3-2005

Passwords: A Survey on Usage and Policy

Kurt W. Martinson

PASSWORDS: A SURVEY ON USAGE AND POLICY

THESIS

Kurt W. Martinson, First Lieutenant, USAF

AFIT/GIR/ENV/05M-11

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

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

AFIT/GIR/ENV/05M-11

PASSWORDS: A SURVEY ON USAGE AND POLICY

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Kurt W. Martinson, BS

First Lieutenant, USAF

March 2005

AFIT/GIR/ENV/05M-11

PASSWORDS: A SURVEY ON USAGE AND POLICY

Kurt W. Martinson, BS
First Lieutenant, USAF

Approved:

/signed/	15 March 2005
Dennis D. Strouble (Chairman)	date
/signed/	16 March 2005
Alan R. Heminger (Member)	date
/signed/	15 March 2005
David D. Bouvin (Member)	date

Abstract

Computer password use is on the rise. Passwords have become one of the primary authentication methods used today. It is because of their high use that organizations have started to place parameters on passwords. Are password restrictions a nuisance? What are some of the consequences that result as organizations place the burden of their computer security on passwords?

This thesis is an analysis of a survey instrument used to identify if individuals are using similar techniques or patterns when choosing or remembering their passwords. It also looks at how individuals feel about using passwords. Additionally, we examine the literature to determine the importance of choosing strong passwords.

This study reveals some critical issues associated with password choice. Many respondents feel that organizational parameters are a nuisance and many are still writing passwords down. In addition, the survey shows that over 70% of respondents remember more than five passwords. We see a need for organizations to minimize the number of passwords individuals must remember. We also found that many individuals are using the same password for multiple applications. Finally, we discovered that the intent of password policy is not being followed. Overlooking these findings is a serious threat to the future of computer security.

Acknowledgements

I would like to express my gratitude to my thesis advisor, Dr. Dennis Strouble, for his assistance, support and encouragement. I am also indebted to my mother, father and sister, for their support and patience during this effort.

Kurt W. Martinson

Table of Contents

Page

Page

List of Figures

Figure Page

List of Tables

Table Page

PASSWORDS: A SURVEY ON USAGE AND POLICY

I. Introduction

Overview

Reliability and confidentiality of information systems is critical to an organization's success. One of the most common control mechanisms for authenticating an individual's access into information systems is the use of computer passwords. In the 1980's, it was common to recommend polysyllabic dictionary words as passwords (Garfinkel & Spafford, 1991), but older techniques are no longer providing the security most systems need. Password-cracking tools are faster and more readily available. Therefore, the best defense to avoid compromising security is the use of strong passwords (Kruck, Scianddra, & Forcht, 2001). A strong password is complex. A strong password contains at least eight characters, includes a combination of letters, numbers, and symbols and is easy for one to remember, but difficult for others to guess (Microsoft Corporation, 2004).

Yet the characteristics of strong passwords are often hard to remember because they are so often very complex. Human beings need ways to remember passwords without having to write them down. Because passwords are so heavily used today in authentication, users may choose passwords that are easy to remember and therefore easier to crack. Aware of these facts, organizations have created distinct parameters that

users must follow when creating passwords. To date, research on password security has focused on designing technical mechanisms to protect access to systems (Adams & Sasse, 1999) but the research investigating the usability and security of these mechanisms is rare. Hitchings, Davis and Price argue that parameters in place to protect systems have produced security mechanisms that are, in practice, less effective (Hitchings, 1995; Davis & Price, 1987).

Devising strong passwords has become difficult. The universe (number of possible combinations) of strong passwords is enormous, yet systems and organizations require users meet a certain criteria when choosing computer passwords. As a result, persons may be limiting this universe to aid in password memorization. How well are users choosing their passwords based on organizational guidance and policy?

Problem Statement

Administrators demand strong passwords, while users demand passwords that are easy to remember. Strong passwords have certain criteria and the emphasis placed on creating strong and secure passwords leads to numerous problems. Therefore, requiring individuals to create strong passwords may in fact make organizations less secure, not more.

Research Question

If users are not following the policy related to the proper use of strong and secure passwords, do password policies give organizations and users a false sense of security?

Purpose Statement

The purpose of this research is to find out whether or not individuals are following the current guidance of password usage. Password parameters established by

organizations effect human behavior and this behavior leads to insecure practices related to passwords and computer systems. For example, current guidance states that individuals should not write their password down and should use different passwords for different systems. According to one study, 50% of questionnaire respondents wrote their passwords down in one form or another (Adams & Sasse, 1999). This research will seek to validate this. It will also try to capture how people are remembering their passwords and if they use the same passwords for multiple applications. The research will focus on password usage to the extent of asking people their methods of password memorization. The research would also like to capture the passwords of individuals if it can. The investigative questions try to interpret the nature of password usage and seek to understand some problems that exist with password policy.

Method

Individuals that use computer passwords on a regular basis will attempt to answer these investigative questions in the form of a web-survey (Appendix B). A pretest will review the survey's readability and give participants an opportunity to explain to the researchers any unclear or confusing questions. The survey should identify methods individuals use to choose passwords as well as capture the perceptions of organizational parameters and constraints on computer passwords. This research will compare responses from individuals and use frequency of responses and histograms to present a majority of the data. This research will be a quantitative in nature with the data collected through a web-based survey instrument. One group will be used, a military sample, both officer and enlisted. The subjects taking the survey must all use passwords in either their work or in their personal time. We plan to conduct the research at the Air Force Institute

of Technology (AFIT) using a web-based survey. The survey is voluntary and only those in the military will participate. The final survey instrument is found in Appendix B.

Limitations

This research focuses on those individuals who use passwords for their job or for access to personal information systems, like e-mail and internet web pages. A reasonable sample size is critical so that we are able to make inferences about the population in general.

Research Hypotheses

1) Individuals are not following the current guidance for developing strong passwords. Many individuals are following the current guidance for developing strong passwords, but the manner in which they choose those passwords has a distinct pattern.
2) Individuals are developing ways to remember their passwords that are not secure, either through writing down their passwords or using a pattern on the keyboard for example.
3) Individuals are using the same passwords for multiple applications.

Overview

Background information, collected through a brief literature review, addresses the issue of passwords and password vulnerabilities. The goal of the survey instrument is two fold, to interpret the data, and evaluate the results. An analysis of the results will distinguish the characteristics that individuals use to choose passwords. Coding will allow us to calculate the frequency of responses in different categories. The use of tables

and graphs will be a way of representing this data is a clear, concise and organized fashion.

Anticipated Results/Significance

Organizations place a heavy burden on users to choose secure yet memorable passwords. The findings of this research will help explain how people use and remember passwords. The research may find that people are not following the rules set forth by the organization. The research may also find that people are following the rules, but the manner in which they do does not follow the overall intent of the rules. The research may also show that password usage is still a problem and it may serve as further awareness to both organizations and individuals. The results will include the following: description of the facts relating to password usage, description of the data that we collected, and a discussion of the patterns that we found. Finally, the research will tie its findings into the big picture of passwords as authentication and we may have to give recommendations for better ways of authentication.

Thesis Overview

Chapter 1 contains subject matter background and a brief description of the study. Chapter 2 contains a brief review of the history and background of computer password usage, as well as some of the threats directed at computer passwords. Chapter 3 discusses the research methodology used in this study, provides descriptive information of the data gathered, an analysis of the collected data, and the findings from this survey. Chapter 4 provides discussions, conclusions, recommendations, and suggestions for further research.

II. Background

For many years, the security of computer systems has relied on passwords (Kruck, Scianddra, & Forcht, 2001). Traditionally, authentication procedures divide into two stages: identification (User ID), to identify the user; and authentication, to verify that the user is the legitimate owner of the ID (Adams & Sasse, 1999). It is the second stage that requires a password. To date, research on password security has focused on designing technical mechanisms to protect access to systems but the usability and security of these mechanisms has rarely been investigated (Adams & Sasse, 1999). Hitchings and Davis and Price argue that parameters in place to protect systems have produced security mechanisms that are, in practice, less effective (Hitchings, 1995; Davis & Price, 1987). In addition, since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design (Adams & Sasse, 1999).

Computer Security

Securing information systems is a major issue with organizations. Every year hackers illegally access thousands of computers because of weak passwords (National Infrastructure Protection Center, 2001). Over time, passwords have become easier to crack for many reasons. Password cracking tools are becoming faster and more readily available, thus the need for stronger passwords are necessary (Spafford, 1992). Computer intruders, judging from a survey conducted by the FBI and reported by the Associated Press in April of 2002 (Mitnick, 2002), have attacked nine out of every ten large corporations and government agencies. A compromised password may lead to fraud, illegal activities, unauthorized transactions, or public disclosure of private

information (Wakefield, 2004). Having information like a password, is like "having keys to the kingdom" (Mitnick, 2002) and an attacker can move freely around and find the treasure they seek.

Password Vulnerabilities

Selecting strong passwords enhances the security by reducing the chance an attacker will find the password by trial and error, dictionary attack, or brute force attack (Mitnick, 2002). Problems such as dictionary attacks, brute force attacks and social engineering are some of the methods used to break passwords.

Dictionary Attacks and Brute Force

The National Infrastructure Protection Center (NIPC) has identified numerous ways hackers will try to infiltrate a computer system. The first passwords an intruder will try are the simple, commonly used words found in a dictionary. Another thing a hacker will attempt to do against a system is run a program that will attempt to guess the correct password on a computer. These programs can contain entire dictionaries from several different languages. In addition to words found in dictionaries, these programs often contain words from popular culture such as science fiction movies and novels.

NIPC also suggests that hackers are also aided because users "have a tendency to keep the same password for a long period of time, thereby allowing the attacker that much more time to gain access to a system" (National Infrastructure Protection Center, 2001). Because of these threats, many organizations demand complex passwords, some randomly generated, and require users to change them regularly. However, an even more dangerous approach to gain access to a person's password is through attack on people's weaknesses.

Social Engineering

Protecting passwords is a dangerous game. Using social engineering, hackers are able to appeal to emotion or weakness while tricking the people into giving away information. Many use deceptive techniques to gain access to information, particularly, computer passwords. In Kevin Mitnick's book, "The Art of Deception," he argues that most attacks do not focus on the technology, but on the weakness of the human component (Mitnick, 2002). In many social engineering attacks, the hacker poses as a member of the company's tech-support department and asks new employees for their passwords (Experts, 2005). This illustrates why an understanding of a company's security policy is so important. If *people* do not understand the importance of security, then they place an entire organization at risk. Hence, one should ever share a password with anyone. No matter how advanced the computer system and its security, organizations will always face strategies and methods of the social engineer.

Individuals must constantly be vigilant and aware of their surroundings. If a person is shoulder surfing, or watching someone type on a keyboard from behind, there is a risk of compromising a password. Ways in which unauthorized individuals are gaining access to passwords has become quite mischievous.

Another common technique that hackers use is something called phishing. Microsoft warns its users "to make sure you visit Web sites by entering the Web address into your browser or by using your Favorites link, as opposed to clicking the link in a suspect e-mail" (Microsoft, 2004). Phishing refers to putting a link in a fake e-mail that appears to go to a popular site, but actually takes an individual to an unofficial site that looks exactly like the official site. Once the hacker has convinced unsuspecting users

that they are at the official site, they will try to lure them into entering passwords, credit card numbers, and other sensitive information. Importance should not only be placed on protecting passwords, but also staying alert to the latest news on potential threats that target computer users. Part of staying alert is maintaining strong passwords.

Strong Passwords

In the 1980's, it was common to recommend polysyllabic dictionary words as passwords, but that is no longer prudent (Garfinkel & Spafford, 1991). The United States Federal Information Processing Standards suggest several criteria for assuring different levels of password security: 1) password composition, 2) password lifetime, and 3) password ownership (FIPS, 1985). With respect to password composition, the following rules *were* typical:

> "A good password has both upper and lower case letters, has digits and punctuation characters as well as letters, is easy to remember, so it does not have to be written down, is seven or eight characters long, and can be typed quickly so someone else cannot look over your shoulder" (Garfinkel & Spafford, 1991).

More recent and specific advice is available from the National Infrastructure Protection Center states:

> "Remembering long passwords can be difficult, but there are some basic techniques users can employ to lessen the pain. First, choose a phrase that you will remember. As an example, we will use the phrase "The pearl in the river." You can then take a number that you are familiar with, such as a birthday. For this example we will use 7/4/01. Next, you can take the first letter of your phrase and interlace it with the chosen date to make something similar to t7p4i0t1r. This method creates a password that won't be found in any dictionary and is unique to the person who created it" (National Infrastructure Protection Center, 2001).

Organizations normally ask users to adhere to the following requirements:

Passwords must be at least eight characters long, contain at least one number, one symbol, one lowercase letter, one upper-case letter. Yet a password should not contain

any word in the dictionary (in any language), any word related to family, hobbies, work, vehicle, license plate, address, social security number, telephone number, pet's name, or birthdates (Mitnick, 2002). Many times organizations require that computer passwords not be a variation of previously used passwords. The United States Air Force instructs its personnel to comply with all the above (Department of the Air Force, 2004). The theory is that if a user follows the parameters listed above, it will be hard for attackers to guess the password. In a study done at Cambridge University, researchers found that passwords based on mnemonic phrases, like passphrases, are just as hard to crack as randomly generated passwords (Yan, Blackwell, Anderson and Grant, 2000). Their study also demonstrates that by creating simple, usable instructions with clear examples, password compliance in an organization could increase. However, many password users do not comply with these suggested rules. In an attempt to make the password easier to remember, individuals often link their password to something that is familiar to them. To combat this, more and more organizations are becoming increasingly vigilant about enforcing security policies through technical means (Mitnick, 2002). These "technical means" translate into parameters that could be seen as burdensome.

Some Parameters

Organizations place a heavy burden on users to choose secure yet memorable passwords. Devising strong passwords has become difficult because many administrators demand password complexity, strong passwords, while users demand password simplicity, easy to remember passwords. As a result, organizations have created distinct parameters that users must follow. These parameters include certain password lengths, numbers, and special characters. Other parameters prohibit certain characters in

passwords. Time parameters are also enforced. As a result, studies have found that users with many different passwords, that frequently change, feel forced to write them down (Gehringer, 2002) and that having a large number of passwords reduces their memorability and increases insecure work practices. Common advice to improve password management includes monitoring failed login attempts, changing passwords regularly, and avoiding easily guessed passwords (Neumann, 1994). The only defense is to make passwords nearly impossible to guess. This would require users to generate passwords in a seemingly random fashion.

Need for Multiple Passwords

It only takes a single website with minimum-security requirements to disclose passwords to an attacker. Requiring users to have a large number of passwords, for multiple applications, was found to create serious usability problems (Adams & Sasse, 1999). Furthermore, Adams and Sasse found that usability problems reduce the overall password security in an organization. Their research also found that users required to change their passwords frequently produce less secure passwords (because they have to be more memorable) and disclose their passwords more frequently. Many of the users felt forced into these circumventing procedures, which subsequently decreased their own security motivation (Adams & Sasse, 1999). Memorization is also complicated because different systems require different passwords. The lack of common standards for passwords makes it difficult for a user to remember which password to use for different systems or applications. Adding to the problem are systems that frequently revoke a user's access after a password has been incorrectly entered as few as three times (Gehringer, 2002). Therefore, there are compromises between user memorability and

security of a system. Conventional and reusable computer passwords may seem convenient, but they are also dangerous (Neumann, 1994).

How Many Password Should You Have

There is conflicting advice on this topic. One might think that having one strong password should be good for all logins. As the number of passwords one must remembers increases, the likelihood of writing down those passwords increases. If one were to have only one password, this might solve the problem. Yet, if this is the case, once compromised, an intruder has access to all of the accounts. So maybe a different password should be used for different areas of one's life, like work, home, shopping, and finance. Multiple passwords lessen the impact if one is compromised, but a serious problem is that users have many systems they now must keep track of. Different organizations require different combinations of passwords. These mixed authentication formats only add to the complications of trying to choose a strong password.

Individual Password Choice

Password selection is the most vital step in computer security and yet human fallibility makes it nearly impossible to follow all of the recommended rules simultaneously (Gehringer, 2002). "It never ceases to amaze me that when people choose their passwords, their creativity and imagination seem to disappear" (Mitnick, 2002). Passwords that people choose are normally composed of meaningful information, such as a name of a person or a sequence of numbers such as birth-date (Beedenbender, 1990; Gehringer, 2002). Other examples of meaningful information are names of people, places, pets, or other common items. Any person attempting to gain unauthorized access to a system might need only to look at a personnel record or associate with the person

holding the desired password in order to discover the password (Beedenbender, 1990). Where people have shown themselves to be inventive regarding passwords, is in finding ways to make complex passwords that have some sort of pattern.

There is evidence that many password users do not comply with the suggested rules. DeAlvare found that a user's knowledge of what constitutes secure password content (the character content of the password) was inadequate and once a password is chosen, a user is unlikely to change it until it has been shown to be compromised (DeAlvare, 1998). Adams and Sasse identified that unless there is feedback from security experts, users create their own rules on password design and they were often anything but secure (Adams & Sasse, 1999). Restrictions introduced to create more secure password content may produce less memorable passwords, leading to increased password disclosure, writing them down or having to call a help desk to retrieve a forgotten password (Adams & Sasse, 1999). Users, on the other hand, perceive many security mechanisms as laborious and unnecessary. Passwords, commonly seen as an "overhead that gets in the way of their real work" (Adams & Sasse, 1999) provide the front line security mechanism to prohibit "ill-intentioned individuals to violate the information systems' integrity and validity" (Zviran & Haga, 1999). Yet organizations continue to place much of the burden of computer security on the human element.

Humans are not good password generators (Armstrong, 2003). Even for individuals who understand the security issues of computer passwords, they still fall into predictable patterns and repetition when they create passwords manually. We need then, an analysis of passwords that takes both human factors and security into account (Gehringer, 2002). It seems to be common knowledge that people write down their

passwords, but there is still little research that addresses this particular issue. A survey that asks people such direct questions is the best means to capture this data.

Passwords work relatively well for most applications, but when individuals are careless with passwords, that is when problems can arise.

Thesis

The parameters organizations place on individuals and computer passwords contribute to similar characteristics and behavioral patterns, therefore organizations are actually creating a false sense of security with regard to passwords.

Conclusion

The use of passwords is not going away. Passwords are one of the easiest methods of access control because they are quick and convenient. It is important to restrict access to information systems and organizations are doing this by enforcing strict password policies. But some policies are also making it hard for users to remember passwords. Password choice, password pattern recognition, and password memorability are not highly researched subjects because of the sensitivity of the topic. Nevertheless, they are the focus of this research. Maintaining password security involves striking a balance between having enough rules to maintain security and not having so many rules that users will revert to actions that compromise security (Gehringer, 2002). If strong passwords are so important, then how are we handling the situation? Are we protecting these strong passwords?

Chapter Review

This chapter briefly summarizes computer passwords and it addressed the need to create strong passwords. The ramifications of not protecting passwords was also

discussed. While specific literature related to ways in which individuals choose their passwords is numerous, this chapter provides an overview examination of what relates to this study.

III. Methodology

This chapter describes the research methods used and the analysis performed in our study of passwords. This study involves a web-based survey of military personnel. The thought here is that military members, respected for their integrity as well as for their ability, follow rules. We felt that the results found in this survey would lend credibility to the findings. We could not hope for a better population. The survey focuses on answering the research hypotheses outlined in Chapter 1.

Survey Instrument

A survey is one of the best tools in order to understand a present situation (Leedy & Ormrod, 2001). The researchers in this thesis developed the survey questions. The Air Force Institute of Technology provided the personnel that developed the web-based survey. After the survey was loaded onto the web page, we selected a pilot group of twenty individuals to test the survey and find any errors or problems with the instrument. After finding no errors and no problems with accessibility from the internet, the survey was ready for offering. An e-mail was send to all military members assigned to the Air Force Institute of Technology, a population of 923. The e-mail included a link to the survey site as well as instructions stating that the survey was voluntary (See Appendix B for copy of the web-survey instrument). The survey was accessible for one month from 10 December of 2004 to 10 January of 2005. After stopping the web-survey on 10 January, we had 338 respondents, a response rate of about 36%, which was sufficient and a representative sample of the population. We also feel that the external validity of the research is high, or the extent to which the conclusions drawn from this survey can be

generalized to other contexts (Leedy & Ormrod, 2001). The study does not include a control group; therefore, it takes into account many factors of the outside world. We also feel that the representative sample was very conservative, lending to the credibility of the findings. Military members, perceived as trusted and honest, whose jobs rely on following rules and the chain of command, were an excellent population to draw from. We feel that such factors contribute to the validity, reliability and applicability of our findings.

We imported the data from the survey into an Excel 2003 Spreadsheet. After review, we consolidate this data into a program called JMP, which counts the frequencies of the answers and displays the data into histograms in the following categories:

- Do you use passwords?
- Has your password ever been compromised?
- Do you use recycle or use similar passwords for different applications?
- In the last year, have you written down a password?
- In the last year, have you ever shared a password with friends, family, co-workers or others?
- How do you remember your password(s)?
- Have you ever voluntarily changed a password so that it is easier to remember?
- Are there any negative consequences to not changing passwords regularly?
- Do you feel that password procedures and parameters are a nuisance?
- How many passwords are you currently remembering/using?
- How would characterize your organization's training and education relating to the creation of passwords?

- Do you follow the password procedures based on organizational guidance?
- Do you feel the password policies of your organization are burdensome?

Limits of the Data

The survey data is comprised of individuals proceeding through the survey and not allowed to go back and change answers. Due to this restriction, the data may not include the true feelings and attitudes of the respondents after they have completed the survey. One investigative technique was the use of open-ended questions, although designed to capture critical feedback, this technique may not have been the most efficient way of gathering old passwords. In addition, the question that asks, "Has your password ever been compromised?" may be ambiguous and many respondents may not know if their passwords have been compromised if no one has told them. Also, the question that asks "Have you even voluntarily changed a password so that it is easy to remember?" does not take into account and does not specify whether the individual was foced to change their password by an administrator.

Building the Spreadsheet

Before analysis, we inspect the data for errors and inconsistencies. We exclude any questions where all the responses are blank. We also consolidate the comments provided by the respondents in the open-ended questions and group them into categories. In the question asking how respondents remember passwords, if they chose 'other' we grouped the comments in the most logical fashion.

Table Analysis

Some of our analysis involves examining the association between different types of categories. For example, in order to analyze the characteristics of whether or not a person has any experience working in the computer field. We are also interested in whether or not gender plays a role in password behavior. A table provides a means for analyzing and viewing interesting characteristics. Since the data of this study consists of several categories, this method of analysis proves highly useful.

Data Analysis

In the following section, we analyze the data using the methods outlined above. Since data sets are in the form of spreadsheets, we use Microsoft Excel (2003) in order to view the raw data. For analysis and histograms, we use JMP® Version 5.1 (2003). A score of 999 in the web-survey refers to a non-response where the question was left blank.

Investigative Question One

The first investigative question asks, "Do you use passwords?" There was a 100% response to this question and each response was "Yes." All of those who took the survey did use passwords.

Investigative Question Two

The second investigative question asks, "Has your password ever been compromised?" The results are in Figure 1.

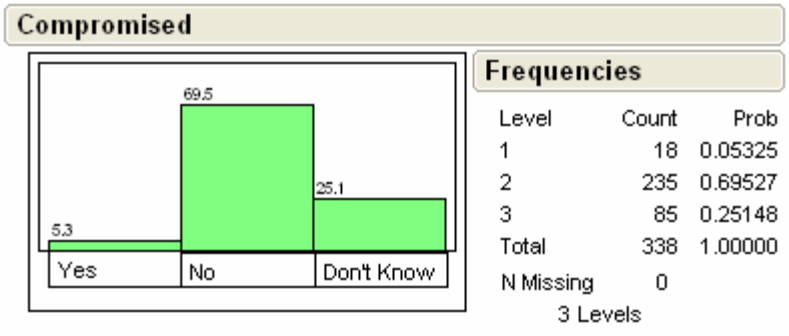

Figure 1. Has your password ever been compromised?

The results of this question show that most respondents feel confident in their passwords, but a quarter felt that they did not know whether they passwords are safe. Five percent said that their passwords had been compromised.

Investigative Question Three

People must never use a password that is the same or similar to one they are using on any corporate system on an Internet site (Mitnick, 2002). The third investigative question asks, "Do you recycle or use similar passwords for different applications?" The results are in Figure 2.

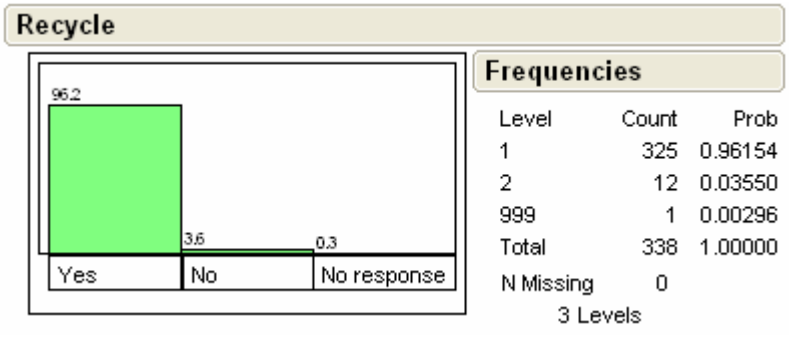

Figure 2. Do you recycle or use similar passwords for different applications?

An alarming 96% of respondents said that they do recycle or use similar passwords. The negative implications are numerous. If people do not use different passwords, then one

compromised password can compromise many other systems. An attacker then has access to not only one system, but also multiple systems. For example, if one uses the same password at work as they do for online banking, then both the work account and bank account are in jeopardy. The result of this particular survey question is startling. Because more systems require a logon user ID and password, this problem should be at the forefront of investigation. More and more sites on the internet require user names and passwords. Using a single password for most sites makes it easy, but also exacerbates the potential danger.

Investigative Question Four

The fourth investigative question asks, "In the last year, have you written down a password?" The results are in Figure 3.

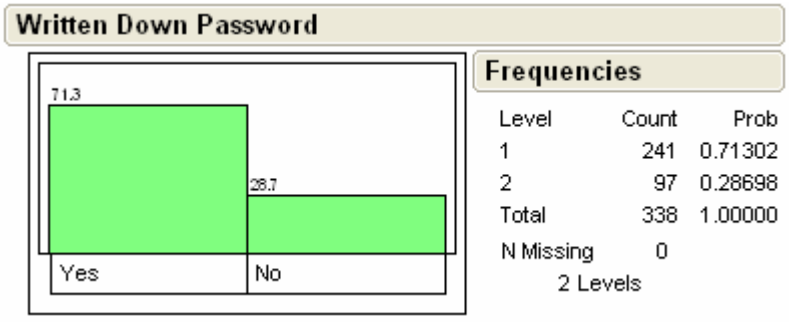

Figure 3. Have you written down a password in the last year?

Again, this is critical finding. One of the purposes of this research was to validate the findings of the Adams and Sasse study that said 50% of the respondents wrote down their password. In the last year, this research shows that 71% of the respondents wrote down their password. This goes against most every password policy in most every organization. This is a significant spike in the number given by Adams and Sasse (1999). Rules for creating strong and secure passwords were "rarely communicated" (1999) to the

respondents in their study. More than 5 years later, there seems to be more of a problem than before. As we will see, the respondents in this study show that they are well aware of the rules, yet they are more prone to writing their passwords down.

Investigative Question Five

No matter what the circumstance, individuals must understand that passwords must never be disclosed or shared with anyone (Mitnick, 2002). The fifth investigative question asks, "In the last year, have you ever shared a password with friends, family, co-workers or others?" The results are in Figure 4.

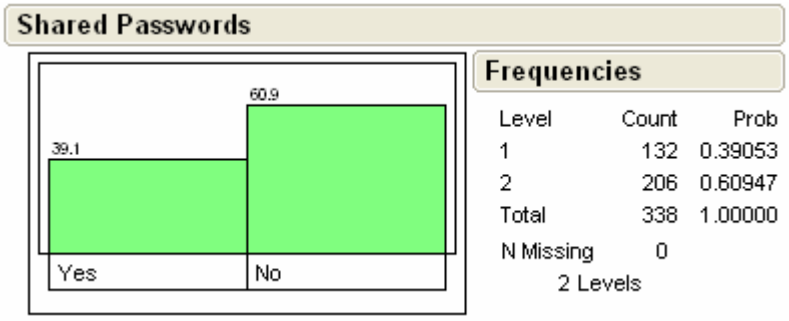

Figure 4. Have you shared a password?

This is interesting, noting the importance of keeping passwords secure. Almost 40% of the respondents admitted to sharing a password in the last year. If individuals were following the guidance of their organizations and of literature, then this number should be zero. Obviously there is a disconnect between what individuals are told to do and what they are actually doing.

Investigative Question Six

The sixth investigative question asks, "How do you remember your password(s)?" The results are in Figure 5. Note the numbering scheme:

1. Familiar Names, Places, Dates
2. Keyboard Pattern
3. Sports Reference
4. Certain letters in a familiar sequence
5. Other

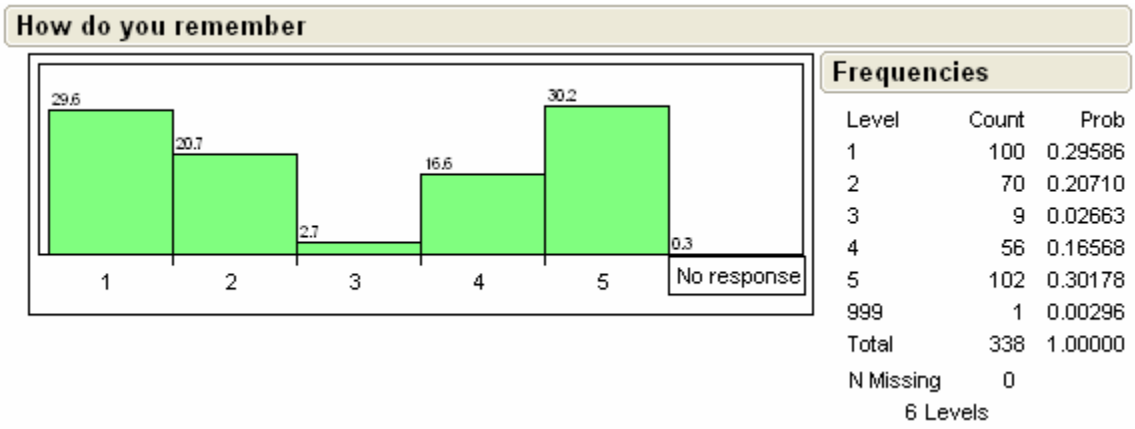

Figure 5. How do you remember your password(s)?

In this study, the use of familiar names, dates and place is contrary to the practice of good password management. Much of the literature does not preclude users from using a keyboard pattern for passwords, but knowing that almost 20% of respondents use a keyboard pattern, this information could help hackers. The literature shows that using letters of a familiar sequence with the addition of character and numbers is a good choice for creating strong passwords and over 16% said they use this method. This method is common in passphrases. Of those that chose "Other," the following is how we categorized the response. For example, we consolidate responses such as '*I use a passphrases*' or '*sentence technique'* into a category called *passphrases*. Of those who chose 'other,' only 28 responded that they used a technique similar to passphrases. Thus,

the overall count of individuals who use the suggested secure technique rises from 16% to 25%. Therefore, only 25% of the overall respondents are using suggested technique for creating strong passwords. The following table represents some of the memory techniques used by respondents. The table also gives some examples of these techniques.

Table 1. Memory Techniques

Memory Techniques	Example
Passphrase	*CUL8rG8r*
Keyboard Pattern	*!QAZ2wsx*
Nickname	*Scooter!1978*
Letter, Number substitutes	*pa$$word*
	N&E4ever
	D@ddy&J@c0b
Phonetically spelled words	*D8Me4Ever!*
Familiar Details	
Familiar Numbers	*Birthday1/10/78*
Familiar Place	*BostonMass$$*
Familiar Objects	*1993=Miata*
Unique experience	*hawaii50**
Familiar Dates	*Wedding2/23/80*
Hobby	*Ifly4Fun2*
Pet Names	*Fluffy&spot2000*
Personal Goal, Lose weight	*160byMay06*
Personalized License Plate	*4mula4*
Names from stories	*Cindarella&PrinceC*
Job Related	
Office Symbol	*88ABW/sc*
Work related location	*Dayton#2004*
Math Equation	*E=mc2*
Bible Reference	*Isaiah68*
Sports Team	*Mavericks123*
Long vocabulary word	*SesquicentennialTX*
Foreign Words	*Je_suisfatigue*
Write them down	
Computer Generated	
Combination of techniques	
Store on computer	

This table is useful to analyze because it gives others more ideas on what to use for password choice. The sharing of this knowledge will not only help others come up with different memory techniques, but it will aid in overall computer security because new ideas will give people more options when the time comes to change their password. Many of the respondents who disclosed previously used passwords showed similar patterns in their passwords. For example, many use a keyboard pattern for their password, so in effect, they are following the rules by using the proper number of symbols and characters, but they are in essence getting around the guidance.

Investigative Question Seven

The seventh investigative question asks, "Have you ever voluntarily changed a password so that it is easier to remember?" The results are in Figure 6.

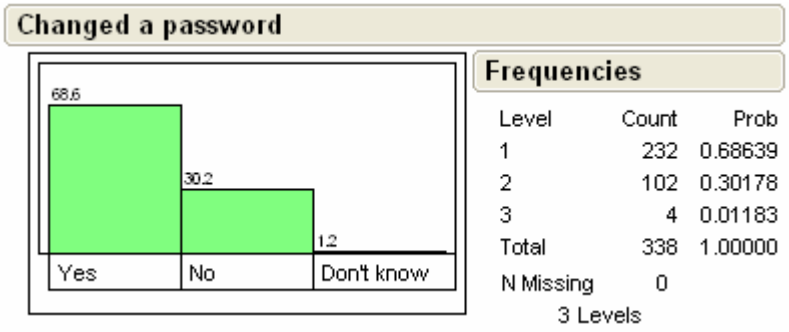

Figure 6. Have you changed a password so that it is easier to remember?

The results of this question highlight the fact that users want to use passwords that are easy to remember. Over 68% willingly changed a password so that they could remember it. This finding agrees with most of the research. Users seek simplicity.

Investigative Question Eight

The eighth investigative question asks, "Are there any negative consequences to not changing passwords regularly?" The results are in Figure 7.

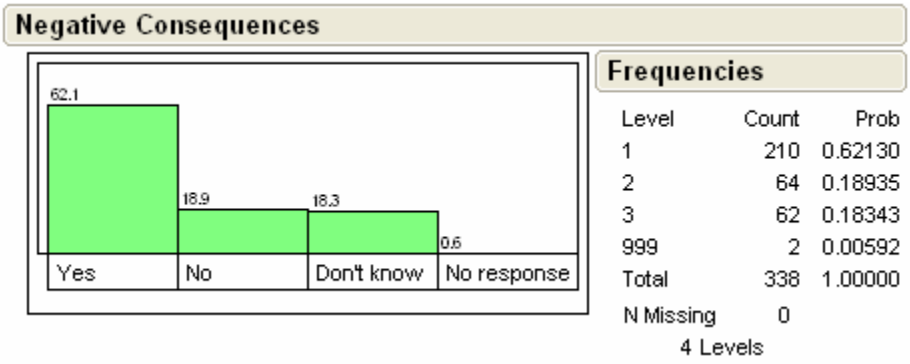

Figure 7. Are there negative consequences to not changing passwords regularly?

Over 62% felt that there are negative consequences to not changing passwords regularly. Over 18% felt there were no negative consequences and 18% did not know. Considering the respondents who said there were no negative consequences, one might assume they are unaware of the potential dangers or they are frustrated with the idea of changing passwords regularly. This is understandable. This researcher has yet to change his online bank account password in over 7 years and cannot see any negative consequences in not doing so.

Investigative Question Nine

The ninth investigative question asks, "Do you feel that password parameters are a nuisance?" The results are in Figure 8.

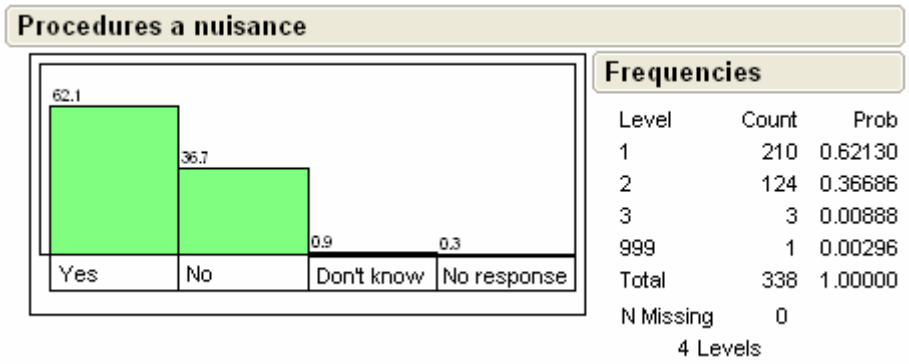

Figure 8. Are password procedures and parameters a nuisance?

This survey found that over 62% of respondents felt that password parameters are a nuisance. This can have serious implications if not addressed correctly. How can organizations effectively reinforce the importance of the password policies? Users understand that there are negative consequences, yet they still desire a system that is easy to use.

Investigative Question Ten

The tenth investigative question asks, "How many passwords are you currently remembering/using?" The results are in Figure 9.

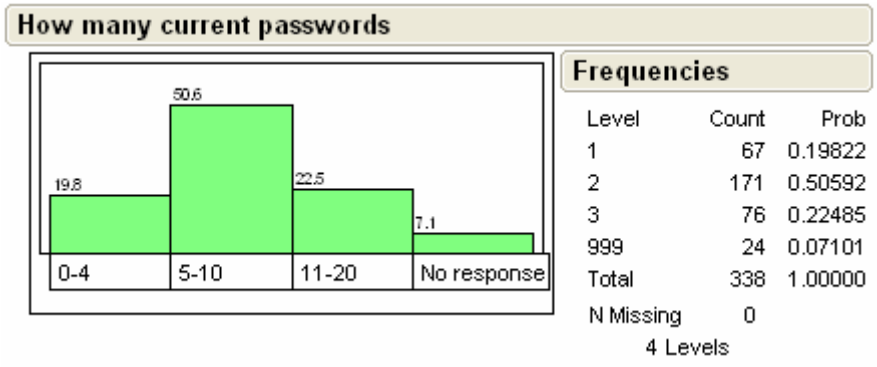

Figure 9. How many passwords are you currently remembering?

Half of respondents are remembering anywhere between 5 and 10 passwords. But over 20% are remembering over eleven passwords and based on the literature, the tendency to write down passwords goes up as the number of passwords remembered goes up (Adams & Sasse, 1999). An interesting finding here is that no one responded saying they remember or use more than 20 passwords. This may indicate that there may be some sort of ceiling. At some point, individuals do not see the need to remember so many passwords.

Investigative Question Eleven

The eleventh investigative question asks, "How would you characterize your organization's training and education relating to the creation of passwords?" This question measures of attitudes of the subjects regarding their feelings toward an organization's education and training with respect to password creation.

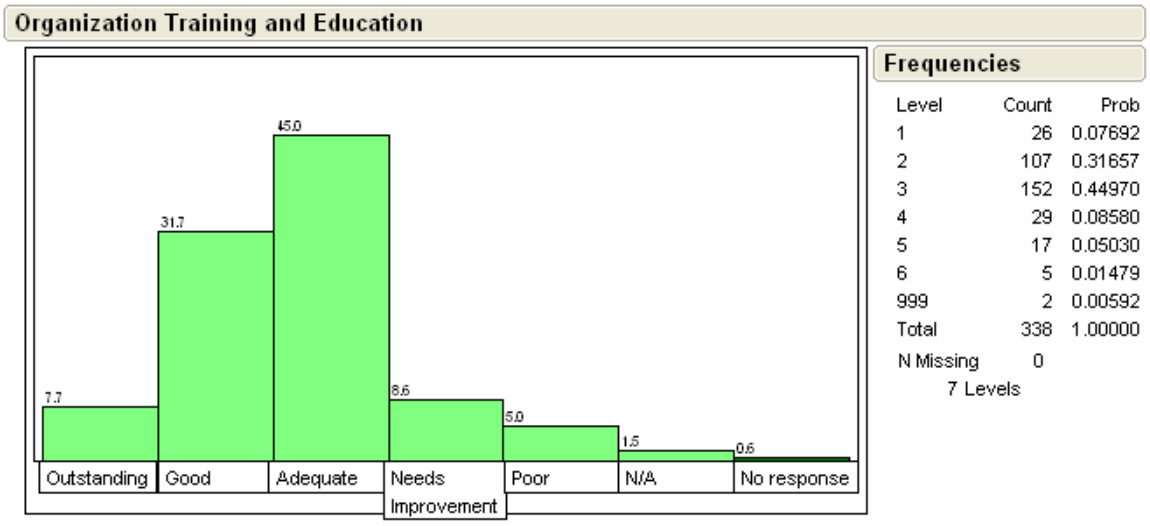

Figure 10. How would you characterize organizational training of password creation?

Over 83% of the respondents felt that their organizational training of password creation was adequate or better. But this brings up an interesting finding: If people feel properly trained, then why the bad decisions when it come to following the rules? There should have been evidence of greater compliance among the respondents if they felt that training and education was adequate or better.

Investigative Question Twelve

The twelfth investigative question asks, "Do you follow the password procedures based on organizational guidance?" The results are in Figure 11.

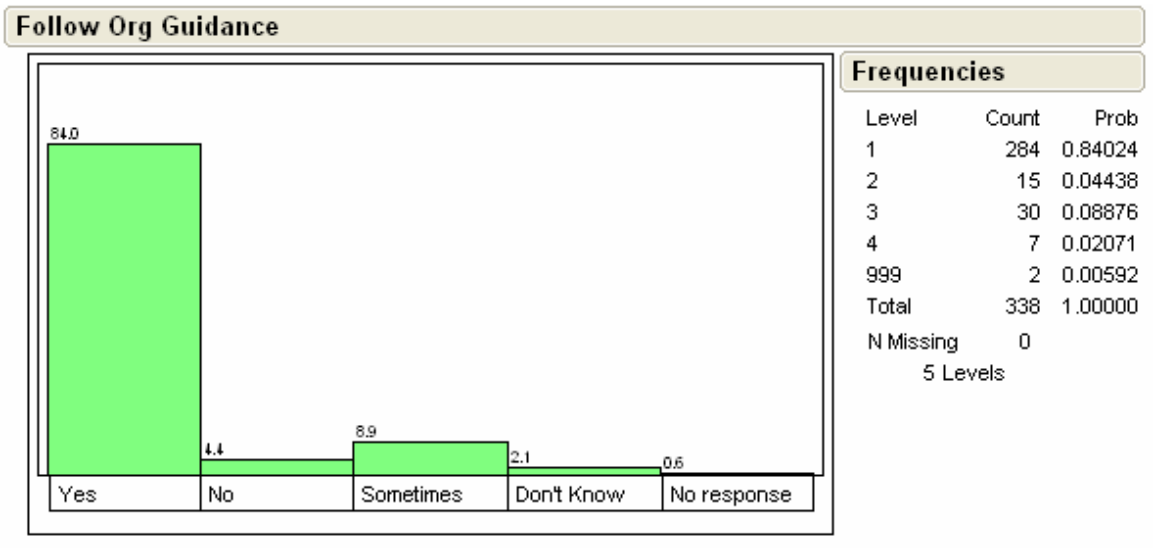

Figure 11. Do you follow the password procedures based on organizational guidance?

There are certainly some inconsistencies found with respect to this investigative question. In the questions that asked if individuals wrote down or shared passwords, it was obvious that these practices do not conform to organizational policies. How can 84% say that they are following the procedures? There seems to be some disconnect between what people perceive as following the rules and what they are actually doing. This research highlights this interesting fact of human perception. People want to believe they are following the rules. Each year, AFIT trains its computer users on the proper methods of creating passwords and secure computing practices. Again, we expected much greater compliance from this group of military professionals.

Investigative Question Thirteen

The thirteenth investigative question asks, "Do you feel the password policies of your organization are burdensome?" This question seeks to revalidate the findings in Investigative Question 9. The results are in Figure 12.

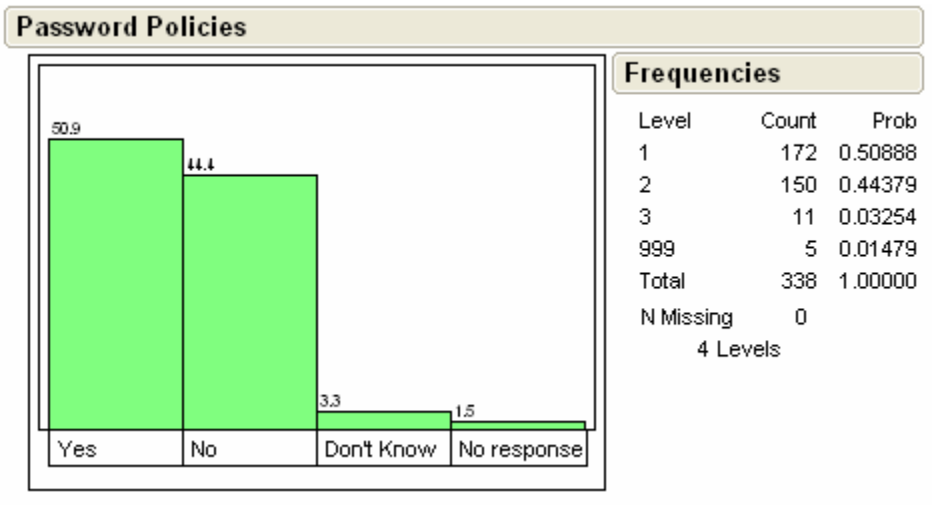

Figure 12. Do you feel the password policies of your organization are burdensome?

Here, more people feel that password policies are not burdensome. But the results are similar, meaning half of the respondents felt that password policies are in fact not easy to use.

Demographics

The total number of respondents was 338. Five respondents failed to classify their gender. The percentage of respondents who were female amounted to 14%, and the latest quarterly demographics report of the Air Force's active-duty population has the number of female active duty members at 19.6% (Air Force Personnel Center, 2005). Getting certain demographics in this study was not a concern of the researchers. We know the sample is homogenous, and this should lend to the reliability of the findings. The demographic information is in Figures 13-16. Finally, we will try to generalize the findings and relate them to the demographics.

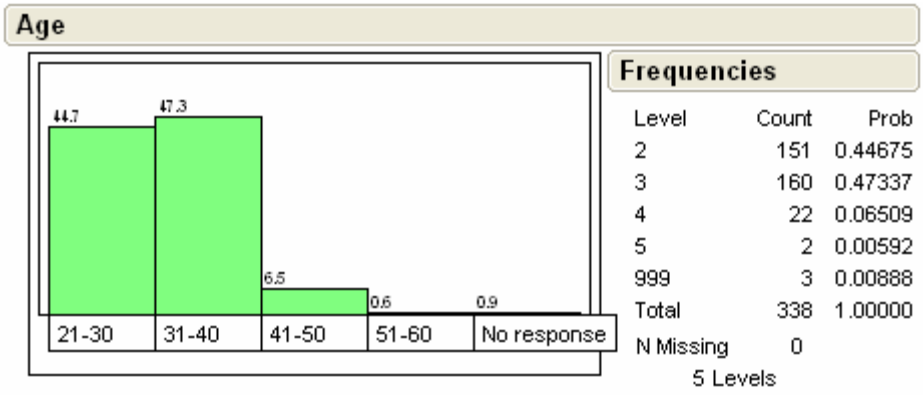

Figure 13 Age of Respondents

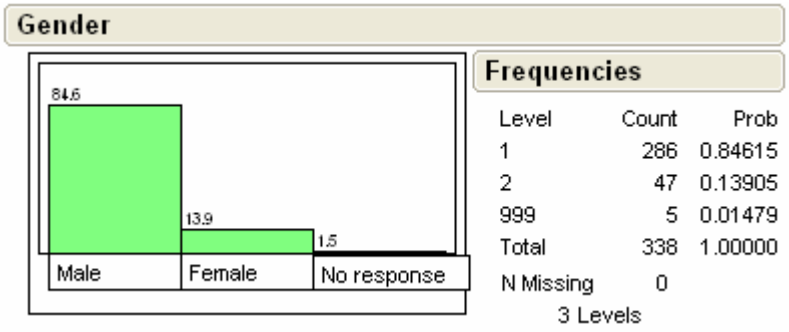

Figure 14. Gender of Respondents

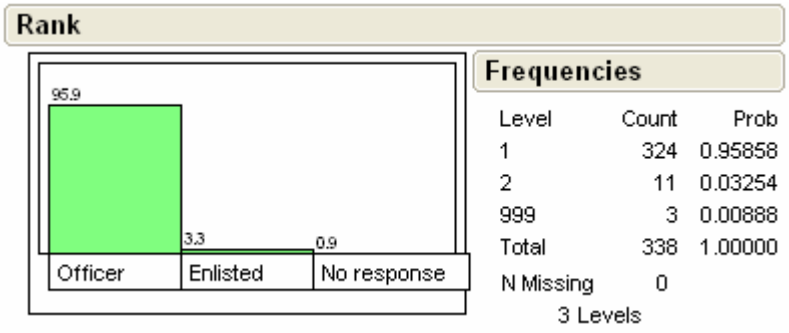

Figure 15. Rank of Respondents

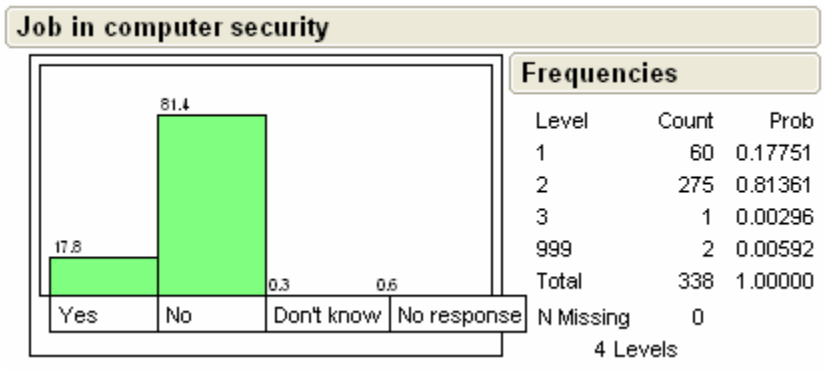

Figure 16. Job in computer or network security

Respondents with IT Background

We wanted to see whether exposure in the computer or network security arena had any effect on the responses. The only findings that differed from the responses of the overall sample were in the category of "Are there any negative consequences to not following the rules." In Table 2, we see that those who said they had experience in IT were more aware of the negative consequences of not following password rules. This makes sense because of the exposure to the environment of computer security and the importance passwords play in authentication. We would hope to see more awareness in these individuals. Table 2 reemphasizes the need to expose more people to the dangers and possible consequences of not following policies and guidance.

Table 2. Negative Consequences

	Are there negative consequences to not following rules		
Job in IT	**Yes**	**No**	**Don't Know**
yes	**78.3%**	**15%**	**5%**
no	**57.8%**	**19.6%**	**20.7%**

For in-depth analysis, we use JMP® Version 5.1 (*JMP*, 2003). In all cases, alpha = 0.05 for the purposes of hypothesis testing. The null hypothesis in this case is that the two means are equal, there is no difference in response to this question, whether their job was in IT or not. In order to test the significance of this data, we employed a Student t-test to see if there was in fact a difference in the means. The results are in the following figure.

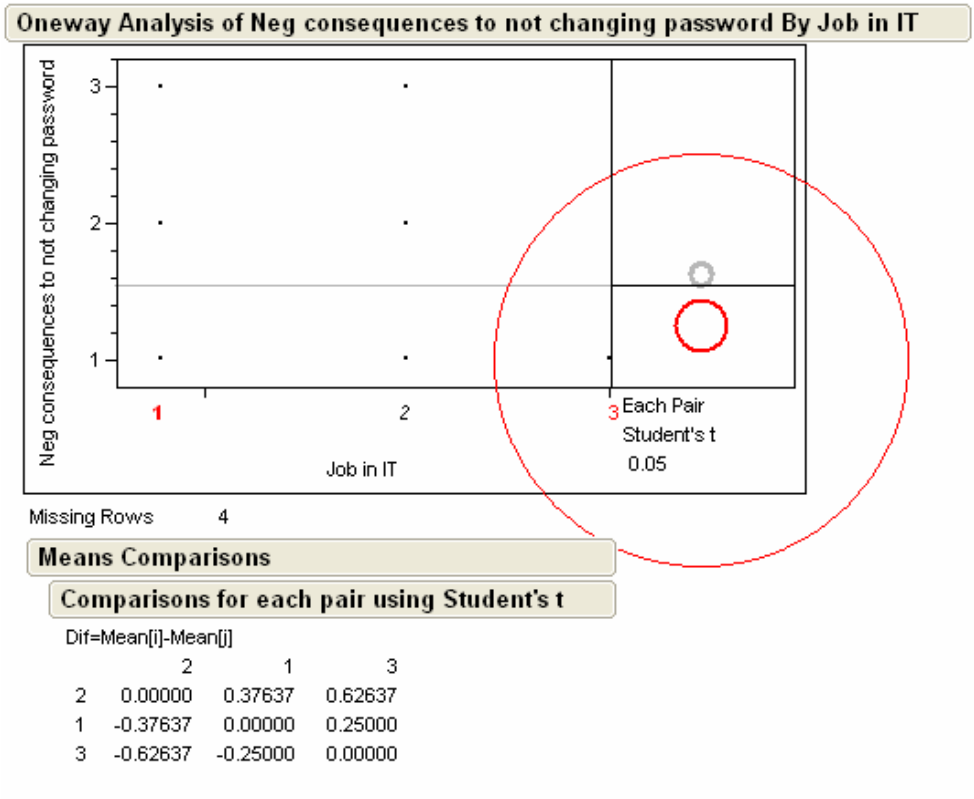

Figure 17. Comparison of Means (Job in IT)

In Figure 17, a response of 1, indicates that the respondent did have experience in IT, while a response of 2 indicates an answer of 'no,' and a response of 3 indicates an answer of 'I don't know.' The dependent axis, in this case, asking whether or not there were any negative consequences to not changing one's password, a response of 1 indicates an answer of 'yes' there are negative consequences, while the answers of 2 and 3 are 'no,'

and ‘I don’t know,’ respectively. If in the statistical test, the two inner circles intersect, then we are not given the liberty to say that their means are significantly different. But since in this case, we find that there are two circles do not intersect, we can say that there is a difference between those that have IT experience and those that do not, when it comes their feelings of negative consequences and changing passwords. The same method described here was used to look at gender and the tendencies to share or write down passwords.

Tables 3-7 show several categories where having a history in IT make little impact to the response. The same statistical tests were run to test the significance but it was determined that the differences were not significant.

Table 3. Compromised

	Has your password ever been compromised		
Job in IT	**Yes**	**No**	**Don’t Know**
yes	**3.3%**	**66.6%**	**30%**
no	**5.45%**	**69.8%**	**23.6%**

Table 4. Recycle Passwords

	Do you recycle passwords	
Job in IT	**Yes**	**No**
yes	**93.3%**	**5%**
no	**96.4%**	**2.9%**

Table 5. Written Down Password

	Have you written down your password	
Job in IT	**Yes**	**No**
yes	**68.3%**	**30%**
no	**71.6%**	**28.4%**

Table 6. Shared Passwords

	Have you shared your password	
Job in IT	**Yes**	**No**
yes	**36.6%**	**63.3%**
no	**39.6%**	**60.4%**

Table 7. Changed Password

	Has you ever changed your password so that it is easier to remember		
Job in IT	**Yes**	**No**	**Don't Know**
yes	**66.6%**	**31.6%**	**1.6%**
no	**69.1%**	**29.8%**	**1.1%**

Table 8 shows a considerable amount of disparity between those who have had a job in IT and those that said they did not. This makes sense, again because of the exposure to the environment. More people in the IT field understand the importance of password parameters. Yet the test for comparison of the means did not prove to show that there was enough significance to make such a claim.

Table 8. Are parameters a nuisance?

	Do you feel that password parameters are a nuisance		
Job in IT	**Yes**	**No**	**Don't Know**
yes	**50%**	**45%**	**0%**
no	**64.7%**	**34.1%**	**1.1%**

Again, Tables 9 and 10 do not show much different in the attitude of individuals relating to the adherence to organizational procedures or burdensome policies.

Table 9. Do you follow organizational procedures?

	Do you follow organizational procedures			
Job in IT	**Yes**	**No**	**Sometimes**	**Don't Know**
yes	**83.3%**	**8.3%**	**6.6%**	**0%**
no	**83.6%**	**3.27%**	**9.1%**	**2.5%**

Table 10. Are policies burdensome?

	Do you feel that password policies are burdensome		
Job in IT	**Yes**	**No**	**Don't Know**
yes	**50%**	**46.6%**	**0%**
no	**51.2%**	**43.6%**	**4%**

Gender Issues

We conducted the following analysis to see whether gender plays a part in password behavior. We chose to focus on the issues of writing down passwords and

sharing passwords. The results are startling. Table 11 compares male, females, and the extent each said they write down their passwords.

Table 11. Gender vs. Written Password

	Have you written down your password	
Gender	**Yes**	**No**
Male	**67.1%**	**32.9%**
Female	**93.6%**	**6.4%**

The fact that over 93% of females respondents wrote down their password in the last year could have implications with how organizations effectively manage and train individuals. If gender is found to be such an important factor, there may be some inherent differences in the ways people feel about the importance of security. Table 12 shows that a majority of females responded that they have in fact shared their passwords with others, compared to only 36% of males. This researcher feels that such a finding is critical information.

Table 12. Gender vs. Shared Password

	Have you shared your password	
Gender	**Yes**	**No**
Male	**36.4%**	**63.6%**
Female	**55.3%**	**44.7%**

Not only do women have more of a tendency to write down passwords, but they also have more or a tendency to share them with others. We wonder if this disparity is common throughout the population. If such a difference does exist, social science must play more of a role in the training and education of computer password security.

Again, in order to test this, we use a Student t-test to compare the means of the two groups. The following figures are the results of those tests.

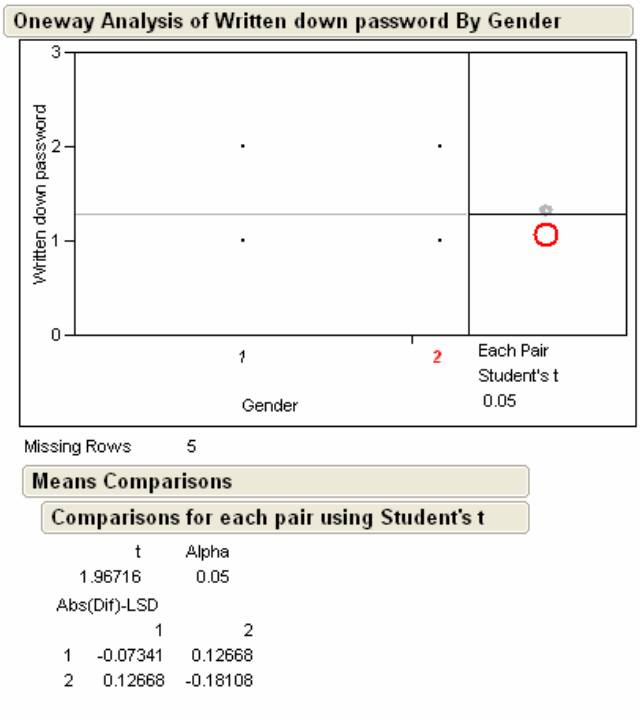

Figure 18. Comparison of the Means, Gender and Writing Down Passwords

In this case our the null hypothesis would be that that gender does not make a difference in determining whether someone is more or less likely to write down or share a password. A response of 1 indicates male, and 2 indicates female, while a response on the dependent side, in this case, Have you written down your password?, a 1 indicates a 'yes' response and a 2 indicates a 'no' response. The lower circle in the figure represents the mean response of the females and it does not intersect the circle that represents the mean of male responses. We accept the alternate hypothesis that men and women do differ in their likelihood to write down a password,

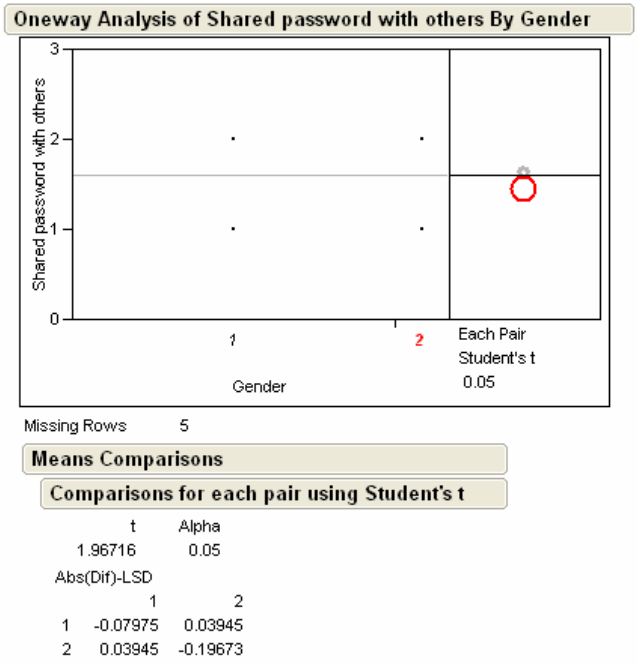

Figure 19. Comparison of the Means, Gender and Sharing Passwords

In this figure, a response of 1 indicates male, and 2 indicates female, while a response on the dependent side, in this case, Have you shared your password?, a 1 indicates a 'yes' response and a 2 indicates a 'no' response. The lower circle in the figure represents the mean response of the females and it does not intersect the circle that represents the mean of male responses. The figures here show that there is a significant difference in the means between men and women when it comes to sharing passwords. We accept the alternate hypothesis that men and women do differ in their likelihood to share a password. Females are more likely to write down or share a password.

Assumptions

There were some assumptions made in the tests checking for a significant

difference in the means. We assumed that the variables were independent, in this case, male/female, job in IT/job not in IT. We also assume that the populations are normally distributed.

Chapter Summary

There appears to be some relationship between gender and tendency to either share or write down a password. We find that users are in fact writing down passwords and that even though most perceive that they are following organizational policy, this survey shows that this perception is invalid.

This chapter describes results of the web-survey. In the next chapter, we discuss the findings from this chapter.

IV. Conclusions, Recommendations, and Further Study

In this chapter, we discuss our conclusions, recommendations, and suggestions for future research.

Conclusions

In Chapter 1, we expressed our research hypotheses:

1) Individuals are not following the current guidance for developing strong passwords. Many individuals are following the current guidance for developing strong passwords, but the manner in which they choose those passwords have a distinct pattern.

We feel that this survey shows that people are not following the current guidance. Many feel that they are following the guidance when in reality they are not. Many are still using familiar names, places and dates, while others are using a keyboard pattern. On a good note, many are using passphrases, which is an easy and effective way to remember passwords. This research captured a number of passwords that the respondents volunteered in response to Survey Question 15. Many respondents admitted to using a keyboard patter, and one respondent spoke for many when they said, “I cannot share any old passwords because I am using only 3 and do not plan on changing them any time in the future.”

2) Individuals are developing ways to remember their passwords that are not secure, either through writing down their passwords or using a pattern on the keyboard for example.

We show in this research that people are still writing their passwords down.

3) Individuals are using the same passwords for multiple applications.

This research also shows that people are using the same passwords for multiple applications. Investigative Question 3 proves that most use the same password for different things.

Additional Findings

With respect to the definition of strong passwords, this research shows how there may be a disconnect among perceptions of what entails a strong, secure password. A strong and secure password is more than password composition. It involves the proper use and management of those passwords. Users must not share or write their passwords down. Users must continually change their passwords, and they should use different passwords for different applications. Users should be cognoscente of the tendencies to make password management easier. This research shows how certain behaviors may give a false sense of security to computer users. If members of an organization use a keyboard pattern for example, this knowledge, in the wrong hands, could spell disaster.

In addition, it is interesting to see differences with regard to those that said they had IT experience and those that did not. We also unexpectedly found that there was significant difference in the tendency to write or share passwords based on gender.

This research can classify its finding into three categories. 1) Respondents to the survey are not following the password policy set forth by the organizations.
2) Respondents feel that password policies are a nuisance and bothersome, which leads to poor judgment when choosing strong, secure passwords. 3) Finally, this research shows how passwords policies have caused individuals to use a subset of the large domain of passwords that policy intends to enforce.

Recommendations

The emphasis placed on passwords will only increase. Individuals remember too many passwords and unless policies or procedures change, users will continue to find ways that are easier and less secure. As discussed in Chapter 2, users want passwords that are easy to remember and proper training may not be enough to convince individuals to choose strong passwords. As our analysis in Chapter 3 showed, the majority of individuals still write down their passwords. We find this to be disturbing. Additionally, unless we limit the number of passwords we use, we see that this trend will continue. It is imperative that organizations limit the number of passwords their employees must use. Organizations should work with users to help them take an interest in security. If they feel burdened with multiple passwords and multiple parameters, this interest wanes.

This study focused on some basic information and attitudes related to passwords. While the information in this study is important, more discoveries should take place. Learning from past mistakes can lead to exciting opportunities. We want individuals to make the best choice when it comes to password selection. However, by looking ahead, we feel that the problem of choosing strong passwords compounds with the addition of more parameters.

Researchers should look at whether people use the same password throughout their daily lives. In this survey, we showed that people are using the same password for multiple application and sites, so we recommend further investigation of this problem.

Better Authentication

Strong passwords are creative passwords. This research is a good way of letting others know what new and innovative ideas individuals use when choosing their

passwords. This research should help others to think critically about better and more secure methods and better memory techniques. Different password techniques allow for better security.

The results of the survey in relation to gender issues were a surprise. Females and males are different, but we did not expect to see such a difference in how they behave when it comes to writing down or sharing passwords. Knowing this, organizations should limit the opportunities for others to share passwords and people should not feel that they have to write them down to remember strong passwords. Different authentication techniques are available that should minimize this risk.

Organizations should utilize biometrics, smart cards, and other authentication techniques. Emphasis on multiple techniques is necessary. Companies go to great lengths to protect themselves, but they are at a serious risk when someone compromise just one password.

Organizational Culture/Attitude

Individuals demand easier methods to remember passwords. When an online bank does not require password changes, then why should anyone else. The individual and the organization must take some responsibility for the improvements to password selection, but who is ultimately responsible? It will be hard to realize the full impact of a compromised password. As this study has shown, the reliability of individuals will always be in question. Future policies will probably place more parameters on password choice. More pressure and stress placed upon the individual will always invite problems unless the training is in place to help with password selection. This subject will continue to draw attention because computer passwords are the most common front-line defense

against unauthorized access. Organizations much make strong password selection a part of a positive security attitude.

Suggestions for Further Study

This study addressed the importance of computer password choice. It discussed the findings of a web-survey asking volunteers to disclose different aspects of passwords. A study of this type may help many organizations realize that people many not be adhering to all password policies. Studies that demonstrate the understanding and subtleties of what is easy and hard for humans (Yan et. al, 2000), particularly on how the mind works, are key to designing things that are easy to use. We recommend future research on password selection practices that help individuals choose passwords, like passphrases, that are in fact easy to use. A mistake by one individual can compromise entire systems because of the emphasis on passwords as the single point of authentication. Fortunately, more authentication techniques are available. Future research could include the current steps that organizations are taking toward multiple authentication techniques and if those techniques improve security. It would be interesting to question those in Investigative Question 2 who said their passwords had been compromised. What steps were taken to rectify the situation and how exactly were their passwords compromised? Taking this a step further, one might ask who is responsible for actions taken on a system that uses your ID. If a password is compromised, is the liability on the user or the provider?

A study done on Extended ASCII and Unicode might also increase the knowledge of computer users and give them more choices for password creation. More possible password combinations are available if more characters are used.

Usability issues for different systems are a major concern. The literature fails to address many of the discrepancies. While one system does not allow special characters, one system requires special characters. If systems are unique and require different passwords, users will continue to find ways to make it easier. Moreover, the tendency to make things easier usually makes things less secure.

Deciding what level of security is adequate is a constant struggle. Many systems have adopted practices where after a few unsuccessful login attempts, that user is locked out until they contact the system administrator to either reset or create a new password. What prevents an individual with malicious intent from locking out every user on a specific network? I can foresee a time when password policies require users to not only protect their passwords, but their user names as well, in order to prevent denial of service attacks. In many Windows based systems, if a user tries multiple unsuccessful authentication attempts, then the person would lose access to the system and have to contact an administrator. Future research may involve how organizations are handling the security of user names. Another topic would be to examine to what extent customer service centers are dealing with calls from users who have been locked out of their accounts. What are the costs associated with running customer service centers? How can we measure the cost of the complexities organizations place on passwords. In addition, an interesting research topic might be one that addresses time spent by the help desk dealing with password issues.

Today, many banks rely on the functionality of web browsers and password authentication to handle a majority of customer transactions. If it were not for this ease of use, many customers would be driven away from using the service (Bohm, Brown, &

Gladman, 2000). How much risk are organizations willing to accept so that users can access their accounts and what are the incentives for providers to improve security against account compromises? Future research could try to quantify the costs and benefits of different types of authentication and computer security.

Chapter Summary

In this chapter, we discussed the conclusions of the study and the impact is has on those who use computer passwords. We found many factors that contribute to users choosing easy to remember passwords. We conclude that unless password policies change, users will use similar memory techniques in the future. We recommend that individuals improve password selection techniques. We also recommend that individuals not write down their passwords in the case that the password falls into the wrong hands. Finally, we discussed topics for future research.

Last Word

This study revealed three critical issues associated with computer passwords. First, individuals are writing down passwords. Second, because of current guidance, individuals must use different passwords for different systems and this only adds to the problem above. Third, the parameters organizations place on passwords will continue to cause problems unless there is a common standard applied to most authentication systems. Selecting strong computer passwords continues to be a problem, and unless those in authority place more importance on selecting strong passwords in addition to using multiple authentication techniques, the security of computer systems will continue to be an uphill battle.

Appendix A: Definition of Terms

Strong Password - password that is at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess (Microsoft, 2004)

Phishing - a technique that hackers use that puts a link in a fake e-mail that appears to go to a popular site, but actually takes you to a fraudulent site that looks exactly like the official site (Microsoft, 2004)

Shoulder Surfing – The act of watching a person type at his keyboard to detect and steal his password of other user information (Mitnick, 2002).

Appendix B: Survey Instrument

The following information is provided as required by the Privacy Act of 1974:

Purpose: The purpose of this study is to gather information on how respondents choose, remember and use passwords.

Routine Use: The results of this study will help to determine if individuals are using similar patterns or memory techniques when choosing passwords.

Analysis of individual responses will be conducted and only members of the Air Force Institute of Technology research team will be permitted access to the raw data.

Participation: Participation is VOLUNTARY. No adverse action will be taken against any member who does not participate in this survey or who does not complete any part of the survey.

Instructions

- Base your answers on your own thoughts & experiences
- Please make your answers clear and concise when asked to answer in a response or when providing comments
- Be sure to select the correct option button when asked because when you move on you cannot come back

Contact information: If you have any questions about this request, please contact Dr. Dennis Strouble (Primary Investigator) – Phone (937) 785-3355 x3323; E-mail – dennis.strouble@afit.edu or Lt Kurt Martinson (Graduate Student) - Phone (937) 429-3404; E-mail – kurt.martinson@afit.edu.

Start Survey

Notice and Consent Banner:
Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Password Choice

Please take a few minutes to fill out this survey on password usage. We welcome your feedback, and your answers will be kept confidential. Thank you for your participation.

General Information

1. Do you use passwords?

○ Yes ○ No ○ N/A

2. Has your password ever been compromised?

○ Yes ○ No ○ Don't Know

3. Do you use recycle or use similar passwords for different applications? Example: Personal E-mail, Work E-mail, Online Banking, Online Ordering, etc.

○ Yes ○ No

4. In the last year, have you written down a password?

○ Yes ○ No

5. In the last year, have you ever shared a password with friends, family, co-workers or others?

○ Yes ○ No

Password Choice

6. How do you remember your password(s)?

○ Familiar Names, Places, Dates ○ Keyboard Pattern ○ Sports Reference ○ Certain letters in a familiar sentence ○ Other (please explain below)

7. Please share your memory technique. DO NOT write down your password.

_____

_____

_____

8. Have you ever voluntarily changed a password so that it is easier to remember?

○	○	○
Yes	No	Don't Know

9. Are there any negative consequences to not changing passwords regularly?

○	○	○
Yes	No	Don't Know

10. Do you feel that password procedures and parameters are a nuisance?

○	○	○
Yes	No	Don't Know

11. How many passwords are you currently remembering/using?

○	○	○	○
0 to 4	5 to 10	11 to 20	Over 20

Password Guidance

Many organizations have a password policy. For example, users must create passwords that are upper/lower case, contain symbols and words not found in the dictionary. Based on this, please answer the following.

12. How would characterize your organization's training and education relating to the creation of passwords?

○	○	○	○	○	○
Outstanding	Good	Adequate	Needs improvement	Poor	N/A

13. Do you follow the password procedures based on organizational guidance?

○	○	○	○
Yes	No	Sometimes	Don't Know

14. Do you feel the password policies of your organization are burdensome?

○	○	○
Yes	No	Don't Know

Additional Feedback

15. Please write down any <u>old</u> passwords that you have used but <u>are not</u> using today. The purpose is to determine if individuals are using similar patters or characteristics.

_____

_____

16. Please share any additional comments.

_____

_____

Personal Information

17. What is your age?

○	○	○	○	○	○
Under 20	21-30	31-40	41-50	51-60	Over 60

18. What is your gender?

○	○
Male	Female

19. Job or Organization?

○	○
Military Officer	Military Enlisted

20. Is your job now or was your job ever in the computer or network security industry?

○	○	○
Yes	No	Don't Know

Thank you for taking the time to fill out our survey. Your input is greatly appreciated.

AFIT SCN 04-119, Expires 31 December 2005

Appendix C: Survey Data

Q1	Q2	Q3	Q4	Q5	Q6	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q17	Q18	Q19	Q20
1	3	1	1	1	2	1	1	1	1	3	3	1	2	1	1	1
1	2	1	1	1	5	1	1	2	1	1	1	2	3	2	1	1
1	3	1	1	2	4	2	1	1	2	3	1	1	2	1	1	2
1	2	1	1	2	1	1	1	1	3	2	1	2	3	1	2	1
1	2	1	2	1	4	2	1	2	1	3	1	2	2	1	1	2
1	2	1	1	2	4	2	2	1	2	1	1	1	3	1	1	1
1	2	1	1	2	3	2	1	2	2	2	1	2	3	1	1	2
1	2	1	1	1	4	1	1	1	3	2	1	1	2	1	1	1
1	2	1	2	2	1	1	2	2	1	4	1	2	3	1	1	1
1	2	1	1	1	1	1	2	2	2	4	1	2	3	1	2	2
1	2	1	1	1	3	1	1	1	1	2	1	2	3	1	1	1
1	2	1	1	1	2	3	1	1	3	2	1	1	3	2	1	1
1	3	1	1	2	3	2	1	1	2	3	1	1	2	1	1	1
1	2	1	1	1	1	1	2	1	2	3	3	1	2	1	1	2
1	3	1	1	2	5	1	2	1	3	2	1	1	2	1	1	1
1	3	1	1	2	2	2	1	2	2	2	1	2	4	1	2	2
1	3	1	1	1	4	1	3	2	2	3	1	2	2	2	1	2
1	2	1	1	2	2	1	1	2	2	3	1	2	3	1	1	1
1	3	1	1	2	1	1	3	1	2	2	1	1	2	2	1	2
1	2	1	2	2	5	1	1	1	1	3	1	1	2	1	1	2
1	3	1	1	1	1	1	3	1	3	3	1	2	5	1	1	2
1	2	1	1	1	1	1	1	1	2	2	3	1	2	2	1	2
1	2	1	2	1	2	1	1	1	2	3	1	1	2	1	1	1
1	2	1	1	1	1	1	2	1	999	3	1	1	3	1	1	2
1	3	1	1	1	2	2	3	1	999	3	1	1	2	1	1	2
1	2	1	2	2	2	2	2	2	2	3	4	3	3	1	1	2
1	2	1	2	2	2	1	1	2	2	3	1	2	3	1	1	1
1	2	1	1	2	2	1	1	2	1	3	1	1	3	1	1	1
1	3	1	2	1	4	1	1	1	3	2	1	1	2	1	1	1
1	1	1	1	1	5	3	1	1	999	2	1	2	3	1	1	2
1	2	1	1	2	5	1	1	1	3	2	1	2	3	1	1	2
1	2	1	1	2	5	1	1	1	999	2	1	2	2	1	1	2
1	2	1	2	2	4	1	1	1	999	2	1	1	3	1	1	2
1	3	1	1	2	1	1	1	2	3	2	1	2	3	1	1	2
1	2	1	1	1	5	1	1	2	1	3	1	2	3	1	1	2
1	2	1	1	1	2	1	1	1	2	3	1	1	3	1	1	2
1	3	1	1	2	5	1	3	1	999	4	1	1	5	1	1	2
1	2	1	2	1	5	1	1	1	2	2	1	1	3	1	1	2
1	2	1	2	2	2	2	1	1	2	4	2	1	2	1	1	1
1	2	1	1	2	4	1	1	1	2	3	1	1	3	1	1	2
1	3	1	2	2	1	1	2	1	1	3	1	1	3	2	1	2
1	2	1	1	2	1	1	2	1	2	3	3	1	3	1	1	2
1	2	1	1	1	4	2	2	1	2	2	1	1	4	1	2	2
1	2	1	1	1	2	2	2	1	2	2	1	1	2	1	1	2

1	2	1	2	1	4	1	1	1	3	1	1	2	2	1	1	2
1	2	1	2	1	1	2	3	2	1	2	1	2	2	1	1	1
1	3	1	1	2	1	1	1	1	2	1	1	1	2	1	1	2
1	2	1	2	2	2	1	1	1	2	2	1	1	3	1	1	2
1	2	1	1	1	5	2	1	2	999	1	1	2	3	2	1	2
1	2	1	1	2	1	1	2	1	3	5	1	1	3	1	1	2
1	3	1	2	1	4	1	1	1	2	4	1	1	4	1	1	2
1	3	1	1	1	1	1	1	2	999	3	1	1	4	1	1	2
1	2	1	1	2	3	1	1	1	2	3	1	1	3	1	1	2
1	2	1	1	2	5	1	1	2	2	3	1	2	3	1	1	2
1	2	1	2	1	4	1	3	1	2	3	1	3	2	1	1	2
1	3	1	1	1	5	2	2	2	3	2	1	1	3	1	1	2
1	2	1	1	2	4	2	1	2	3	3	3	2	3	1	1	2
1	2	1	1	2	4	1	1	1	2	2	1	1	2	1	1	1
1	3	1	1	2	1	1	1	2	1	2	1	2	3	2	1	2
1	2	1	1	2	2	1	1	1	2	3	2	1	2	1	1	2
1	2	1	2	2	4	2	1	2	1	2	1	2	3	1	1	1
1	1	1	1	1	5	2	1	2	3	3	1	2	2	1	1	2
1	2	1	1	2	2	1	3	1	2	1	1	1	3	1	1	2
1	3	1	1	1	1	1	1	1	2	3	1	1	3	1	1	2
1	2	1	2	2	5	2	2	1	2	3	1	1	3	1	1	2
1	2	1	1	1	1	1	1	2	2	2	1	2	4	2	1	2
1	2	1	2	2	1	1	2	1	2	2	1	2	3	1	1	2
1	2	1	1	1	5	1	1	2	1	1	1	2	3	2	1	1
1	2	1	2	2	2	1	2	1	2	2	1	1	3	1	1	2
1	2	1	1	1	1	1	3	1	2	3	1	1	2	1	1	2
1	3	1	1	1	5	1	1	3	2	2	1	2	2	1	1	2
1	2	2	2	2	5	2	2	1	2	5	1	1	3	1	1	1
1	2	2	2	2	1	2	3	2	1	4	1	1	4	1	1	2
1	2	1	1	2	5	2	3	1	1	1	1	2	4	1	1	2
1	2	1	1	2	4	2	2	1	2	3	1	1	3	1	1	2
1	3	1	1	1	2	1	1	1	999	3	1	1	3	1	1	1
1	3	1	1	2	1	1	3	2	2	2	1	2	4	1	1	2
1	2	1	2	2	2	1	3	2	1	4	4	3	2	1	1	2
1	2	1	1	2	5	2	1	2	999	2	2	2	2	1	1	1
1	2	1	2	2	4	1	3	1	3	4	3	1	2	1	1	2
1	2	1	1	2	1	1	1	1	1	3	1	1	3	1	2	2
1	2	1	2	2	4	2	1	1	2	3	1	1	3	1	1	2
1	2	1	1	2	5	2	2	1	2	5	1	1	2	1	1	2
1	2	1	1	1	5	1	2	2	3	1	1	1	2	1	1	2
1	1	1	1	1	5	2	2	1	3	3	1	1	3	1	1	1
1	2	1	2	2	1	2	1	2	2	2	1	2	3	1	1	2
1	2	1	2	2	2	1	1	1	2	2	1	2	3	1	1	2
1	1	1	2	1	1	1	2	1	1	3	3	1	2	1	1	2
1	2	1	2	2	5	1	1	2	1	4	1	2	2	1	1	2
1	2	1	2	2	2	1	3	1	2	3	1	2	3	1	1	2
1	1	1	2	2	5	1	2	1	999	2	1	1	3	1	1	2
1	2	1	1	2	2	2	3	2	1	2	1	2	2	1	1	1
1	2	1	1	1	1	2	1	2	2	3	1	2	4	1	1	2

1	2	2	1	2	5	1	999	2	3	4	1	1	3	1	1	2
1	1	1	1	2	5	1	2	2	2	2	1	1	2	1	1	1
1	2	1	2	2	5	1	2	1	2	4	2	1	2	1	1	2
1	3	1	1	2	3	1	1	2	2	2	1	2	3	1	1	2
1	2	1	2	2	5	1	3	2	2	3	1	2	3	1	1	2
1	3	1	1	2	3	1	1	2	1	2	1	2	3	1	1	2
1	2	1	1	1	4	1	1	1	2	2	1	2	2	2	1	2
1	2	1	1	1	1	1	1	1	3	4	3	1	2	1	1	2
1	2	1	1	1	1	1	3	1	2	3	3	1	2	2	1	2
1	2	1	1	2	4	1	2	1	999	3	1	2	2	1	1	2
1	1	1	2	2	2	1	1	2	2	1	1	2	3	1	1	2
1	2	1	1	2	4	1	2	1	2	4	2	1	999	999	1	2
1	2	1	1	2	5	1	1	2	3	3	1	2	4	2	1	1
1	2	1	2	2	2	1	1	1	1	3	3	2	3	1	1	2
1	2	1	1	1	4	2	3	2	2	2	1	2	3	1	1	2
1	2	1	1	2	5	2	3	2	2	2	1	1	3	1	1	2
1	3	1	1	2	5	2	1	2	3	1	1	2	3	1	2	1
1	2	1	2	1	1	1	2	1	3	2	1	1	2	1	1	2
1	2	1	1	2	2	2	1	2	2	3	1	1	3	2	1	2
1	3	1	2	2	5	2	1	2	2	2	1	2	2	1	1	2
1	2	1	1	1	4	1	3	1	2	3	1	3	2	1	1	2
1	2	1	1	2	1	1	1	2	2	3	1	2	2	1	1	2
1	2	1	1	1	2	1	1	1	2	3	1	2	2	1	1	2
1	2	1	1	1	1	1	2	1	3	3	1	1	3	1	1	2
1	2	1	1	2	4	1	1	1	2	3	1	2	2	1	1	1
1	2	1	1	1	1	1	3	1	2	3	3	1	4	1	1	2
1	2	1	2	2	4	1	1	1	1	3	1	1	3	1	1	2
1	3	1	1	1	1	1	1	1	2	3	1	3	3	1	1	2
1	2	1	1	2	5	1	1	2	2	4	1	2	2	1	1	2
1	2	1	1	1	5	1	1	1	3	2	1	1	2	2	1	2
1	2	999	2	2	1	1	2	2	2	2	1	2	2	1	1	2
1	2	1	1	1	1	1	2	1	2	3	1	2	2	2	1	2
1	2	1	1	2	1	2	1	2	2	4	1	2	2	1	1	2
1	2	1	1	1	1	1	1	2	2	2	1	2	3	1	1	2
1	2	1	1	1	4	1	3	1	3	2	1	2	3	1	1	2
1	3	1	1	2	1	1	1	2	2	2	1	2	2	1	1	2
1	1	1	1	1	2	1	1	1	2	3	1	1	3	1	1	2
1	2	1	2	1	5	1	1	1	1	3	1	1	2	1	1	2
1	2	1	2	2	1	1	1	1	1	2	1	2	2	1	1	2
1	3	1	1	2	4	1	1	1	2	3	1	3	3	2	1	2
1	2	1	1	2	3	1	1	1	3	2	1	1	3	1	1	2
1	2	1	1	2	2	1	1	1	1	2	1	1	3	1	2	2
1	3	1	1	1	4	1	1	1	3	2	1	1	2	2	1	2
1	2	1	1	1	1	2	1	1	3	3	1	2	2	2	1	2
1	3	2	1	1	5	2	1	2	999	4	1	1	2	1	1	1
1	2	1	1	2	1	1	3	1	2	3	1	1	2	1	1	2
1	2	1	2	1	4	2	2	1	1	6	4	999	3	1	1	2
1	2	1	1	1	2	1	2	1	2	3	1	1	3	1	1	2
1	1	1	1	2	1	1	2	1	1	3	2	1	2	1	1	2

1	3	1	1	2	2	2	2	1	2	6	1	1	2	1	1	2
1	2	1	1	2	5	1	2	1	1	1	1	1	2	1	1	2
1	2	1	1	2	4	2	3	1	2	3	1	3	3	1	1	2
1	2	1	1	1	1	2	1	1	3	3	1	1	2	2	1	2
1	2	1	1	1	1	1	1	2	2	3	1	2	2	1	1	2
1	3	1	1	2	1	2	1	1	2	3	1	2	2	2	1	2
1	2	1	1	1	1	2	3	1	2	2	1	2	2	1	1	2
1	2	1	1	1	5	2	1	1	2	3	1	2	2	1	1	1
1	2	1	1	2	5	1	1	2	2	1	1	2	3	1	1	2
1	3	1	1	2	5	2	1	2	2	5	1	2	2	1	1	1
1	2	1	1	1	3	1	2	1	2	3	3	1	2	1	1	1
1	2	1	2	1	4	1	1	2	2	3	1	2	4	2	1	2
1	2	1	2	1	2	2	1	1	2	3	1	1	3	1	1	2
1	2	1	1	2	4	1	1	1	999	2	1	1	2	1	1	2
1	2	1	1	2	2	3	3	1	2	3	4	3	2	1	1	2
1	3	1	2	2	2	1	3	1	2	6	4	3	4	1	1	2
1	2	1	2	1	1	1	1	2	2	2	1	2	3	1	1	2
1	2	1	1	1	2	3	2	1	2	2	1	1	2	2	1	2
1	3	1	1	2	2	1	1	1	3	5	1	2	3	1	1	1
1	2	1	1	2	1	1	3	1	2	3	1	1	3	1	1	2
1	3	1	1	1	5	2	1	1	999	2	1	2	3	1	1	2
1	2	1	2	2	1	1	1	999	2	2	1	2	3	1	1	1
1	3	1	2	2	1	1	1	1	2	3	1	1	3	1	1	1
1	2	1	1	2	1	1	1	1	2	2	1	2	3	1	1	2
1	2	1	1	1	2	2	1	1	3	4	1	2	2	1	1	2
1	2	1	1	2	1	1	1	1	2	3	1	1	2	1	1	2
1	2	2	1	2	4	1	3	2	1	2	1	2	2	2	1	2
1	2	1	1	2	3	1	999	1	1	3	1	1	3	1	1	2
1	3	1	2	2	5	1	2	2	2	3	1	2	2	1	1	1
1	2	1	2	2	5	1	1	1	3	5	3	1	2	1	1	2
1	3	1	1	1	5	1	1	2	3	3	1	2	2	1	1	2
1	2	1	1	1	1	1	3	1	1	3	1	1	3	1	1	2
1	2	1	1	1	4	2	2	1	2	3	1	1	3	1	1	2
1	2	1	1	1	1	1	2	1	3	3	1	1	2	1	1	2
1	3	1	1	1	5	1	3	1	2	2	1	1	2	1	1	2
1	2	2	1	1	5	1	1	2	3	2	1	2	2	1	1	2
1	2	1	1	2	5	1	1	1	3	3	4	1	3	1	1	2
1	2	1	2	1	1	1	3	2	3	3	1	2	2	1	1	2
1	2	1	2	2	4	1	1	1	3	4	3	1	2	1	1	2
1	2	2	1	2	5	1	1	2	1	2	1	2	3	1	1	2
1	2	1	1	2	2	1	1	2	2	3	1	2	3	1	1	1
1	1	1	2	1	2	1	1	1	2	2	1	1	3	1	1	2
1	2	2	1	2	5	2	3	2	1	2	1	2	4	1	1	2
1	1	1	2	2	1	2	1	1	1	1	1	2	2	1	1	2
1	1	1	2	2	5	2	1	2	2	3	1	2	2	1	1	2
1	3	1	1	2	5	1	1	2	2	3	1	2	3	1	1	2
1	3	1	2	1	5	1	1	1	1	3	3	1	3	1	1	2
1	3	1	1	1	1	1	3	2	1	3	3	2	3	1	1	2
1	2	1	2	2	5	1	1	2	1	2	1	2	3	1	1	1

1	2	1	2	1	5	1	1	1	2	3	2	1	2	1	1	2
1	2	1	1	1	1	1	2	1	999	3	2	1	3	1	1	2
1	2	1	1	2	2	2	1	1	3	4	1	2	3	1	1	2
1	2	1	1	2	1	1	1	1	3	3	3	2	2	2	1	2
1	2	1	2	1	1	2	3	2	1	2	1	2	4	1	1	2
1	3	1	2	1	5	1	2	2	1	2	1	2	2	2	1	2
1	2	1	1	1	5	1	1	1	2	3	1	2	3	1	1	2
1	3	1	1	1	2	2	2	1	999	3	3	1	3	1	1	2
1	2	1	1	1	2	1	1	2	2	999	999	999	999	999	999	999
1	2	1	1	2	2	2	1	2	2	2	1	1	3	2	1	1
1	2	1	1	1	2	1	3	2	3	3	1	2	2	1	1	2
1	2	1	1	2	1	1	1	2	2	999	999	999	3	1	1	2
1	3	2	2	2	5	2	1	2	2	3	1	2	3	1	1	1
1	3	1	1	2	4	2	1	3	2	3	1	1	2	1	1	2
1	3	1	1	2	5	1	1	2	2	2	1	2	3	1	1	2
1	2	1	2	2	5	1	2	1	2	5	2	1	2	1	1	2
1	2	1	1	2	2	1	3	1	2	3	4	1	3	999	1	2
1	3	1	1	2	2	1	3	1	2	3	1	1	2	2	1	2
1	2	1	2	2	2	1	3	1	1	3	1	1	3	1	1	2
1	1	1	1	1	4	1	2	1	2	6	1	1	2	2	1	2
1	3	1	2	2	2	1	2	1	1	1	1	2	2	1	1	2
1	2	1	1	2	2	2	1	1	2	2	1	1	2	1	1	2
1	2	1	1	2	5	2	1	1	999	5	1	1	3	1	1	2
1	3	1	2	2	4	2	1	1	2	1	1	1	3	1	1	2
1	3	1	1	1	2	1	1	2	2	2	1	2	4	1	1	1
1	3	1	2	1	4	1	1	1	2	2	1	1	2	1	1	2
1	2	1	1	2	1	1	1	1	2	2	1	1	2	1	1	2
1	2	1	2	2	1	1	1	1	2	4	1	1	2	1	1	2
1	2	1	2	2	5	2	1	1	1	4	2	1	3	1	1	1
1	2	1	1	2	1	1	3	1	2	3	1	3	3	1	1	2
1	2	2	2	2	5	2	1	2	1	3	1	2	2	1	1	3
1	2	1	1	2	2	1	1	2	999	3	1	2	2	2	1	2
1	2	1	1	2	2	1	1	1	3	3	1	1	3	1	1	1
1	3	1	1	1	5	1	1	1	3	5	2	1	3	1	1	1
1	2	1	1	1	5	1	3	2	1	3	1	2	2	1	1	2
1	2	1	1	2	1	2	1	2	2	3	1	2	2	1	1	2
1	3	1	2	2	4	2	1	1	2	2	1	2	2	1	1	2
1	2	1	2	2	5	1	2	1	2	1	1	1	4	1	1	2
1	3	1	2	2	5	1	3	2	2	3	1	2	3	1	1	2
1	3	1	1	1	1	1	1	1	2	2	1	1	2	2	1	2
1	2	1	1	2	1	1	1	1	2	3	1	1	3	1	1	2
1	2	1	2	2	5	2	1	2	3	5	1	2	2	1	1	1
1	2	1	2	1	4	1	1	2	1	3	1	2	2	1	1	2
1	3	1	2	2	5	1	1	1	2	3	1	2	4	1	1	2
1	2	1	1	2	4	2	1	2	1	2	1	2	3	1	1	2
1	3	1	1	1	4	1	1	1	2	3	3	1	2	1	1	1
1	2	1	1	2	5	2	1	2	3	1	1	2	2	1	1	2
1	2	1	1	1	1	2	3	1	1	3	1	1	2	1	1	2
1	2	1	1	2	2	1	3	2	2	2	1	1	2	1	1	2

1	2	1	1	2	5	1	1	1	1	3	3	1	3	1	1	2
1	2	1	1	1	1	1	1	1	2	3	3	1	3	2	1	2
1	2	1	1	2	4	1	3	1	2	3	3	1	3	2	1	2
1	1	1	1	1	1	1	1	1	1	3	1	2	3	1	1	2
1	2	1	1	1	1	1	1	1	3	4	1	2	2	2	1	2
1	2	1	2	2	999	2	2	1	1	3	1	1	3	1	1	2
1	2	1	2	2	2	1	3	2	2	2	1	2	2	1	1	2
1	2	1	1	2	2	1	1	2	2	2	3	2	3	1	1	2
1	2	1	1	1	2	2	1	1	3	3	1	1	2	1	1	2
1	2	1	2	2	1	1	1	1	2	4	2	1	2	1	1	1
1	3	1	1	1	5	2	1	2	3	5	3	2	2	1	1	2
1	2	1	2	2	1	2	1	2	1	3	1	2	3	1	1	2
1	3	1	1	2	5	1	1	2	1	3	1	2	3	1	1	2
1	2	1	2	1	4	2	1	2	2	3	1	2	3	1	1	2
1	2	1	1	2	2	1	3	1	3	3	1	1	3	1	1	2
1	3	1	1	1	4	1	1	1	3	3	1	1	3	1	1	1
1	2	1	1	1	4	1	2	1	3	2	1	999	4	1	1	2
1	2	2	1	2	2	2	1	2	2	2	1	2	3	2	1	2
1	2	1	1	2	5	2	2	1	1	3	2	1	2	2	1	2
1	2	1	1	1	2	1	1	2	1	2	1	2	2	2	1	2
1	3	1	1	2	5	1	1	1	3	3	1	1	2	1	1	2
1	2	1	1	2	1	2	1	1	2	5	2	1	2	1	1	2
1	3	1	1	2	4	1	3	1	2	3	1	1	3	1	1	1
1	2	1	2	2	5	2	1	2	2	3	1	2	2	1	1	2
1	3	1	1	2	1	1	1	1	1	2	1	2	3	1	1	2
1	2	1	1	1	5	1	2	1	3	2	3	1	2	1	999	2
1	2	1	2	2	5	1	2	1	3	5	1	1	3	1	1	2
1	2	1	1	1	1	2	1	2	3	3	1	2	2	1	1	2
1	2	1	1	1	5	1	2	1	2	4	1	1	3	1	1	2
1	2	1	1	1	1	1	1	1	2	1	1	1	3	999	1	1
1	2	1	1	2	1	2	2	3	2	3	1	3	3	1	1	2
1	2	1	1	2	1	2	1	1	2	3	1	1	2	1	1	2
1	2	1	1	2	1	1	3	1	3	2	1	1	999	999	999	999
1	2	1	2	2	5	1	1	1	2	4	1	1	3	1	1	2
1	3	1	1	2	4	2	3	1	3	5	1	1	3	1	1	2
1	1	1	2	2	5	1	3	1	1	3	1	2	3	1	1	2
1	3	1	2	2	1	1	2	1	3	2	1	2	2	1	1	2
1	3	1	1	2	5	2	2	2	1	3	1	2	2	1	1	2
1	2	1	1	2	5	1	2	1	1	4	1	2	2	1	1	2
1	3	1	1	2	1	1	1	2	2	3	1	2	3	1	1	2
1	2	1	1	1	1	1	1	2	2	3	1	2	2	2	1	2
1	2	1	1	1	2	1	1	2	2	3	1	2	3	1	1	2
1	2	1	1	2	1	2	1	2	3	3	1	2	4	2	1	2
1	2	2	1	2	1	2	1	1	2	1	1	1	2	1	1	2
1	1	1	1	2	1	2	1	1	1	3	1	1	2	1	1	2
1	3	1	1	2	4	2	1	2	3	2	1	2	2	2	1	2
1	3	1	1	1	5	1	1	1	3	5	3	1	2	1	1	2
1	2	1	1	2	5	2	3	2	999	2	1	2	2	1	1	2
1	2	1	1	1	1	1	3	1	2	3	1	1	2	1	1	2

1	2	1	1	1	2	1	1	2	2	5	1	1	3	1	1	2
1	1	1	2	2	5	1	1	1	2	3	1	1	3	1	1	2
1	3	1	1	1	5	1	3	1	1	3	1	2	3	1	1	2
1	3	1	1	1	1	2	1	1	3	1	1	1	2	2	1	2
1	2	1	2	2	2	2	2	1	3	2	1	1	2	1	1	2
1	2	1	2	1	1	1	1	2	1	2	1	2	2	1	1	1
1	2	1	1	2	1	2	3	1	2	2	3	1	2	1	1	2
1	2	1	1	2	1	1	1	1	3	4	1	1	3	1	1	2
1	3	1	1	1	1	1	1	1	2	2	1	2	2	1	1	2
1	2	1	1	1	4	2	2	2	2	2	1	2	3	1	1	1
1	2	1	1	1	4	1	1	2	3	3	1	2	2	1	1	2
1	3	1	1	2	1	2	1	2	3	1	1	2	2	2	1	2
1	2	1	2	1	1	1	1	1	3	2	1	1	2	1	1	2
1	2	1	1	2	5	1	1	2	2	3	1	2	3	1	1	1
1	2	1	1	1	1	1	2	1	2	3	3	1	3	1	1	2
1	2	1	2	2	5	1	1	2	2	6	1	1	3	1	1	2
1	2	1	1	1	2	1	1	2	3	2	1	1	3	1	1	2
1	3	1	1	2	5	1	1	1	2	2	1	1	2	1	1	2
1	2	1	2	2	5	1	1	1	2	2	1	1	2	1	1	2
1	3	1	1	2	5	1	1	2	1	3	3	999	2	1	1	1
1	3	1	1	1	2	2	3	1	2	3	1	1	2	1	1	2
1	3	1	1	2	5	1	1	1	999	3	1	1	3	1	1	1
1	1	1	1	1	2	1	1	1	3	3	1	1	2	2	1	2
1	2	1	1	2	1	1	2	1	2	1	1	2	3	1	1	2
1	3	1	1	2	2	1	1	1	2	3	2	1	4	2	1	2
1	2	1	2	2	5	1	1	2	2	1	1	2	3	1	2	1
1	2	1	1	2	4	2	1	1	2	2	1	2	3	1	2	2
1	2	1	1	2	5	1	1	2	1	3	1	2	2	1	1	2
1	2	1	1	1	4	2	1	2	3	3	1	2	3	1	1	1
1	2	1	1	2	2	2	1	2	1	2	1	2	2	1	1	2
1	2	1	1	2	1	1	3	1	1	2	3	1	2	1	1	2
1	2	1	1	2	5	1	1	2	3	2	1	1	3	1	1	2
1	3	1	1	1	2	2	3	1	999	2	1	1	3	1	1	2
1	2	1	2	2	2	1	3	1	1	3	1	1	3	1	1	2
1	2	1	2	2	1	2	1	1	2	2	1	1	3	1	2	2
1	2	1	1	2	1	1	1	1	2	1	1	1	2	2	1	1
1	3	1	1	2	5	1	1	1	3	1	1	1	3	1	1	2
1	2	1	1	2	5	1	1	1	2	4	1	2	4	2	1	2
1	2	1	1	1	2	1	2	2	999	2	1	2	3	1	1	2
1	2	1	1	1	1	1	1	2	3	2	1	1	3	1	1	2
1	2	1	1	2	2	1	1	1	3	3	1	1	3	1	2	2
1	2	1	1	2	4	1	1	1	999	3	1	1	3	1	1	1
1	3	1	2	2	5	1	1	1	2	3	1	2	2	1	1	2
1	2	1	1	2	5	1	3	1	3	4	1	1	3	1	1	2
1	3	1	1	2	4	2	1	1	3	3	1	1	3	1	1	2
1	2	1	1	2	5	2	1	2	2	2	1	2	3	1	1	2
1	2	1	2	2	5	1	3	1	2	5	1	1	3	1	1	2
1	2	1	1	1	2	1	2	2	3	2	1	2	3	2	1	2
1	2	1	2	2	5	2	1	2	2	3	1	2	2	1	1	2

Bibliography

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. [Electronic Version]. *Association for Computing Machinery. Communications of the ACM., 42*(12), 40-7. Retrieved May 24, 2004, from the ABI/INFORM Research database.

Armstrong, I. (2003). "Passwords exposed users are the weakest link." Scmagazine. June 2003. Accessed: Dec 2004, http://www.scmagazine.com/scmagazine/2003_06/cover/index.html.

Air Force Personnel Center, (2005). Randolph AFB, TX. Service Demographics, Release No. 007.

Beedenbender, M. G. (1990). *A Comparison of Password Techniques* (Masters ed.). MONTEREY CA: NAVAL POSTGRADUATE SCHOOL. Retrieved May 24, 2004, from http://stinet.dtic.mil/

Bohm, N., Brown, I., Gladman, B. (2000). Electronic Commerce: Who Carries the Risk of Fraud? (3) *The Journal of Information, Law, and Technology*.

Gehringer, E. F. (2002). Choosing passwords: security and human factors. [Electronic Version]. *2002 international symposium on technology and society (ISTAS'02). Social implications of information and communication technology.* Piscataway, NJ, USA, Retrieved May 25, 2004, from the Inspec database.

Davis, D. and Price, W. (1987) *Security for Computer Networks*. Chichester: Wiley.

DeAlvare, A. (1998). A framework for password selection. In *Proceedings of Unix Security Workshop II*. Portland.

Department of the Air Force. *Identification and Authentication*. AFM 33-223. Washington: HQ AFCA, 19 June 2004.

Experts: Phishing more sophisticated, (2005). CNN.com. Accessed: Jan 20, 2005. http://www.cnn.com/2005/TECH/internet/01/20/tech.phishing.reut/index.html

FIPS (1985). *Password Usage.* Federal Information Processing Standards Publication. May 30, 1985.

Garfinkel, S. & Spafford, G. (1991). Practical UNIX Security, Sebastopol, CA: O'Reilly & Associates, Inc., p. 35.

Gehringer, E. F. (2002). Choosing passwords: security and human factors. [Electronic Version]. *2002 international symposium on technology and society (ISTAS'02). Social implications of information and communication technology*. Piscataway, NJ, USA, Retrieved May 25, 2004, from the Inspec database.

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers and Security, 14*, 377–383.

JMP (2003). Version 5.1, Computer Software. SAS Institute Inc., Cary NC.

Kruck, S. E., Sciandra, J. R., and Forcht, K. A. (2001). New concepts in password management. [Electronic Version]. *Journal of International Information Management, 10*(2), 37-44. Retrieved May 25, 2004, from the Inspec database.

Leedy, P., and Ormrod, J. (2001). *Practical Research: Planning and Design*. (7th Ed.). Upper Saddle River, NJ: Merrill Prentice Hall.

Microsoft Excel (2003). Version 2003, Computer Software. Microsoft Corporation, Redmond WA.

Microsoft Corporation (2004). *Creating Stronger Passwords*. From: http://www.microsoft.com/athome/security/privacy/password.mspx

Mitnick, K. (2002). The Art of Deception. Indianapolis: Wiley.

National Infrastructure Protection Center. (2001). *Password protection 101*. Washington, D.C.: National Infrastructure Protection Center. from http://purl.access.gpo.gov/GPO/LPS19697

Neumann, P. G. (1994). Risks of passwords. [Electronic Version]. *Association for Computing Machinery. Communications of the ACM., 37*(4), 126-1. Retrieved May 24, 2004, from the ABI/INFORM Research database.

Spafford, E., (1992). Opus: Preventing Weak Password Choices, *Computers & Security*, 11, 273-278.

Wakefield, R. L. (2004). Network security and password policies. *The CPA Journal, 74*(7), 6. Retrieved August 8, 2004, from the ABI/INFORM Research database.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2000). The Memorability and Security of Passwords – Some Empirical Results. Technical Report No. 500, Computer Laboratory, University of Cambridge.

Zviran, M. and Haga W.J. (1999), "Password Security: An Empirical Study", *Journal of Management Information Systems* (JMIS), Vol. 15, No. 4, pp. 161-185.

Vita

First Lieutenant Kurt William Martinson graduated from James Martin High School in Arlington, Texas. He entered undergraduate studies at the United States Air Force Academy in Colorado Springs, Colorado where he graduated with a Bachelor of Science degree in Management in May 2001.

His first assignment was at RAF Lakenheath, United Kingdom as a communications officer. While stationed in England, he deployed to Pakistan as the aid to a base commander during Operation Enduring Freedom. In August 2003, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
21-03-2005	**Master's Thesis**	Oct 2004 – Mar 2005

4. TITLE AND SUBTITLE

Passwords: A Survey on Usage and Policy

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Martinson, Kurt W., 1st Lieutenant, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05M-11

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research was to see how individuals use and remember passwords. Specifically, this thesis sought to answer research questions addressing if organizational parameters are influencing behaviors associated with password choice and to what effect. Volunteers answered the research questions via a web-survey. The research identified the need for an evaluation of how organizations limit password choice by setting parameters for individuals.

15. SUBJECT TERMS

Passwords, Security, Patters, Memory Techniques, Authentication

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dennis D. Strouble, Dr. (ENV)
U	U	U	UU	74	19b. TELEPHONE NUMBER *(Include area code)* (937) 785-3355; e-mail: dennis.strouble@afit.edu

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