their names as passwords, users tend to select passwords that are short. DeAlvare (1998) states that users select passwords having as few characters as possible. Weak passwords are created by using only lowercase letters only, passwords being too short, using only digits, or being easily found in a dictionary. Wu (1999) conducted a study of over 25,000 users and found that $26 \%$ of passwords used at least one digit and four percent of passwords used at least one non-alphanumeric symbol. Wu's data about the number of characters in a password is:

- Two characters: $0.1 \%$;
- Three characters: $0.6 \%$;
- Four characters: 3.8\%;
- Five characters: 7\%;
- $\quad$ Six characters: $11 \%$;
- $\quad$ Seven characters: $8 \%$;
- Eight characters: 54\%;
- Nine characters: 8\%;
- Ten characters: $4.5 \%$.

Approximately $88 \%$ of the passwords were therefore eight characters or less (Wu, 1999). Morris and Thompson's (1979) study complemented Wu's finding. In their study listed above, they found that 15 passwords were only a single American Standard Code for Information Interchange (ASCII) character long; 72 passwords were strings of just two ASCII characters; 464 were three ASCII characters; 477 passwords were four alphanumeric characters long; 706 passwords were five characters; 605 had six characters. Of all passwords included in the study, $86 \%$ had six or fewer characters. In another study, Riley (2006) found that the average number of characters used in a password was 6.84 . Sixty-three percent of users recognized they should use seven or more characters in their password, but only $35.5 \%$ do so. Another study showed that $60 \%$ of respondents use fewer than eight characters (Harada \& Kuroki, 1996). Riddle et al. (1989) also found that passwords were too short; $61 \%$ of them were only four characters. Dhamija and Perrig (2000) found an average password length to be six characters.

In addition to selecting passwords that are too short, users are deficient concerning the composition of their passwords. In Zviran and Haga's study (1999), $80.1 \%$ of users prefer to use alphabetic characters in their passwords. They determined that users do not use nonalphanumeric symbols. Riley's (2006) study found that $85.7 \%$ of users employ lowercase letters and $56.5 \%$ use numbers or digits in their passwords. However, half the users who use numbers choose ones that have some personal meaning, such as a telephone number. Half of the study participants say they should use special characters in their password, but only $5 \%$ do so. Morris and Thompson (1979) found that $86 \%$ of passwords did not mix upper- and lower-case letters, nor did they include special characters. Wu (1999) found that only $4 \%$ of passwords used at least one non-alphanumeric symbol and determined that $86 \%$ of passwords could be typed without the shift key. The study conducted by Riddle et al. (1989) provides further support that users do not
mix case. They found that a combination of letters and numbers were used by just $4 \%$ of users. Harada and Kuroki (1996) found that $60 \%$ of respondents do not mix case, and $59 \%$ of respondents do not use non-letter symbols. The study conducted by CentralNic (2001) concluded that approximately $10 \%$ of users select passwords that include upper- and lower-case letters, numbers, and punctuation. Most passwords that include a mix of letter case or use numeric characters are composed of alphabetic characters "appended by one or two numerical characters"(Dhamija \& Perrig, 2000).

Users rely upon information about which they are knowledgeable when selecting passwords. Thus, when creating passwords, most people use personal information (McDowell, Rafail, \& Hernan, 2009; Wakefield, 2004). Users do not believe their personal information is easily retrievable (Wakefield, 2004).Morris and Thompson's (1979) study showed the fallacy of that view. Brown et al. (2004) support Morris and Thompson's study. Their study concluded that $67 \%$ of passwords were selected based on personal information. Approximately $50 \%$ of the passwords included names and birthdays. Furthermore, CentralNic's (2001) study concluded that people select passwords that represent themselves in some way. Finally, Bunnell et al. (1997) found that $77 \%$ of the participants created their password based on one meaningful detail - either a name or date.

The literature also reveals that users have certain attitudes towards passwords and their selection. First, most users will meet only the minimum requirements for password creation (Dhamija \& Perrig, 2000). Users will ignore established guidelines for password creation. Zviran and Haga (1999) found that $47 \%$ of respondents did not create passwords that follow generally accepted guidelines. Moreover, Riley (2006) found that $52.7 \%$ of users never change their password when not required by the system. They also found that $33 \%$ use a variation of the same
password for multiple accounts. Another study concluded that users did not understand what constitutes a strong password. "Some users devise their own methods for creating memorable multiple passwords through related passwords - 50\% of users employed this method"(Adams \& Sasse, 1999). Moreover, people freely share their passwords with friends and/or family (Adams \& Sasse, 1999; see also Dhamija \& Perrig, 2000). Another user behavior is compensating for forgetting passwords by limiting their strength along with restricting how many passwords they use (Wiedenbeck et al., 2005).

Sasse et al. (2001) conducted a study in which they found seven issues that resulted in poor password selection. The first issue is identity. The researchers concluded that people who use strong passwords are often considered paranoid. Other users are proud that they are not 'nerds.' The second issue pertains to socialization. They found that sharing passwords is considered to be a sign of trust among colleagues. The third issue is that users believe no one will target them. Users do not think that their protected information is important enough to be targeted by a hacker. The fourth issue is that users believe hackers could not do much damage even if their password were compromised. The next issue relates to employment. Users believe that someone should be able to access their account when they cannot work. The sixth issue relates to accountability. Users do not expect to be held accountable if a hacker breaks into their account. The last issue is the 'double-binds' issue. Users believe that if an information system is well protected, it will challenge hackers.

Users are not diligent about changing their passwords. Riley (2006) found that $52.7 \%$ of users never change their password unless they are required to do so by the system. DeAlvare (1998) states that once a user selects a password, they are not likely to change it until it is
compromised. When forced to change their passwords, most users change the password to a variant of the original (Dhamija \& Perrig, 2000).

## Password Selection Guidelines

Though users follow certain patterns when selecting their passwords, guidelines do exist for choosing passwords that are secure. Narayanan and Shmatikov (2005) state that organizations often establish complex password policies. These policies generally require that passwords include numerals and special characters. This is done to decrease the vulnerability of passwords to brute-force dictionary attacks. Wagner (2003) recommended that organizations require and enforce strong passwords for Windows. He further recommends that organizations prohibit the re-use of Windows logon passwords.

There are additional guidelines for password selection found in the literature. First, passwords should not contain words that are commonly found in a dictionary (Frank \& Charron, 2002; SANS Top-20 2007 Security Risks, 2007; Wakefield, 2004). Second, passwords should not contain personal information (Garrison, 2008; McDowell et al., 2009). Third, secure passwords should consist of a mix of upper- and lower-case letters. A combination of letters, numbers, and symbols are recommended (Frank \& Charron, 2002; Garrison, 2008; McDowell et al., 2009; Wakefield, 2004; Wiedenbeck et al., 2005). Yan, Blackwell, Anderson, and Grant (2004) also recommended that users should select passwords that contain numbers and special characters. They found that if these instructions are not provided, users will select their passwords from a limited password space that inhibits password strength. Passwords should also be eight or more characters long (Frank \& Charron, 2002; Garrison, 2008; Wakefield, 2004; Wiedenbeck et al., 2005). Passwords need to be changed at regular intervals as well (Florencio et al., 2007b) and should not be shared with co-workers or family (Wakefield, 2004). In certain
cases, federal guidelines explicitly state that passwords should not be shared or written down (Heckle \& Lutters, 2007). Other research findings corroborate the benefits of not writing down passwords for assistance (Florencio et al., 2007a; Wakefield, 2004).

Although alphanumeric passwords remain the most common form of authentication in use today, secure information systems designed in the future that consider what you have and who you are will eventually replace conventional passwords. However, the displacement of traditional passwords may be years away due to resistance to change. As a result, traditional textual passwords will continue to be used (Brown et al., 2004; Kuo et al., 2006; Pinkas \& Sander, 2002).

## Alphanumeric Password Challenges

Passwords as authentication mechanisms face certain challenges. Passwords are the weakest element in information security (Mulligan \& Elbirt, 2005). More specifically, users that select passwords are the weakest link in information security. A password is most often cracked by exploiting the human aspects of the password rather than breaking the cipher (Narayanan \& Shmatikov, 2005). Users do not generally understand authentication and do not understand what constitutes a strong password (Chiasson \& Biddle, 2007). Additionally, they are not educated about challenges to information security (Adams \&Sasse, 1999). Many recommendations exist for the creation of secure passwords. However, using password guidelines or rules do not assist users in recalling their passwords (Chiasson et al., 2006). Further, telling people what they should do, of course, has little or no positive effect (Bosworth \& Kabay, 2002). This means that users have a tendency to circumvent procedures, which they view as complicating to their ability to accomplish a task. Shostack and Syverson (2004) wrote that users are concerned about
information security only when they see a direct threat. However, this type of risk usually happens only after a breach.

A primary concern regarding passwords is the memorability limitations of users. When people remember a sequence of items, those items must be in sections of familiar information. User memory is reliant on redundancy; users remember passwords better if they can encode it in multiple ways (Yan et al., 2004). The limitations of a user's memory cause a number of flawed behaviors. These behaviors include selecting passwords with low entropy, re-using of passwords, writing down passwords, and making a conscious decision to circumvent established security procedures.

Another challenge facing text-based authentication is the number of passwords users must have when logging into different computer systems. Various studies have been conducted to determine the number of passwords per user. The research shows that the number of passwords required by a user is increasing (Dhamija \& Perrig, 2000). That number varies according to the research. Brown et al.'s (2004) study of college students found an average of 4.45 passwords with 8.18 password uses. Summers and Bosworth (2004) found that $50 \%$ of users had at least five passwords, and nearly one-quarter of users had more than eight passwords. Ives, Walsh, and Schneider (2004) found that users may use up to 15 passwords daily. Swartz (2006) found that $50 \%$ of users have four to seven passwords to remember. Furthermore, $17 \%$ of users have 8-10 passwords to remember. Gaw\& Felton (2006) state that users had 1-7 unique passwords for 10-50 websites. Yet another study by Rosencrance (2003) found that over 24\% of users have at least eight user names and passwords. Average users have more than five passwords. Florencio and Herley (2007) conducted a study that measured and reported the password habits of web users. Average users have 6.5 passwords. Another survey conducted by

Kim and Bzullak (2008) found an average of six passwords per user. One user had 30 passwords for work. Riley (2006) concluded that her participants had an average of 8.5 accounts which required a password. Sasse et al. (2001) conducted a study of 144 participants and found that the average number of passwords was 16. Finally, participants in Dhamija and Perrig's study (2000) had between 10-50 accounts that required a password. The number of passwords is of concern because usability problems arise when users are forced to have a large number of passwords (Adams \& Sasse, 1999). Users cannot remember unique, random characters for each account that requires a password. User's select memorable passwords, which tend to be weak (Forget et al., 2007). It is recommended that password guidelines not exceed Miller's scale of $7 \pm 2$ items (Carstens et al., 2004).

Users have an increasing number of passwords to remember. This is compounded by additional factors, such as having to remember what password restrictions apply to each system. Added to this, users must remember their user IDs and the respective system for which the user ID and password validates them (Sasse et al., 2001). Additionally, users have to remember if they have changed a password. If the password has changed, the user must remember that new password (Sasse et al., 2001). An antagonizing factor is that passwords must be changed frequently. Users must memorize these passwords to ensure the security of the network (Wakefield, 2004). As the number of passwords and their complexity increase, the memory capacity of the user can become overloaded (Carstens et al., 2004). Carstens, et al. (2004) conducted a study that measured the impact users have on passwords. They surveyed over 250 participants in an attempt to determine if the number of passwords a person must remember affects the overall security of an information system. Their results showed that people who have 8-11 passwords to remember are at the greatest risk for not remembering them at least once per
month. Their results also showed that if a user selects a password that is meaningful, their ability to remember the password is greater than if the password does not contain meaningful data. Their research also indicated that workload and the number of required passwords work together to create weaknesses in the information system.

Memory limitations of users are another challenge facing authentication. Due to the constraints of memory, users select passwords with low entropy. This is because strong passwords are too hard to remember (Forget et al., 2007). Even with low entropy passwords, users still struggle to remember their passwords. Giovannini and Ensor (2006) state that users cannot remember their passwords. Users will devise various methods to recall their password, but a study by Gaw and Felton (2006) determined that user memory was the most common recall method.

Yan et al. (2004) stated that users inhibit the security of passwords as a result of their memory limitations. If users were not responsible for remembering passwords, maximum entropy could be achieved by using a character string as long as the system would allow. Additionally, the characters would be truly random.

The memory of users is limited. A study conducted by Miller (1956) found that a person may remember $7 \pm 2$ pieces of information. This is contradicted to a degree by Adams and Sasse (1999). They found that four or five passwords are the most that a user can be expected to remember. Furthermore, another study found the ability of a user to recall strong passwords to be impossibility. This is due to the inability of a user to find meaning in random characters (Sasse et al., 2001). Even when users remember a password, it could be the wrong password for the specific system. Brown et al. (2004) found that $22.5 \%$ of users confused their passwords.

Once a user selects a password, it is memorized for only a brief time. The amount of time between creating a password and using it is critical to being able to recall it accurately (Bunnell et al., 1997). Users lose the ability to recall passwords as time elapses. If enough time goes by, the user will lose access to the information (Ellison, Hall, Milbert, \& Schneier, 2000). Furthermore, if a person attempts to remember random pieces of information, the result is a reduction in short-term memory capacity (Carstens et al., 2004). A study conducted by Bersch (2000) found that only $35 \%$ of users could remember their passwords after three months, and only $23 \%$ of users could remember assigned passwords.

When permitted to select their own passwords, users choose passwords that have low entropy. Wu (1999) found that users are adept at selecting passwords that "are just good enough." Goldberg (2002) stated that password security "fails in practice because users select predictable passwords." Users are not completely to blame, though. Chiasson and Biddle (2007) found that, as a result of organizational password guidelines, users select unsafe passwords. These passwords are easy for them to remember. Kuo et al. (2006) determined that user selected password entropy is low because users seldom generate truly random passwords. In addition, Florencio and Herley (2007) confirmed the lack of password quality among users through their research.

Passwords with low entropy are a concern in information security. The selection of weak passwords can be almost as effective as not having a password at all (McDowell et al., 2009). A study conducted by Florencio \& Herley (2007) determined that most users choose passwords that contained lowercase letters only, unless they are required to do otherwise. Furthermore, Schchter, Brush, and Egelman (2009) ascertained that acquaintances were able to breach a user's
account $17 \%$ of the time. Feldmeirer and Karn (1989) state that long term password security will improve only if users increase the entropy of the passwords they select.

The reuse of passwords across multiple computer systems is another challenge facing user authentication. This practice can result in security weaknesses across multiple systems (Mulligan \& Elbirt, 2005). The propensity to reuse passwords has been researched and found to be widespread (Chiasson \& Biddle, 2007; Dhamija \& Perrig, 2000; Dhamija, Tygar, \& Hearst, 2006; Gaw \& Felton, 2006; Halderman, Waters, \& Felton, 2005; Wiedenbeck et al., 2005). Brown et al. (2004) even state that "almost all" users reuse passwords. This practice is unsafe because it makes it easier for a hacker to breach multiple accounts (Gaw\& Felton, 2006). This problem is escalating as users have increased the number of accounts that require passwords, but chose not to create new passwords (Gaw \& Felton, 2006). This is supported by research conducted by Florencio and Herley (2007). They state that the growing number of passwords per user is maintained by using a small number of passwords. The user has trouble remembering which five or six passwords were used for which account.

Users reuse passwords due to a variety of reasons. They may choose to reuse a password on a website because they do not know how often they will use the account. However, after a prolonged period of time, users would be burdened by choosing a unique password and having to remember which site used which password. The reuse of passwords replicates itself (Gaw \& Felton, 2006). In addition, users in the research study conducted by Gaw and Felton (2006) viewed the creation of new passwords as difficult. They do, however, understand that reusing passwords diminished information security.

The practice of reusing passwords has been studied to how prevalent the practice has become. Riley (2006) determined that $54.6 \%$ reuse passwords across multiple accounts "very
frequently" or "always." In another study conducted by Dhamija and Perrig (2000), participants had between 10 to 50 accounts that require a password, but only had one to seven unique passwords. Florencio and Herley (2007) found that the average password is used at approximately six websites. They also found that individual users had approximately 25 accounts that required passwords. In a study conducted by Brown et al. (2004), 218 participants used 844 unique passwords for 1471 different accounts. Although the number of password reuses varies across studies, research concludes that users do reuse their passwords.

The issue of users forgetting passwords is another concern regarding authentication. Based on research conducted by Sasse et al. (2001), user login attempts often fail for two reasons: First, the user remembered part of the password, but not all of it. The second reason is the user remembered a password for a different system or one that was replaced. The Power Law of Forgetting states that people experience an initial rapid rate of forgetting followed by a slow rate of forgetting over a long period of time. Essentially, a password that is not used regularly by a user is likely to be forgotten (Wiedenbeck et al., 2005). This is evidenced by several research studies. Florencio and Herley (2007) found that at least $1.5 \%$ of Yahoo users forget their passwords each month. Schechter et al. (2009) found that users forget their passwords $20 \%$ of the time. Swartz (2006) found that approximately $33 \%$ of users have forgotten their passwords. A study conducted by Brown et al. (2004) uncovered that passwords were forgotten by $31.1 \%$ of users. Research conducted by Bunnell et al. (1997), discovered that $30 \%$ of users could not remember assigned passwords. Finally, Armstrong (2003) revealed that 25-50\% of IT helpdesk calls are related to passwords. Armstrong's study concluded that, on average, a helpdesk will receive five calls per end-user per year.

Another problem facing authentication is the act of users writing down passwords. Research has determined that the majority of users write down their passwords (Chiasson \& Biddle, 2007; Dhamija \& Perrig, 2000; Wakefield, 2004; Wiedenbeck et al., 2005; Yan et al., 2004). Armstrong (2003) concluded that users make a choice of writing down their passwords or making the passwords weak. Users write down their passwords for convenience. Wakefield (2004) found that, because passwords must be changed frequently and memorized, users tend to write their passwords down in plain view or store them in a drawer. Another study found that the longer the password, the higher the probability that the user will write the password down or not be able to remember it (Held \& Bowers, 2001). Garrison (2008) conducted a study at a CPA conference. The session leader asked attendees to write their passwords down to determine their vulnerability. Only one person declined to write their password down.

A number of studies have been conducted to determine how many users write their passwords down. A study conducted by Riley (2006) discovered that $15 \%$ of users write down their passwords. Another study conducted by Horowitz (2001) found that up to $20 \%$ of users write their passwords down on a post-it note and stick it to their monitor. Carstens et al. (2004) determined that $27 \%$ of users write their passwords down on paper. Zviran and Haga (1999) found $35.3 \%$ of users write down their password. This is further supported by a study conducted by Brown et al. (2004). Their study showed that more than $50 \%$ of users write their passwords down. Adams and Sasse (1999) also determined that $50 \%$ of users write down their passwords. Rosencrance (2003) found a slightly higher percentage; this particular study concluded that 55\% of users write down at least one password. To make matters worse, Zviran and Haga (1999) determined that, when a user writes down their password, they do so in an unsafe location.

An additional obstacle facing authentication is the lengths to which users will go to avoid secure authentication procedures. Research has found that users will circumvent tedious authentication procedures (Yan et al., 2004). This is due to a variety of reasons. First, bypass if security keeps a user from performing a task, the user will circumvent the security measures or use them incorrectly (Adams \& Sasse, 1999; see also Bosworth \& Kabay, 2002; Chiasson et al., 2006; Mulligan \& Elbirt, 2005). A second reason users will bypass procedures is because security is not a primary task for users. The completion of their task is their primary focus, which means security is secondary (Forget et al., 2007). A third reason why users would violate existing password rules is when they must change a password immediately in order to continue working. A fourth reason is when users need access to a number of different computer systems that all require unique passwords (Sasse et al., 2001). Users employ a myriad of schemes to avoid authentication procedures. One method is the act of adding a character to the end of the password when using it across systems (Wiedenbeck et al., 2005). Another method is employed when users are forced to change their passwords. Most often, they want to change to the one used previously. If the system prohibits users from using their last few previous choices, users will change their passwords quickly to cycle back to their favorite password (Mulligan \& Elbirt, 2005; Yan et al., 2004). What users do not realize is that these seemingly innocent acts can unintentionally expose their employers to multiple security threats (SANS Top-20 2007 security risks, 2007).

## Password Management

Effective password management reduces the problems associated with text-based authentication. Specifically, the use of password management software will assist users in the selection of passwords with higher entropy than they have selected in the past. Password
managers are designed to assist the user by allowing them to select one master password, which grants access to their other passwords. This can result in an increase in usability and security since users are only responsible for one password (Chiasson \& Biddle, 2007). Password management software is designed to keep user passwords safe. These applications should diminish how much users write down their passwords. It also reduces password theft (Leon, 2008). Based on the principle of reduction, users should be motivated to utilize password managers, as they do not have to manage multiple passwords (Chiasson \& Biddle, 2007).

There are two categories of password managers. These are browser plug-ins and stand alone password management applications (Chiasson et al., 2006). Examples of browser plug-ins include PwdHash, Password Multiplier, and Passpet. Yee and Sitaker (2006) presented a new plug-in for logging into websites more securely. The tool, called Passpet, has not been made available to the public. Password Multiplier was proposed by Halderman et al. (2005). This plugin is designed to be a plug-in to the Mozilla Firefox Internet browser. Halderman et al. (2005) also proposed an additional plug-in password manager called Password Multiplier. They chose to make Password Multiplier an extension to a browser because most passwords will to be used to access web sites. Research concerning use of specific password management applications is scarce. However, Chiasson et al. (2006) conducted a study on two plug-in password managers. The plug-in password managers used by Chiasson et al. were PwdHash and Password Multiplier. The study results show that $96 \%$ of participants reuse passwords on different websites. The study also shows that users select passwords based on ease of recall (69\%) and being the same as another password already in use ( $62 \%$ ). The study indicated that users did care for not knowing their passwords. These specific password managers do not show the passwords to the user. Another category of password management software is the stand-alone password management
application. Examples of standalone password management software include Password Safe, AES software, and RoboForm (Leon, 2008). KeePass is another example. Out of these applications, KeePass is the only free open source password manager (KeePass).

User selected passwords presents challenges to the security of information systems. While research has been conducted on user-selected passwords, future research opportunities exist (Carstens et al., 2004). Wiedenbeck et al. (2005) state that authentication is "a critical area of security research and practice." Pinkas and Sander (2002) concur with Wiedenbeck in stating that the improvement of user-selected passwords is a "promising field of research." Particularly, the further study of password management is recommended in the literature. Sasse et al. (2001) recommend that investigation into the use of password management may help companies strengthen their passwords. Swartz (2006) states that businesses should determine a secure, viable solution for password management to help their employees. This is, Armstrong (2003) states, in part because saving time and money is a reason to look at password management. Even though the literature recommends research into password management, the impact of password management systems on password quality is unknown (Kuo et al., 2006).

Coupled with an investigation of password management, research supports further investigation into making users more aware of password entropy. Carstens et al. (2004) state that a level of user awareness must be obtained in order to reduce the potential for security breaches. Wakefield (2004) concurs with Carstens et al. regarding password policies. Wakefield states that employees should be educated on computer vulnerabilities. This is supported by HIPAA Section 164.308(a)(5)(i). This specific section addresses security awareness and training. The rule requires that "awareness and training be reasonable and appropriate"(Mulligan \& Elbirt, 2005). Unfortunately, organizations are not making their users aware of security issues. Bresz (2004)
states that security training is not widely used. Approximately $42 \%$ of companies spend less than one percent of their security budgets on awareness programs. Furthermore, $18 \%$ of organizations do not use awareness training (2008 CSI/FBI Computer Crime and Security Survey, 2008).

According to Armstrong (2003), users need to be trained on what constitutes a strong password. This is because password awareness efforts do affect user behavior (Kuo et al., 2006).

## CHAPTER 3

## METHODOLOGY

This chapter presents the methodology of the research experiment. This chapter describes the research design, ethical considerations, research participants, data collection and data analysis techniques.

## Experimental Design of the Study

This study was intended to answer research questions concerning techniques that individuals can implement to generate passwords that contain a higher entropy level and thus are more resistant to attack. Moreover, this study determined if the use of a password management application affected the entropy of user-selected passwords. In addition, this study determined if the entropy of user-selected passwords was influenced by awareness efforts when used in conjunction with a password management application.

The entropy of user-selected passwords was the focus of this study because of the effect users have on information system security. Research has shown that users are the weakest link in information security (Kim \& Bzullak, 2008). Specifically, passwords selected by users are a contributing factor humans are considered a weak element of an information system (Mulligan \& Elbirt, 2005). This is due to several reasons which include low user awareness concerning strong passwords (Chiasson \& Biddle, 2007), limited memory capacity (Miller, 1956), password reuse (Gaw \& Felton, 2006), and the conscious user circumvention of establish security procedures
(Bosworth \& Kabay, 2002). This study sought to determine if the use of a password management application caused an increase in the entropy of user-selected passwords. This study also determined if awareness efforts, when combined with the use of a password management application, affected the entropy of user-selected passwords.

The first research hypothesis was that the average password entropy would be increased when participants used a password management application. This hypothesis, and all subsequent hypotheses, were tested using an alpha level of 0.05 . This research hypothesis was tested by rejecting or failing to reject the following null hypothesis:
$\mathrm{H}_{0} 1$ - The average password entropy of participants that utilized a password management application will be equal to the average password entropy of participants that did not utilize a password management application.

Chiasson and Biddle (2007) asserted that the use of a password management would result in an increase of information security. This was supported by Sasse et al.'s study in which they recommended the use of password management techniques to strengthen passwords (2001).

The second research hypothesis was that an increase in the average password entropy of participants would occur when participants utilized a password management application and received verbal secondary information. This research hypothesis was tested by rejecting or failing to reject the following null hypothesis:
$\mathrm{H}_{0} 2$ - The average password entropy of participants that utilized a password management application and received verbal secondary information will be equal to the average password entropy of participants that did not utilize a password management application or receive verbal secondary information.

The SANS Institute stated that user awareness is a critical component in information security (SANS Top-20 2007 security risks, 2007). This was supported by Kuo et al.'s study (2006) in which they concluded that user awareness surrounding password entropy does affect user behavior. This hypothesis determined if verbal user awareness, when combined with the use of a password management application, affected the strength of user-selected passwords.

The third research hypothesis was that an increase in the average password entropy of participants would occur when participants utilized a password management application and received electronic secondary information. This research hypothesis was tested by rejecting or failing to reject the following null hypothesis:
$\mathrm{H}_{0} 3$ - The average password entropy of participants that utilized a password management application and received electronic secondary information will be equal to the average password entropy of participants that did not utilize a password management application or receive electronic secondary information.

The fourth research hypothesis was that an increase in the average password entropy of participants would occur when participants utilized a password management application, received verbal secondary information, and received electronic secondary information. This research hypothesis was tested by rejecting or failing to reject the following null hypothesis:
$\mathrm{H}_{0} 4$ - The average password entropy of participants that utilized a password management application, received verbal secondary information, and received electronic secondary information will be equal to the average password entropy of participants that did not utilize a password management application, receive verbal secondary information, or receive electronic secondary information.

## Ethical Considerations

Participants in this study were informed that their involvement in this research study was voluntary. Participants that elected to be a part of the research study were directed to an informed consent page on the website (Appendix A). Volunteers electing to participate in this study indicated their intent by clicking the appropriate link on the consent page. This consent page, along with this research study, was reviewed and approved by the Institutional Review Board at Indiana State University (Appendix B).

Research Participants
The participants in this study were student volunteers from two community colleges in North Carolina that require a computer placement exam prior to entrance into CIS 110. Catawba Valley Community College, located in Hickory, North Carolina, granted permission to the researcher to conduct this study at their institution (Appendix C). Cleveland Community College, located in Shelby, NC, granted permission to the researcher to conduct this study at their institution (Appendix D). This study had a sample population of 250 participants who were evenly distributed across the five groups. The research study was extracurricular to the instruction the participants were receiving. Additionally, there was no direct impact on their standing in their class because of their participation in this study. The use of student participants provided distinct advantages. The first advantage of using student volunteers enrolled in CIS 110 was the uniform computer knowledge they possess. Students chosen to participate possessed a consistent range of computer skills, which was evidenced by the successful completion of the computer placement test or remedial course. The computer placement tests at Catawba Valley Community College and Cleveland Community College do not contain information relating to passwords or the selection of passwords.

A second advantage of using student volunteers was the awareness they gained from participating in the study. Each participant had the opportunity to learn the results of the study. Regardless of the outcome of the study, participants were exposed to password management and the implications it has on password entropy.

## Data Collection and Analysis

It was necessary to use a methodology that allowed the researcher to test the impact of specific elements on password entropy. As a result, this study employed a posttest-only methodology. No pretest was administered, as the groups were assigned at random. Furthermore, a posttest-only design reduced the risk of the mortality effect.

This research study consisted of five steps. These steps included (a) the identification of research participants, (b) the random assignment of these participants into a treatment group or the non-treatment group, (c) the administration of the treatments to the respective groups, (d) the administration of the posttest to the groups, and (e) the analysis of the data.

The researcher collected demographic information of the study participants. This information included academic major, age, gender, and employment status. The participants were assigned a random number using the random number function in Excel. This random number placed the participant in a treatment group or the control group.

## Treatment

There were a total of four treatment groups and one control group in this study. Each group completed a short quiz about information security prior to the creation of all seven of their passwords. The first treatment group utilized the password management application only and took the quiz prior to the creation of all seven of their passwords. The second treatment group utilized the password management application and received verbal secondary information
(Appendix E). The second treatment group took the quiz after receiving verbal secondary information but before the creation of all seven of their passwords. The third treatment group utilized the password management application and received electronic secondary information (Appendix F).The third treatment group took the quiz after receiving the electronic secondary information but before the creation of all seven of their passwords. The fourth treatment group utilized the password management application and received both electronic secondary information and verbal secondary information. The fourth treatment group took the quiz after receiving the electronic secondary information and verbal secondary information but before they created all seven of their passwords. The control group did not make use of a password management application nor did they receive electronic secondary training or verbal secondary training. The control group took the quiz prior to the creation of all seven of their passwords.

## Posttest

All participants established passwords to gain access to seven different websites. These websites were developed by the researcher and provided participants with information regarding the importance of selecting passwords with high entropy levels. This study utilized seven websites as a result of Miller's (1956) research that determined users could remember seven items, plus or minus two. Participants who did not use the password management application received instructions that explained the process (Appendix G), but no information was provided concerning password strength. Participants who used the password management application received instructions that explained the process (Appendix H), but no information was provided concerning password strength. This was to ensure that users created passwords consistent with ones they would normally have created.

## Debriefing

The objective of this study was to answer research questions regarding methodologies users can employ to create passwords that contain a higher entropy level and are more resistant to attack. Furthermore, this study revealed whether the use of a password management application influenced the entropy of user-selected passwords. Finally, this study sought to determine if awareness efforts, combined with the use of password management software, influenced the entropy of user-selected passwords. The independent variables included: (a) the use of password management software, (b) the receipt of verbal secondary training, and (c) the delivery of electronic secondary training. The dependent variable was the entropy of passwords created by the participants.

The number of participants that received electronic secondary training was recorded, as was the number of participants that received verbal secondary training. Additionally, the number of study participants that received both direct and electronic secondary training was recorded. Finally, the number of participants that employed password management software was recorded.

## Data Analysis

The measurement of user-selected password entropy was based on the standard established by the National Institute of Standards and Technology (NIST). The NIST Electronic Authentication Guideline Special Publication 800-63 provides "technical guidance to Federal agencies implementing electronic authentication" (NIST Special Publication 800-63, 2006). The measurement of password entropy is the basis of this document and is the only widespread model of entropy measurement for user-selected passwords. Consequently, it has been used as the foundation for many private and government password policies (Weir, 2010) and has been utilized in research by Weir (2010), Helkala and Snekkenes (2009), and Boklan (2009).

Consequently, the entropy of passwords developed by participants in this research study was determined by the following model set forth by the NIST:

- The first character had an entropy value of 4 bits.
- The next seven characters had an entropy value of 2 bits per character.
- The ninth through the 20th character had an entropy value of 1.5 bits per character.
- Characters 21 and above had an entropy value of 1 bit per character.
- Six bits of entropy was assigned for passwords that contained both upper case and nonalphabetic characters.
- Six additional bits of entropy was added for an extensive dictionary check (NIST Special Publication 800-63, 2006).

The passwords that were developed by the participants were analyzed and the resulting entropy was calculated using Microsoft Excel.

Significance testing can result in a Type I error or a Type II error. Type I error rates "are almost always set at 0.05 or at $0.01 "$ (Lane, n.d.). Triola (2000) defines a Type I error as a mistake that occurs when the null hypothesis is rejected when it should actually be accepted. The symbol $\alpha$ is used to denote the probability of the occurrence of a Type I error. Triola defines a Type II error as the mistake that occurs when the null hypothesis is accepted when it should be rejected. This study used an alpha of 0.05 . By setting alpha at 0.05 , there was a five in one hundred chance that the null hypothesis was rejected when it should have been accepted. Maxwell and Delaney (1990) state that the Type I alpha level is set at 0.05 for general research. Given the type of study that was conducted, reducing the Type I error rate to 0.01 is not necessary. In the event a Type I error caused the researcher to come to false conclusions, these conclusions will not ultimately affect the creation of user passwords.

The null hypotheses were tested using a general linear model univariate procedure. Analyses of variance (ANOVA) are considered general linear procedures; the specific ANOVA to be used is considered univariate because the study will contain one dependent variable. For purposes of this research study, a one-way analysis of variance (ANOVA) was used to test the null hypotheses. A one-way ANOVA has advantages such as the ability to test multiple independent variables using one method and the ability to hold the Type I error rate at the desired level.

The Analyses of Variance procedure has assumptions that must be tested. Berenson and Levine (1996) and Hayden (2005) list three major assumptions in the analysis of variance:

1. Subjects are randomly selected from population
2. Normality
3. Homogeneity of variance.

Siegl and Morgan (1996) state the randomness assumption "is a fixed part of the experimental design, and usually nothing can be done once the data have been collected." The sample population was selected at random, thus addressing the randomness assumption. The second assumption, normality, was tested using descriptive statistics. In testing for normality, the mean, standard deviation, skewness, and kurtosis were generated. The third assumption, homogeneity of variance, was tested using Levene's Test of Equality of Error Variance.

## CHAPTER 4

## FINDINGS AND ANALYSIS OF DATA

Overview
The purpose of this research study was to test the impact of certain password management techniques on user-selected password strength. A total of 250 volunteers participated in this study.

Descriptive statistics were first calculated on the measures included in this study in order to describe the sample of respondents and to ensure the normality of the dependent variable, entropy, for the purposes of the ANOVA. Descriptive statistics were also calculated for entropy separately to present an initial picture of the differences in this measure. A one-way ANOVA was conducted to test whether significant differences in entropy were present. This analysis, along with the post-hoc analysis, serves to test the hypotheses included in this study.

## Descriptive Statistics

Initially, a series of descriptive statistics were conducted in order to ensure normality of the dependent variable, which is an assumption of ANOVA. The descriptive statistics also served to illustrate differences in the dependent variable of entropy and to summarize demographic information relating to the respondents included in this study.

Figure 1 presents the distribution of the dependent variable entropy. The normality of the dependent variable was examined, as it is an important assumption of analysis of variance. The
histogram presented in Figure 1 provides evidence of positive skew as well as leptokurtosis. Outliers are also indicated based on this histogram.


Figure 1. Entropy Histogram
Table 2 summarizes descriptive statistics relating to entropy. The mean value was found to be 28.741 with a standard deviation of 6.512 . The ratio of the measure of skewness and kurtosis to their associated standard errors was used to determine whether abnormally high or low skewness or kurtosis was present. With regard to skewness, this ratio was found to be 8.208 , which indicates very high positive skewness. Additionally, the calculation of this ratio in relation
to kurtosis was found to be 26.792, which illustrates extremely high leptokurtosis. These results demonstrate a strong degree of non-normality and suggest that measures be taken to normalize this measure before the use of the one-way ANOVA.

Table 2

Entropy Descriptive Statistics

| Measure | Actual Value | Normalized Value |
| :--- | :---: | :---: |
| Mean | 28.741 | 0.016 |
| Standard | 6.512 | 1.003 |
| Deviation |  |  |
|  |  |  |
| Skewness | 1.264 | -0.215 |
| Standard Error | 0.154 | 0.154 |
| Skewness / SE | 8.208 | -1.396 |
|  |  |  |
| Kurtosis | 8.225 | 0.215 |
| Standard Error | 0.307 | 0.307 |
| Kurtosis / SE | 26.792 | 0.700 |
| Note: $N=250$. |  |  |

In order to normalize the dependent measure of entropy, Johnson's family of transformations was applied to this measure. Figure 2 presents the histogram of this normalized measure, which portrays a high degree of normality.


Figure 2. Normalized Entropy Histogram
Table 2 presents descriptive statistics associated with this normalized measure. This measure was standardized to have a mean of approximately zero and a standard deviation of approximately one, while the ratios calculated for skewness and kurtosis were all below $|2.0|$, which indicates a high degree of normality. According to these results, this measure did not violate the normality assumption of ANOVA.

Descriptive statistics were then calculated for this normalized measure of entropy. As presented in Table 3, mean values for this measure varied fairly substantially based on condition. The lowest scores were found in the control group, while scores approximating the mean were
found in regard to the KeePass group, the KeePass and VSI group, and the KeePass and ESI group. Average scores that were approximately half a standard deviation above the mean were found in the final group, which included all three conditions. These results suggested that significant differences were likely present in entropy on the basis of condition.

Table 3
Normalized Entropy Descriptive Statistics by Condition

|  |  |  |  | 95\% Confidence Interval |  |
| :--- | :---: | :---: | :---: | :---: | :---: |
| Group | N | Mean | Standard <br> Deviation | Low | High |
| Control Group | 52 | -0.471 | 0.824 | -0.701 | -0.242 |
| KeePass | 62 | 0.003 | 1.168 | -0.294 | 0.299 |
| KeePass, VSI | 40 | 0.170 | 0.980 | -0.144 | 0.483 |
| KeePass, ESI | 51 | 0.061 | 0.921 | -0.199 | 0.320 |
| KeePass, VSI, |  |  |  |  |  |
| ESI | 45 | 0.408 | 0.860 | 0.149 | 0.666 |
| Total | 250 | 0.016 | 1.003 | -0.109 | 0.141 |

Next, a series of descriptive statistics were calculated on the demographic measures included in this study. First, Table 4 summarizes respondents in regard to college major. Slightly over $40 \%$ of respondents stated that they were transfer students, while approximately $10 \%$ of individuals stated that they major in business administration or computer information systems. Approximately 5\% of respondents were found to major in nursing, accounting, or office administration. A substantial number of additional majors were represented, but were not strongly represented in this sample. All majors of which two respondents or less were found to major in were collapsed into the "other" category as presented in Table 4.

Table 4
College Major

| College Major | N | $\%$ |
| :--- | :---: | :---: |
| College Transfer | 104 | $41.6 \%$ |
| Business Administration | 27 | $10.8 \%$ |
| Computer Information Systems | 25 | $10.0 \%$ |
| Nursing | 14 | $5.6 \%$ |
| Accounting | 11 | $4.4 \%$ |
| Office Administration | 11 | $4.4 \%$ |
| Early Childhood | 7 | $2.8 \%$ |
| Criminal Justice | 6 | $2.4 \%$ |
| Computer Programming | 5 | $2.0 \%$ |
| Networking | 4 | $1.6 \%$ |
| Health Care Management | 3 | $1.2 \%$ |
| Health Information Technology | 3 | $1.2 \%$ |
| Radiography | 3 | $1.2 \%$ |
| Other | 27 | $10.8 \%$ |

Table 5 presents the age demographic. As expected, the majority of respondents were found to be between the ages of 18 and 30 , with slightly over $12 \%$ of respondents being in their 30s. Less than $15 \%$ of respondents in total were over the age of 40 in this sample.

Table 5
Age of Respondents

| Age | N | $\%$ |
| :--- | :---: | :---: |
| $18-30$ | 185 | $74.00 \%$ |
| $31-40$ | 31 | $12.40 \%$ |
| $41-50$ | 21 | $8.40 \%$ |
| $51-60$ | 9 | $3.60 \%$ |
| $60+$ | 1 | $0.40 \%$ |
| Non-Response | 3 | $1.20 \%$ |

Next, the sample was very evenly split between males and females, as presented in Table
6.

Table 6
Gender of Respondents

| Gender | N | $\%$ |
| :--- | :---: | :---: |
| Female | 126 | 50.4 |
| Male | 124 | 49.6 |

Table 7 serves to summarize respondents in regard to employment status. Respondents were most commonly found to work part-time; a slightly smaller percentage of respondents indicated that they are not employed and are not collecting unemployment benefits. Nearly $17 \%$ of participants responded that they work full-time, with less than $10 \%$ of respondents indicating that they are unemployed and collecting unemployment benefits or declined to answer this question.

Table 7
Employment Status of Respondents

| Employment Status | N | $\%$ |
| :--- | :---: | :---: |
| Full time (More than 40 hours per week) | 42 | 16.8 |
| Part-time (less than 40 hours per week) | 96 | 38.4 |
| Not employed and collecting unemployment benefits | 21 | 8.4 |
| Not employed and not collecting unemployment benefits | 86 | 34.4 |
| Prefer not to answer | 5 | 2.0 |

## Data Analysis

As outlined in chapter three, participants completed a quiz as part of this study. This quiz was intended to demonstrate that the participants possessed a similar level of computer knowledge. An ANOVA was conducted on participant quiz scores in order to determine if the quiz scores significantly differed between the groups. As shown in Table 8, the ANOVA results reveal that statistical significance, $F(4,245)=0.489, p=0.744$, was not achieved. This indicates that the quiz scores did not significantly differ between the participant groups. The lack of significance may suggest that the participants did possess similar computer knowledge.

Table 8
Quiz Scores ANOVA

|  | Sum of | Mean |  |  |  |
| :--- | :---: | :---: | :---: | :---: | :---: |
|  | Squares | df | Square | F | P-value |
| Between Groups | 5.444 | 4 | 1.361 | 0.489 | 0.744 |
| Within Groups | 682.156 | 245 | 2.784 |  |  |
|  |  |  |  |  |  |
| Total | 687.600 | 249 |  |  |  |

An ANOVA was conducted in order to determine whether normalized measures of entropy significantly differ on the basis of condition. Table 9 presents Levene's test of the homogeneity of variance. As shown in the table, Levene's test did not find significant differences in variance in entropy on the basis of condition, $W(4,245)=1.509, p=0.200$. This means that the assumption of equal variances was not violated. Table 10 presents the results of the one-way analysis of variance. This was conducted comparing scores on entropy on the basis of condition; the results signify that statistical significance, $F(4,245)=5.400, p<.001, \eta^{2}=0.081$ was achieved. This illustrates that entropy significantly differs on the basis of condition. At an alpha
level of 0.05 , with the sample size of 250 , with five independent groups, the calculated power was found to be 0.976 , which shows a very high level of statistical power. Table 11 summarizes the post-hoc analyses conducted in order to further explore differences in entropy on the basis of condition. Specifically, Table 11 focuses on comparisons between the control group and the respective treatment groups. Tukey's HSD was utilized for this analysis. Finally, for purposes of clarity, Table 12 presents the entropy mean values prior to the application of Johnson's family of transformation.

Table 9
Test of Homogeneity of Variance

| Levene Statistic | df1 | df2 | Sig. |
| :---: | :---: | :---: | :---: |
| 1.509 | 4 | 245 | 0.2 |

Table 10
ANOVA for Entropy

|  | Sum of <br> Squares | df | Mean <br> Square | F | Sig. |
| :--- | :---: | :---: | :---: | :---: | :---: |
| Between Groups | 20.306 | 4 | 5.076 | 5.400 | 0.000 |
| Within Groups | 230.296 | 245 | 0.940 |  |  |
| Total | 250.602 | 249 |  |  |  |

Table 11
ANOVA: Post-Hoc Comparisons of the Control Group (Tukey's HSD)

| Comparison Group | Mean Difference $^{\text {a }}$ | Probability Level |
| :--- | :---: | :---: |
| KeePass | -0.474 | 0.074 |
| KeePass, VSI | -0.641 | 0.016 |
| KeePass, ESI | -0.532 | 0.046 |
| KeePass, VSI, ESI | -0.879 | $<0.001$ |

Notes: ${ }^{\text {a }}$ Calculated as Control Group minus Comparison Group.

Table 12
Non-Normalized Entropy Descriptive Statistics by Condition

| Group | N | Mean | Standard Deviation |
| :--- | :---: | :---: | :---: |
| Control Group | 52 | 25.850 | 4.346 |
| KeePass | 62 | 28.892 | 8.534 |
| KeePass, VSI | 40 | 29.402 | 6.101 |
| KeePass, ESI | 51 | 28.919 | 5.461 |
| KeePass, VSI, ESI | 45 | 31.086 | 5.855 |
| Total | 250 | 28.741 | 6.512 |

## Alternate Hypothesis $H_{1} 1$

The first research hypothesis was that the average password entropy of participants who use a password management application would exceed the average password entropy of participants who do not use a password management application. The mean entropy value of the treatment group $(M=28.892, S D=8.534)$ was found to exceed the mean entropy value of the control group $(M=25.850, S D=4.346)$. These results, however, were found to approach significance but were not statistically significant ( $p=0.074$ ). Therefore, alternate hypothesis $H_{1}$ lwas rejected.

## Alternate Hypothesis $H_{1} 2$

The second research hypothesis was that the average password entropy of participants who use a password management application and receive verbal secondary information would exceed the average password entropy of participants who do not use a password management application or receive verbal secondary information. The mean entropy value of the treatment group $(M=29.402, S D=6.101)$ was found to exceed the mean entropy value of the control group $(M=25.850, S D=4.346)$. Furthermore, these results were found to be statistically significant $(p=0.016)$. Therefore, the study failed to reject alternate hypothesis $H_{1} 2$. Alternate Hypothesis $H_{l} 3$

The third research hypothesis was that an increase in the average password entropy of participants would occur when participants utilized a password management application and received electronic secondary information when compared to participants who did not use a password management application and receive electronic secondary information. Higher entropy was found in the treatment group $(M=28.919, S D=5.461)$ when compared with the control group $(\mathrm{M}=25.850, \mathrm{SD}=4.346)$. These results were found to be significant $(p=0.046)$. Thus, the study failed to reject alternate hypothesis $H_{l} 3$.

## Alternate Hypothesis $H_{l} 4$

The fourth research hypothesis was that the average password entropy of participants who utilized a password management application, received verbal secondary information, and received electronic secondary information would exceed the average entropy of participants who did not use a password management application, receive verbal secondary information, and receive electronic secondary information. The mean entropy value for the treatment group ( $M=$ 31.086, $\mathrm{SD}=5.855$ ) exceeded the mean entropy value of the control group $(\mathrm{M}=25.850, \mathrm{SD}=$
4.346). The difference in entropy values was found to be statistically significant ( $p<0.001$ ). Hence, the study fails to rejects alternate hypothesis $H_{l} 4$.

The results of these analyses serve to strongly support alternate hypotheses $H_{l} 2, H_{l} 3$, and $H_{1} 4$ included in this study. Although alternate hypothesis $H_{l} 1$ was found to have a higher mean entropy value, it did not achieve significance and was therefore rejected.

## Conclusion

The respondents included in this sample were most commonly transfer students, with the majority of respondents being between the ages of 18 and 30 . Additionally, this sample was evenly split between male and female respondents. Regarding employment status, a large number of individuals were found to work part-time, with a smaller but similar percentage indicating that they were not currently employed and were not collecting unemployment benefits. A one-way analysis of variance was conducted on a normalized measure of entropy in order to determine whether significant group differences exist with regard to this measure. Significant differences were found on the basis of the $F$-statistic resulting from the analysis of variance, with Tukey's HSD utilized in the post-hoc analysis. All comparisons between the four treatment groups and the control group were found to have higher entropy levels. Three of the four treatment groups were found to be statistically significant. The KeePass treatment group was found to approach significance, but did not achieve the significance level set in this study.

## CHAPTER 5

## CONCLUSIONS AND RECOMMENDATIONS

## Discussion of Research Findings

The results from this research study indicate that the use of a password management application and efforts to increase user awareness did have an impact on the entropy of userselected passwords. The use of a password management application did result in a higher mean entropy of user-selected passwords; however, this particular finding did not meet the level of significance set forth in this study. The first research hypothesis predicted that the average password entropy of participants who use a password management application would be higher than the average password entropy of participants who do not use a password management application. Although those participants that used the password management application selected passwords with a higher mean, the mean difference was not found to be significant.

The use of a password management application combined with verbal secondary information did result in a significant increase in user-selected password entropy. The second research hypothesis predicted that the average password entropy of participants who use a password management application and receive verbal secondary information would be greater than the average password entropy of participants who do not use a password management application or receive verbal secondary information. A significant difference between the treatment group for research hypothesis two and the control group was determined.

The use of a password management application combined with the delivery of electronic secondary information did result in a significant increase in user-selected password entropy. The third research hypothesis predicted that an increase in user-selected password entropy would occur when participants utilized a password management application and received electronic secondary information when compared to participants who did not use a password management application and receive electronic secondary information. A significant difference between the treatment group for research hypothesis three and the control group was determined.

The use of a password management application combined with the delivery of electronic secondary information and verbal secondary information did result in a significant increase in user-selected password entropy. The fourth research hypothesis predicted that the average password entropy of participants who utilized a password management application, received verbal secondary information, and received electronic secondary information would be greater than the average entropy of participants who did not use a password management application, receive verbal secondary information, and receive electronic secondary information. A significant difference between the treatment group for research hypothesis four and the control group was determined.

A review of the literature reveals that this study further supports previous research conducted by others. Evidence has shown that users do not tend to select passwords with high entropy. This lack of entropy has been identified as a problem with user-selected passwords (St. Clair et al., 2006). Lack of entropy in passwords has been attributed to a combination of factors. These factors include memory limitations and user awareness. Though these constraints exist, computer system users today are required to use an increasing number of passwords (Chiasson \& Biddle, 2007).

Thorpe (2008) determined that even non-text based authentication schemes result in low entropy. Chiasson and Biddle (2007) conducted studies related to password managers and graphical passwords. Another study found password problems were related to the number of passwords a user must remember, the number of systems requiring passwords, and the complexity of the passwords (Carstens, McCauley-Bell, Malone, \& DeMara, 2004).

Chiasson and Biddle (2007) stated that password management software can result in an increase in usability and security since users are only responsible for one password. Furthermore, Kuo, Romanosky, \& Cranor (2006) relate that awareness efforts affect user behavior. Users who have a greater awareness of how to create a strong passwords use this information when creating their passwords.

Other research studies have also investigated the effect of making users more aware of password entropy. Carstens et al. (2004) express that a level of user awareness must be obtained in order to reduce the potential for security breaches. Wakefield (2004) concurs with Carstens et al. regarding password policies. Wakefield advocates that employees should be educated on computer vulnerabilities. This is supported by HIPAA Section 164.308(a)(5)(i). This specific section addresses security awareness and training (Mulligan \& Elbirt, 2005). According to Armstrong (2003), users need to be trained on what constitutes a strong password. This is because password awareness efforts do affect user behavior (Kuo et al., 2006).

## Implications

The results from this research show that the use of a password management application may contribute to an increase in the entropy of user-selected passwords. The results also signify that the entropy of user-selected passwords may be influenced by efforts to increase awareness in addition to use of a password management application. The field of technology management will
benefit from this study as it has provided insight as to what affects the entropy of user-selected passwords.

The implications of this study indicate that the use of a password management application without entropy awareness may not result in a significant increase in the strength of user-selected passwords. The use of a password management application when combined with some type of awareness was shown to significantly increase the strength of user-selected passwords. Organizations should recognize the need for user awareness and act appropriately to ensure this awareness is provided while also providing users with a password management system.

## Recommendations

There are a number of recommendations that may be made based upon the limitations of this research study. One limitation of this study was that it was time-limited. Future studies may explore the elements of this study for a longer duration of time to determine the impact it would have on a similar study. Another limitation of this study was that the participants possessed similar knowledge regarding password selection. Future studies may compare a user's knowledge of information systems and password strength to the respective entropy the users select. Yet another limitation of this study stated that the participant's primary language did not affect their ability to participate in this study. Follow up research may be conducted to determine if a user's primary language affects the selection of their passwords. Furthermore, research could be conducted to determine if the user's primary language affects the impact of awareness efforts.

Notwithstanding the recommendations made based on this study's limitations, recommendations on a broader scope may be made because of the findings of this study. This study was conducted using one password management application. Future research may wish to
use this study as a model but explore the impact a different password management application has on user-selected passwords. This research could begin to provide insight as to whether certain password management applications are more effective than others are. Building upon this recommendation, future research may also explore how users compare different password management applications. This future research may also wish to investigate which of the different types of password management applications are the most effective.

As noted in another recommendation for future research, this study was not longitudinal in nature. While future research may wish to investigate whether time is a factor when using password management software, additional research may wish to determine the persistence level of users employing password management applications. This research may indicate whether users continue to use a password management application after a period of time.

This research study introduced general awareness efforts to determine if they affected the entropy levels of user-selected passwords. While this study found that these awareness efforts were effective in increasing entropy levels, future research may work to determine what specific elements of awareness have an impact on users. Additionally, future research may determine the most effective mechanism for delivery of these awareness efforts.

## Summary

The security of information contained within computer systems poses challenges for users and administrators. This information is often protected by alphanumeric passwords. However, passwords continue to represent a major challenge to information security. Userselected passwords often lack entropy, which lessens the security of the information system A review of the literature discovered that alternatives to the alphanumeric password exist but do not seem to be replacing the traditional password. Strategies using alternatives to the text-based
password have been proposed, but have proven to be marginally effective. However, the literature shows that users choose passwords that contain low levels of entropy when left to select passwords with little guidance. Methods to increase the entropy levels of user-selected passwords are needed.

This research study used empirical research methods to determine if the use of a password management application would affect the entropy of user-selected passwords. Furthermore, this study sought to determine if awareness efforts affected user-selected password entropy when combined with use of the password management application.

The results from this research study indicated that the use of a password management application did result in a higher mean average of user-selected password entropy. This finding was not found to reach significance. This study further determined that the delivery of electronic and verbal secondary information, when combined with the password management application, did result in a significant higher mean entropy average. The implications from this study are that the use of a password management application combined with awareness efforts may result in stronger user-selected passwords. There are a number of recommendations that can be made from this study for future research.

## REFERENCES

2005 CSI/FBI Computer Crime and Security Survey. (2005). Retrieved June 20, 2009, from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf.

2008 Annual study: Cost of a Data Breach. (2008). Retrieved June 28, 2009, from http://www.encryptionreports.com/download/Ponemon_COB_2008_US_090201.pdf.

2008 CSI/FBI Computer Crime and Security Survey. (2008). Retrieved June 28, 2009, from http://i.zdnet.com/blogs/csisurvey2008.pdf.

Adams, A., \&Sasse, M. A. (1999, December). Users are not the enemy. Communications of the ACM, 42(12), 41-46.

Armstrong, I. (2003, June 1). Passwords exposed: Users are the weakest link. SC Magazine. Retrieved June 28, 2009, from http://www.scmagazineus.com/Passwords-exposed-Users-are-the-weakest-link/article/30394/.

Asonov, D., \& Agrawal, R. (2004). Keyboard acoustic emanations. Proceedings of the IEEE Symposium on Security and Privacy (pp. 3-11).

Belgers, W. (1993, December 6). UNIX Password Security. Retrieved July 1, 2009, from http://www.het.brown.edu/guide/UNIX-password-security.txt.

Bersch, C. (2000, February). Outdated, insecure passwords are losing money for Internet businesses. Communications News, 37(2), 10-11.

Berenson, M.L. \& Levine, D.M. (1996). Basic Business Statistics: Concepts and Applications (6 ${ }^{\text {th }}$ ed.). Englewood Cliffs, NJ: Prentice Hall.

Bigler, M. (2004). Single Sign-on. The Internal Auditor, 61(6), 31-34.
Boklan, K. D. (2009). Large key sizes and the security of password-based cryptography. International Journal of Information Security and Privacy, 3(1), 65-72.

Bosworth, S., \& Jacobson, R. V. (2002). Brief history and mission of information system security. In S. Bosworth \& M. E. Kabay (Eds.), Computer security handbook (pp. 1.1 1.13). New York: John Wiley \& Sons.

Bosworth, S., \& Kabay, M. (2002). Computer security handbook. New York: Wiley.
Bresz, F. P. (2004, July). People - often the weakest link in security, but one of the best places to start. Journal of Health Care Compliance, 6(4), 57-60.

Brostoff, S., \& Sasse, A. (2000). Are passfaces more usable than passwords? A field trial investigation. HCI 2000: Proceedings of people and computers XIV - Usability or else (pp. 405-424). Sunderland, U.K.: Springer.

Brown, A. S., Bracken, E., Zoccoli, S., \& Douglas, K. (2004, June). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641-651.

Bunnell, J., Podd, J., Henderson, R., Napier, R., \& Kennedy-Moffat, J. (1997). Cognitive, associative, and conventional passwords: Recall and guessing rates. Computers and Security, 16(7), 629-641.

Burr, W. E., Dodson, D. F., \& Polk, W. T. (2006). Electronic authentication guideline (National Institute of Standards and Technology No. 800-63). Gaithersburg, MD.

Oxid. Cain \& Abel. Retrieved August 8, 2009, from http://www.oxid.it/cain.html.
Canavan, J. E. (2001). Fundamentals of network security. Norwood, MA: Artech House, Inc.

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., \&DeMara, R. F. (2004, August). Evaluation of the human impact of password authentication practices on information security. Informing Science Journal, 7(1), 67-85.

CentralNic. (2001, July 13). Password clues, the CentralNic password survey report. Retrieved from https://www.centralnic.com/company/news/research.

Chiasson, S., \& Biddle, R. (2007). Issues in user authentication. CHI 2007 Workshop on Security User Studies. San Jose, CA.

Chiasson, S., Forget, A., Biddle, R., \& van Oorschot, P. (2007). Influencing users towards better passwords: Persuasive cued click-points (School of Computer Science No. TR-07-16). Carleton University: British Computer Society.

Chiasson, S., van Oorschot, P., \& Biddle, R. (2006). A usability study and critique of two password managers. Proceedings of the 15th USENIX Security Symposium. Vancouver, Canada.

Ciampa, M. (2008). Security + guide to network security fundamentals. Boston: Course Technology.

Conklin, W. A., White, G. B., Cothren, C., Williams, D., \& Davis, R. L. (2004). Principles of computer security: Security+ and beyond. Boston: McGraw-Hill.

Crawford, I. (1997). Marketing research and information systems. Rome: Food and Agricultural Organization of the United Nations.

Crowley, E. (2003). Information systems security curricular development. Conference on Information Technology Education (pp. 249-255). Lafayette, IN: ACM.

DeAlvare, A. (1998). A framework for password selection. Unix Security Workshop II. Portland, Oregon.

Dhamija, R., \& Perrig, A. (2000). Déjà Vu: A user study using images for authentication. Proceedings of the 9th conference on USENIX Security Symposium (Vol. 9). Denver, CO: USENIX.

Dhamija, R., Tygar, J. D., \& Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 581-590). Montreal, Quebec, Canada: ACM.

Elliott, R., Young, M. O., Collins, V. D., Frawley, D., \& Temares, M. L. (1991). Information security in higher education (Educause Center for Applied Research). Retrieved august 14, 2009, from http://net.educause.edu/ir/library/pdf/PUB3005.pdf.

Ellison, C., Hall, C., Milbert, R., \& Schneier, B. (2000, February). Protecting secret keys with personal entropy. Future Generation Computer Systems, 16(4), 311-318.

Evans, A., Martin, K., \& Poatsy, M. (2007). Technology in Action. Prentice-Hall.
Executive Office of the President. (2009, May). Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure. Retrieved August 16, 2009, from
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
Feldmeier, D. C., \&Karn, P. R. (1989, August 20-24). UNIX password security - Ten years later. Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology (pp. 44-63).

Florencio, D., Herley, C., \& Coskun, B. (2007). Proceedings of the 2nd USENIX Workshop on Hot Topics in Security. Boston: USENIX.

Florencio, D., Herley, C., \& Coskun, B. (2007). A large-scale study of web password habits. Proceeding of the 16th International World Wide Web Conference (pp. 657-666). Alberta, Canada.

Forget, A., Chiasson, S., \& Biddle, R. (2007). Persuasion as education for computer security. World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (E-Learn) (pp. 822-829). Quebec City, Quebec, Canada: AACE.

Frank, K., \& Charron, D. (2002, January). Protecting information on laptops, PDAs, and cell phones. Strategic Finance, 83(7), 24-29.

Garrison, C. P. (2008, May). An evaluation of passwords. CPA Journal, 78(5), 70-71.
Gaw, S., \& Felton, E. W. (2006). Password management strategies for online accounts. 2006 Symposium on Usable Privacy and Security (SOUPS) (Vol. 149, pp. 44-55). Pittsburgh, PA: ACM.

Giovannini, E., \& Ensor, B. (2006). Why half of Europe's net users don't bank online (Forrester Research).

Goldberg, J., Hagman, J., \& Sazawal, V. (2002). Doodling our way to better authentication. CHI '02 Extended Abstracts on Human Factors in Computing Systems (pp. 868-869). Minneapolis, Minnesota: ACM.

Halderman, J. A., Waters, B., \& Felton, E. W. (2005). A convenient method for securely managing passwords. Proceedings of the 14th International World Wide Web Conference (pp. 471-479). Chiba, Japan: ACM.

Harada, Y., \& Kuroki, K. (1996). A study on the attitude and behavior of computer network users regarding security administration. In Reports of National Research Institute of Police Science (pp. 21-33).

Hayden, M. (2004, June). Two-way and beyond ANOVA.
Heckle, R. R., \& Lutters, W. G. (2007). Privacy implications for single sign-on authentication in a hospital environment. Symposium on Usable Privacy and Security (SOUPS) 2007 (Vol. 229, pp. 173-174). Pittsburgh, PA: ACM.

Held, J. S., \& Bowers, J. (2001). Securing E-Business Applications and Communications. Virginia: CRC Press, Inc.

Helkala, K., \& Snekkenes, E. (2009). Formalizing the ranking of authentication products. Information Management and Computer Security, 17(1), 30-43.

Henry, P. T. (2007). Toward usable, robust memometric authentication: An evaluation of selected password generation assistance, College of Information, The Florida State University, 2007. Dissertation Abstracts International, 68.

Horowitz, A. S. (2001, July). Top 10 security mistakes. Computerworld. Retrieved July 1, 2009, from http://www.computerworld.com/s/article/61986/Top_10_Security_Mistakes.KeePass. Retrieved June 17, 2009, from http://keepass.info/.

Ives, B., Walsh, K. R., \& Schneider, H. (2004, April). The domino effect of password reuse. Communications of the ACM, 47(4), 75-78. Retrieved June 17, 2009, from Academic Search Premier Database.

Kim, E. B., \& Bzullak, M. (2008, November). Does enterprise size matter in achieving information security? Review of Business Research, 8(6), 41-49.

Klein, D. (1990). A survey of, and improvements to, password security. Proceedings of the USENLX Second Security Workshop. Portland, Oregon.

Kuo, C., Romanosky, S., \& Cranor, L. F. (2006). Human selection of mnemonic phrase-based passwords. Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS) (Vol. 149, pp. 67-78). Pittsburgh, PA: ACM.

Kyas, O. (1997). Internet Security: Risk Analysis, Strategies and Firewalls. London: Thomson Computer Press.

Lane, D. Type I and II errors. Retrieved October 30, 2005, from http://davidmlane.com/hyperstat/A18652.html.

Leon, J. F. (2008, May). Ten tips to combat cybercrime. The CPA Journal, 78(2), 6-11.
Maxwell, S., \& Delaney, H. (1990). Designing experiments and analyzing data: A model comparison perspective. Pacific Grove, CA: Brooks/Cole.

McDowell, M., Rafail, J., \& Hernan, S. (2009). Cyber Security Tip ST04-002. Retrieved June 17, 2009, from http://www.us-cert.gov/cas/tips/ST04-002.html.

Miller, G. (1956). The magical number seven, plus or minus two: Limits on our capacity for processing information. Psychological Review, 63, 81-87.

Morris, R., \& Thompson, K. (1979, November). Password security: A case history. Communications of the ACM, 22(11), 594-597.

Mulligan, J., \& Elbirt, A. (2005, May). Desktop security and usability trade-offs: An evaluation of password management systems. Information Systems Security, 14(2), 10-19.

Narayanan, A., \& Shmatikov, V. (2005). Fast dictionary attacks on passwords using time-space tradeoff. Proceedings of the 12th ACM Conference on Computer and Communications Security (pp. 364-372). Alexandria, VA: ACM.

Network dictionary. Information, computer and network security terms glossary and dictionary. Retrieved July 19, 2009, from http://www.networkdictionary.com/security/b.php.

National Institute of Standards and Technology. (2006, August). NIST Special Publication 80063. Retrieved June 24, 2009, from http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

Openwall Project. John the Ripper password cracker. Retrieved august 8, 2009, from http://www.openwall.com/john/.

Pinkas, B., \& Sander, T. (2002). Securing passwords against dictionary attacks. 9th ACM Conference on Computer and communications security (pp. 161-170). Washington, DC: ACM.

PricewaterhouseCoopers (2010). Information Security Breaches Survey 2010.
Retrieved June 10, 2010 from http://www.ukmediacentre.pwc.com/News-Releases/New-wave-of-security-breaches-hitting-UK-businesses-costing-them-billions-new-report-shows-e8d.aspxReisinger, D. (2007, July 16). 25th anniversary of the computer virus?

Not so fast. CNET. Retrieved August 15, 2009, from http://news.cnet.com/8301-13506_3-9745010-17.html.

Renaud, K. V. (2005). Evaluating authentication mechanisms. In L. Cranor\& S. Garfinkel (Eds.), Security and Usability (pp. 103-128). O'Reilly.

Riddle, B. L., Miron, M. S., \& Semo, J. A. (1989, November). Passwords in use in a university timesharing environment. Computers and Security, 83(7), 569-579.

Riley, S. (2006, February). Password security: What users know and what they actually do. Usability News, 8(1).

Rosenberg, R. S. (2004). The social impact of computers. Boston, MA: Elsevier Academic Press.

Rosencrance, L. (2003, August 8). Survey: Insecure passwords can be costly for companies. Computerworld. Retrieved July 1, 2009, from
http://www.computerworld.com/action/article.do?command=viewArticleBasic\&articleId $=83839$.

SANS Top-20 2007 security risks. (2007). Retrieved July 3, 2009, from http://www.sans.org/top20/2007/top20.pdf.

Sasse, M. A., Brostoff, S., \&Weirich, D. (2001, July). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122-131.

Schechter, S., Brush, A., \&Egelman, S. (2009). It's no secret: Measuring the security and reliability of authentication via 'secret' questions. Proceedings of the 5th Symposium on Usable Privacy and Security. Mountain View, California: ACM.

Shannon, C. E. (1949). A mathematical theory of communication. Bell System Technical Journal, 27, 379-423, 623-656.

Shay, R., \& Bertino, E. (2009). A comprehensive simulation tool for the analysis of password policies. International Journal of Information Security, 8(4), 275-289.

Shirey, R. (2000, May). Internet Security Glossary. Retrieved August 8, 2009, from http://tools.ietf.org/pdf/rfc2828.pdf.

Shostack, A., \& Syverson, P. (2004). What price privacy? (and why identity theft is about neither identity nor theft). In L. Camp \& S. Lewis (Eds.), Economics of Information Security (pp. 129-142). Norwell, MA: Kluwer Academic Publishers.

Siegel, A.F. \& Morgan, C.J. (1996). Statistics and Data Analysis: An Introduction. New York: John Wiley \& Sons, Inc.

Spafford, E. H. (1992, May). OPUS: Preventing weak password choices. Computers and Security, 11(3), 273-278.

St. Clair, L., Johansen, L., Enck, W. P., M., Traynor, P., McDaniel, P., \& Jaeger, T. (2006). Password exhaustion: Predicting the end of password usefulness. International Conference on Information Systems Security (Vol. 4332, pp. 37-55). Kolkata, India: Springer.

Summers, W. C., \& Bosworth, E. (2004). Password policy: The good, the bad, and the ugly. Winter International Symposium on Information and Communication Technologies. Cancun, Mexico.

Swartz, N. (2006, November). Password paralysis. The Information Management Journal, 40(6), 8.

Thorpe, J. (2008). On the predictability and security of user choice in passwords, School of Computer Science, Carleton University, 2008. Dissertation Abstracts International, 69.

Thorpe, J., \& van Oorschot, P. (2007). Human-seeded attacks and exploiting Hot-Spots in graphical passwords. 16th USENIX Security Symposium (pp. 103-118). Boston, MA.

Triola, M. (2000). Elementary statistics. New York, NY: Addison - Wesley.
Wagner, R. (2003). Windows password weaknesses could threaten your enterprise (Gartner, Inc. No. FT-20-6557). . Stamford, CT.

Wakefield, R. L. (2004, July). Network security and password policies. The CPA Journal, 74(7), 6, 8.

Weir, C. M. (2010). Using probabilistic techniques to aid in password cracking attacks. Unpublished doctoral dissertation, The Florida State University, Computer Science.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., \& Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. Symposium on Usable Privacy and Security (SOUPS) 2005 (Vol. 93, pp. 1-12). Pittsburgh, PA: ACM.

Wu, T. (1999). A real-world analysis of Kerberos password security. Proceedings of the Network and Distributed System Security Symposium. San Diego, CA: Internet Society.

Yan, J. J. (2001). A note on proactive password checking. Proceedings of the New Security Paradigms Workshop (NSPW) (pp. 127-135). Cloudcroft, New Mexico: ACM.

Yan, J., Blackwell, A., Anderson, R., \& Grant, A. (2004, September). Password memorability and security: Empirical results. IEEE Security and Privacy, 229(5), 25-31.

Yee, K., \& Sitaker, K. (2006). Passpet: Convenient password management and phishing protection. Symposium on Usable Privacy and Security (SOUPS) 2006 (Vol. 149, pp. 3243). Pittsburgh, PA.

Zhuang, L., Zhou, F., \& Tygar, J. D. (2005). Keyboard acoustic emanations revisited. Proceedings of the 12th ACM Conference on Computer and Communications Security (pp. 373-382). Alexandria, VA: ACM.

Zviran, M., \& Haga, W. J. (1999, Spring). Password security: An empirical study. Journal of Management Information Systems, 15(4), 161-185.

## APPENDIX A: INFORMED CONSENT PAGE


$\leftarrow \rightarrow C$ it $O$ mww.catawbavalleysurvey.com/agreemenththl \& \&

" $\square$ other booknarks

## Catawba Valley Community College

 Student Password Survey
## The Effect of Password Management on User-Selected Passwords

You are being invited to participate in a research study about password management. This research project is being conducted by Mr. John Enamait of Indiana State University. The objective of this research project is to attempt to understand whether the use of a password management application affects the strength of user-selected passwords. It is being conducted in multiple community colleges in North Carolina. The survey is being given to current CIS 110 students
There is minimal risk if you decide to participate in this research study, nor are there any costs for participating in the study. The information you provide will help understand how the use of a password management application affects the selection of passwords. The information collected may not benefit you directly, but what is learned from this study should provide general benefits to students, companies, colleges, and researchers.
If you choose to participate, do not type your name in any fields on the website. Nothing you say on the questionnaire will in any way influence your present or future status as a student at your college. The information you provide as a part of this study will be stored on a remote Internet server that is protected by a unique user name and password.
Your participation in this study is voluntary. If you agree to participate, there will be no future email contact as a result of participating in this study. If you have any questions or concerns about completing the questionnaire or about being in this study, you may contact me at (828) 292-9680 or at jenamait@gmail.com If you have any questions about your rights as a research subject, you may contact the Indiana State University Institutional Review Board (IRB) by mail at Indiana State University, Office of Sponsored Programs, Terre Haute, IN 47809, by phone at (812) 237--8217, or by e-mail at irb(0)indstate.edu.

I agree to participate
No; I do not wish to participate. Print This Page

## APPENDIX B: IRB EXEMPT STATUS LETTER

Incliana State
University
More.from day one.

Thank you for your submission of New Project materials for this research study. The Indiana State University Institutional Review Board has determined this project is EXEMPT FROM IRB REVIEW according to federal regulations (45 CFR 46). You do not need to submit continuation requests or a completion report. Should you need to make modifications to your protocol or informed consent forms that do not fall within the exempt categories, you will have to reapply to the IRB for review of your modified study.
Internet Research: You are using an internet platform to collect data on human subjects. Although your study is exempt from IRB review, ISU has specific policies about internet research that you should follow to the best of your ability and capability. Please review Section L. on Internet Research in the IRB Policy Manual.

Informed Consent: All ISU faculty, staff, and students conducting human subjects research within the "exempt" category are still ethically bound to follow the basic ethical principles of the Belmont Report a) respect for persons; 2) beneficence; and 3 ) justice. These three principles are best reflected in the practice of obtaining informed consent.

If you have any questions, please contact Thomas Steiger within IRBNet by clicking on the study title on the "My Projects" screen and the "Send Project Mail" button on the left side of the "New Project Message" screen. I wish you well in completing your study.

# APPENDIX C: CVCC PERMISSION LETTER 

```
Catawba
    Valley
commUNITY Colllege
```

Indiana State University Institutional Review Board
Erickson Hall, Room 511
Terre Haute, IN 47809-1902

Dear Institutional Review Board Committee
Please note that Mr. John Enamait, Indiana State University Doctoral Student, has the permission of Catawba Valley Community College to conduct research at our campus for his study, "The Effect of Password Management Procedures on the Entropy of User Selected Passwords."

Dr. Keith Mackie, Vice President of Instruction, will serve as the contact person who may provide
information regarding the appropriateness of this study for its population. Catawba Valley
Community College is pleased to make available the necessary capabilities for the completion of this
study.
If there are any questions, please contact my office.
Signed,


Dr. Garrett Hinshaw, President

# APPENDIX D: CCC PERMISSION LETTER 

Cleveland Community College
Acadernic: Programs

Indiana State Universiiy Institutional Review Porard
Erickson Hall, Room 511
Terre Haule, in 47803-19072

Dear Institulional Review Snard Committee

This letter is to confirm, Mr. jahn Ensmait, Indiana Sate University Doctorial Student, has permission Tom Cleveland Community College io Londuct researkh at our campus for his study.

As Vice President for Acacemic. Programs, I will senve as the collese's administrator far the purpose of answering questions that may arlse. Jonathan Davis, Department Chair far Carmpuler Technologies wil: serve as the cantect person for the study. Clevcland Community College is pleased to participate ia this s:ucy.

Ifou trave any questions, please let tre know
Sincerely,
Dr. 日eckysain
Yice Przsident for Academic 9ragrams

## APPENDIX E: VERBAL SECONDARY INFORMATION

$\begin{array}{r}\text { John D. Enamait } \\ \text { jenamait@cvcc.edu }\end{array}$
ASSMOROS

## The User!

- Users of information systems are considered to be the weakest link in information security (Kim and Bzullak, 2008).
- Users will either use the same password repeatedly or use passwords that are easy to remember.
- Users select passwords based on their name, family names, phone numbers, or movies.


## Compromised!

- Kuo et al. (2006) found that passwords are generally compromised in several ways:
- Guessing the password based on knowledge of the user;
- Social engineering;
- Shoulder surfing;
- Using cracking software, such as John the Ripper.


## How Long?

| Number of Possible <br> Characters <br> Combinations | Person Attempt Time | Computer Attempt <br> Time |  |
| :--- | :--- | :--- | :--- |
| 1 | 36 | 6 minutes | 0.000036 second |
| 2 | 1,300 | 4 hours | 0.00130 second |
| 3 | 47,000 | 6 days | 0.04 second |
| 4 | $1,700,000$ | 6 months | 2 seconds |
| 5 | $60,000,000$ | 20 years | 60 seconds |
| 10 | $3,700,000,000,000$ | $>999$ million years | 118 years |

## Attacks

- The number of attacks continue to rise
- 220 million data breaches occurred between January 10, 2005 and March 24, 2008
- Can result in identity theft, loss of personal information, or viruses.


## Strong Passwords?

- To create strong passwords, follow these guidelines:
- Passwords should not contain words that are commonly found in a dictionary (Frank and Charron, 2002)
- Passwords should not contain personal information (Garrison, 2008)
- Passwords should consist of a mix of upper- and lowercase letters. A combination of letters, numbers and symbols are recommended (Frank and Charron, 2002)
- Yan et al. (2004) also recommended that users should select passwords that contain numbers and special characters.
- Passwords should be eight or more characters long (Frank and Charron, 2002).


## Examples

- TbM\&htr1
- J3lly22Fish
- k38\#0J\$dA
- 9fiNgeRS

Questions?

## APPENDIX F: ELECTRONIC SECONDARY INFORMATION

## Catawba Valley Community College

 Student Password Survey
## Dear Student,

Thanks for agreeing to be part of the password strength survey. By participating in this study, you are helping determine what methods affect the creation of strong passwords.

Do you know that users are the weakest link in an information system? Research has shown that users have a variety of deficiencies, but selecting weak passwords is a primary weakness. Users often select passwords based on a small number of factors including their own names, family names, phone numbers, or movies. Furthermore, users often select passwords that only meet the minimum requirements needed by the computer system.

Unfortunately, there are a number of ways that hackers can use in an attempt to "crack" a password. These methods include dictionary attacks and brute force attacks. In a dictionary attack, a computer program tries to guess the password using words in the dictionary and other weak passwords. A brute force attack uses a computer program to try to break each character of the password.

The amount of time it takes to break a password depends on three variables. These are the password itself, the cracking algorithm, and the computer speed. As computer processing speed increases, the amount of time it takes to break a password is going to decrease. For example, a computer can break a five-character password in 60 seconds. However, it can take up to 118 years for a computer to break a 10 character long password.

When creating passwords that are strong, there are certain steps to follow. When developing passwords, users should:

- Avoid using words that are found in a dictionary.
- Use a combination of upper- and lower-case letters, numbers, and symbols
- Use eight or more characters

Using these steps can help users select passwords that are more resistant to attacks from hackers.
Please feel free to let me know if you have any questions. Be sure to include your name and CIS course and section number.

## Regards,

Mr. Enamait

## APPENDIX G: SURVEY INSTRUCTIONS FOR NON-KEEPASS PARTICIPANTS

1) Open an Internet Browser and go to:
www.catawbavalleysurvey.com
2) Read the first page and click the link to continue
3) Read the informed consent page carefully. If you agree with the information provided, click on the "I agree" link. If you do not agree with the information, click on the "I do not wish to participate" link.
4) The first (of seven) page asking that you create a password is presented. Enter a password in the field marked "Password \#1."
5) Re-type the password you selected in the field marked "Re-enter Password \#1."
6) Click on the submit button.
7) Read the information on the next web page. After reading the information, click on the link to continue.
8) The second (of seven) page asking that you create a password is presented. Enter a password in the field marked "Password \#2."
9) Re-type the password you selected in the field marked "Re-enter Password \#2."
10) Click on the submit button.
11) Read the information on the next web page. After reading the information, click on the link to continue.
12) The third page asking that you create a password is presented. Enter a password in the field marked "Password \#3."
13) Re-type the password you selected in the field marked "Re-enter Password \#3."
14) Click on the submit button.
15) Answer the demographic questions on the next page. Once you have answered the questions, click on the submit button.
16) The fourth page asking that you create a password is presented. Enter a password in the field marked "Password \#4."
17) Re-type the password you selected in the field marked "Re-enter Password \#4."
18) Click on the submit button.
19) Answer the remaining demographic questions on the next page. Once you have answered the questions, click on the submit button.
20) The fifth page asking that you create a password is presented. Enter a password in the field marked "Password \#5."
21) Re-type the password you selected in the field marked "Re-enter Password \#5."
22) Click on the submit button.
23) The next page has five questions to answer. Answer these questions to the best of your ability and click on the submit button when finished.
24) The sixth page asking that you create a password is presented. Enter a password in the field marked "Password \#6."
25) Re-type the password you selected in the field marked "Re-enter Password \#6."
26) Click on the submit button.
27) The next page has five more questions to answer. Answer these questions to the best of your ability and click on the submit button when finished.
28) The seventh page asking that you create a password is presented. Enter a password in the field marked "Password \#7."
29) Re-type the password you selected in the field marked "Re-enter Password \#7."
30) Click on the submit button.
31) The website will now prompt you to enter one of the passwords you have created. The screen will instruct you on which password to enter (password \#1, \#2, etc.). Enter the appropriate password in the field marked "Password \#X."
32) Re-type the password that the website has randomly asked for in the field marked "Re-enter Password \#X."
33) Click on the submit button.
34) The survey is now complete. Read the final web page and close the browser. Please return this packet to Mr. Enamait when you are finished. Thank you for your participation.

## APPENDIX H: SURVEY INSTRUCTIONS FOR PARTICIPANTS USING KEEPASS

This survey will prompt you to create passwords seven times. Between the creation of these passwords, you will read information on passwords, complete demographic information, and answer some general computer questions.

The last step of the survey is for you to re-enter one of the seven passwords you create. The survey will instruct you on which password to enter.

## KeePass Overview

You, like most people, now have many passwords they must remember. You may need a password for Windows, e-mail account(s), online passwords, etc. etc. etc. Keep in mind that should use different passwords for each account. If you use only one password everywhere and someone gets this password you could have a problem... A serious problem. The thief would have access to your e-mail account, website, etc. This could be devastating!

KeePass is a free password manager. It helps you to manage your passwords in a secure way. You can put all your passwords in one database that is locked with one master password. So you only have to remember one single master password! This allows you to create passwords that are much stronger since you no longer have to remember them all!

Survey Instructions

1) Insert the flash drive provided into a USB port on the computer. The flash drive provided to you contains the portable version of KeePass that may be stored on a flash drive.
2) View the flash drive contents by clicking on Open folder to view files.

3) Double click on KeePass icon.

4) Click on the "new" button in the upper left hand corner of KeePass.

5) Create a Master Password. The Master password is the only password that you have to remember! Once you have entered your master password, click the OK button.
6) Retype the Master Password. This confirms that you did not make an error when typing the password you selected as the Master password. After typing the Master Password, click the OK button.

7) Do not close KeePass. Open an Internet Browser and go to:
http://www.catawbavalleysurvey.com
8) Read the first page and click the link to continue

9) Read the informed consent page carefully. If you agree with the information provided, click the I agree to participate link. If you do not agree with the information, click the No; I do not wish to participate link. If you wish, you may print this page for your records by clicking the Print this page link.


## Catawba Valley Community College

 Student Password Survey
## The Effect of Password Management on User-Selected Passwords

You are being invited to participate in a research study about password management. This research project is being conducted by Mr. John Enamait of Indiana State University. The objective of this research project is to attempt to understand whether the use of a password management application affects the strength of user-selected passwords. It is being conducted in multiple community colleges in North Carolina. The survey is being given to current CIS 110 students.
There is minimal risk if you decide to participate in this research study, nor are there any costs for participating in the study. The information you provide will help understand how the use of a password management application affects the selection of passwords. The information collected may not benefit you directly, but what is learned from this study should provide general benefits to students, companies, colleges, and researchers.
If you choose to participate, do not type your name in any fields on the website. Nothing you say on the questionnaire will in any way influence your present or future status as a student at your college. The information you provide as a part of this study will be stored on a remote Internet server that is protected by a unique user name and password.
Your participation in this study is voluntary. If you agree to participate, there will be no future email contact as a result of participating in this study
If you have any questions or concerns about completing the questionnaire or about being in this study, you may contact me at (828) $292-9680$ or at jenamait@gmail. com If you have any questions about your rights as a research subject, you may contact the Indiana State University Institutional Review Board (IRB) by mail at Indiana State University, Office of Sponsored Programs. Terre Haute. IN 47809, by phone at (812) 237-8217, or by e-mail at irb@indstate.edu.

I agree to participate.
No. I do now wish to participate.
Print This Page
10) The first page asking that you create a password is now displayed (You will create a total of seven passwords). Copy the URL. You may do this by right clicking on the web address bar and selecting copy.

11) Without closing the Internet Browser, switch to KeePass. You may find the KeePass application on the task bar. If you do not see KeePass on the task bar, you should find a small KeePass icon (small blue padlock) in the Notification area shown here:

12) Click on the add entry button

13) Paste the URL into the $\boldsymbol{U} R L$ field by right-clicking in the box and selecting Paste.

14) Enter a title for this password. Be sure that it describes how the password is used.

15) Enter a password into the Password box. Re-enter the password into the Repeat box and click the OK button.

16) The screen should now similar to this:

17) Right click on the entry and select copy password.

18) Switch to the survey website and right click in the Password \#1 box. Click on the paste command. KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy the password again.


Please enter Password \#1 below.


## 19) Switch back to KeePass and copy Password \#1 again.

20) Switch back to the survey website and right click in the Re-enter Password \#1 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy the password again.

21) Click on the submit button.


Please enter Password \#1 below.

22) Read the information on the next web page. After reading the information, click on the link to continue.
23) Copy the URL. You may do this by right clicking on the web address bar and selecting copy.


25) Paste the URL into the $\boldsymbol{U R L}$ field by right-clicking in the box and selecting Paste.


27) Enter a password into the Password box. Re-enter the password into the Repeat box and click the $\boldsymbol{O K}$ button.

28) The screen should now look similar to this:

29) Right click on the new password entry and select copy password.

30) Switch to the survey website and right click in the Password \#2 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#2 again.


[^0]32) Switch back to the survey website and right click in the Re-enter Password \#2 field. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#2 again.

33) Click on the submit button.

34) Read the information on the next web page. After reading the information, click on the link to continue.
35) Copy the URL. You may do this by right clicking on the web address bar and selecting copy.

36) Switch to KeePass and click on the add entry button.

37) Paste the URL into the $\boldsymbol{U}$ RL field by right-clicking in the box and selecting Paste.

38) Enter a title for this password in the Title field. Be sure that it describes how the password is used.

39) Enter a password into the Password box. Re-enter the password into the Repeat box and click the $\boldsymbol{O K}$ button.

40) The screen should now look similar to the following:

41) Right click on the new password entry and select copy password.

42) Switch to the survey website and right click in the Password \#3 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#3 again.

43) Switch to KeePass and copy Password \#3 again.
44) Right click in the Re-enter Password \#3 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#3 again.

45) Click on the submit button.

Please enter Password \#3 below.

46) Answer the demographic questions on the next page. Once you have answered the questions, click on the submit button.
47) Copy the URL. You may do this by right clicking on the web address bar and selecting copy.

48) Switch to KeePass and click on the add entry button.

49) Paste the URL into the $\boldsymbol{U}$ RL field by right-clicking in the box and selecting Paste.

50) Enter a title for this password in the Title field. Be sure that it describes how the password is used.

51) Enter a password into the Password box. Re-enter the password into the Repeat box and click the $\boldsymbol{O K}$ button.

52) The screen should now look similar to the following:

53) Right click on the new password entry and select copy password.

54) Go back to the survey website and right click in the Password \#4 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#4 again.

55) Switch back to KeePass and copy Password \#4 again.

57) Click on the submit button.


Please enter Password \#4 below.

58) Read the information on the next web page. After reading the information, click on the link to continue.
59) Answer the demographic questions on the next page. Once you have answered the questions, click on the submit button.
60) Copy the URL. You may do this by right clicking on the web address bar and selecting copy.

61) Switch to KeePass and click on the add entry button.

62) Paste the URL into the $\boldsymbol{U} R L$ field by right-clicking in the box and selecting Paste.

63) Enter a title for this password in the Title field. Be sure that it describes how the password is used.

64) Enter a password into the Password box. Re-enter the password into the Repeat box and click the $\boldsymbol{O K}$ button.

65) The screen should now look similar to the following:

66) Right click on the new password entry and select copy password.

67) Switch to the survey website and right click in the Password \#5 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#5 again.

68) Switch back to KeePass and copy Password \#5 again.
69) Right click in the Re-enter Password \#5 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#5 again.

70) Click on the submit button.


Please enter Password \#5 below.

71) The next page has five questions to answer. Answer these questions to the best of your ability and click on the submit button when finished.
72) Copy the URL. You may do this by right clicking on the web address bar and selecting copy.


74) Paste the URL into the URL field by right-clicking in the box and selecting Paste.

75) Enter a title for this password in the Title field. Be sure that it describes how the password is used.

76) Enter a password into the Password box. Re-enter the password into the Repeat box and click the $\boldsymbol{O K}$ button.

77) The screen should now look similar to the following:

78) Right click on the new password entry and select copy password.

79) Switch to the survey website and right click in the Password \#6 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#6 again.

80) Switch to KeePass and copy Password \#6 again.
81) Right click in the Re-enter Password \#6 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#6 again.

82) Click on the submit button.


Please enter Password \#6 below.

83) Read the information on the next web page. After reading the information, click on the link to continue.
84) The next page has five questions to answer. Answer these questions to the best of your ability and click on the submit button when finished.
85) Copy the URL. You may do this by right clicking on the web address bar and selecting copy.

86) Switch to KeePass and click on the add entry button.

87) Paste the URL into the URL field by right-clicking in the box and selecting Paste.

88) Enter a title for this password in the Title field. Be sure that it describes how the password is used.

89) Enter a password into the Password box. Re-enter the password into the Repeat box and click the $\boldsymbol{O K}$ button.

90) The screen should now look similar to the following:

91) Right click on the new password entry and select copy password.

92) Switch to the survey website and right click in the Password \#7 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#7 again.

93) Switch to KeePass and copy Password \#7 again.
94) Switch back to the survey website and right click in the Re-enter Password \#7 box. Click on the paste command. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#7 again.

95) Click on the submit button.

96) The website will now prompt you to enter one of the passwords you have created. The screen will instruct you on which password to enter (password \#1, \#2, \#3, etc.). The screenshots that follow are based on the assumption that the survey is requesting password \#4.
97) Switch to KeePass and right click over the appropriate password. Notice how when Password \#4 is right-clicked, the entry is highlighted in blue. Click on the copy password command.

98) Switch to the survey website and right click in the Password \#: box.

99) Switch back to KeePass and copy the respective password again.
100) Switch back to the survey website and right click in the Re-enter Password \#: box to Reenter the password. Click on the paste command to paste the password. Remember, KeePass allows up to 10 seconds to paste the password. After 10 seconds, you can no longer paste the password. If the paste command is not available, switch back to KeePass and copy password \#2 again.


102) The survey is now complete. Read the final web page and close the browser. You may now close KeePass. If KeePass asks you to save the database, select "discard all changes". Remove the flash drive from the computer. Please return this packet and the flash drive to Mr. Enamait when you are finished. Thank you for your participation.


[^0]:    31) Switch back to KeePass and copy Password \#2 again.
