PASSWORD SECURITY: WHAT FACTORS INFLUENCE GOOD PASSWORD PRACTICES

Troy Touchette
Associate Professor
Computer Information Systems
San Antonio College
1300 San Pedro Ave.
San Antonio, TX 78212
ttouchette@alamo.edu

Barbara Hewitt
Assistant Professor of Computer Information Systems
School of Business
Texas A&M University-San Antonio
One University Way
San Antonio, TX 78224
210-784-2311
barbara.hewitt@tamusa.tamus.edu

Mark L. Huson
Assistant Professor of Computer Science
and Computer Information Systems
School of Business
Texas A&M University - San Antonio
2601 Louis Bauer Drive
San Antonio, TX 78235
210-784-2313
mark.huson@tamusa.tamus.edu

ABSTRACT

This study will explore variances in password strength across demographics such as age, gender, ethnicity, and education level; organizational password rules; and security training. It also determines the degree to which the individual perception of security threats impacts password strength. By using both personal and employment based accounts, the study will examine whether individuals perceive personal or organizational security as more important. It will also investigate whether the type of account influences password selection. A proposed model for password selection will be described and used to determine if individuals select stronger passwords for accounts with password rules if they understand the risks involved in choosing poor passwords.

INTRODUCTION

Computer security is a formidable challenge and will continue to be so for the foreseeable future. In 2010, the number of attacks utilizing the Internet nearly doubled, and the count of new vulnerabilities was higher than any previously recorded year (Cole 2011; Greenemeier 2011). Attacks are designed to breach one or more parts of the fundamental security concepts of confidentiality, integrity, and availability. These concepts can be applied equally to both information and to the systems we use to store, process, and transmit it.

As a complicating factor, most individuals fail to recognize that devices such as mobile phones, cars, and other products with embedded controllers are essentially computers that, if not secured, run the risk of being compromised. The undesirable consequences of a compromise include Denial of Service (DoS), loss of confidentiality and even remote control of those devices by an attacker (Greenemeier 2011).

A key method of maintaining security is controlling access, which is done by allowing access only to those who are authorized. Authentication is the process of confirming the identity of an entity (human or not) before allowing access and is relevant to everyone from corporate system administrators down to home computer users. The three forms of authentication include something you know (passwords), something you are (biometrics) and something you have (card). The most common form of authentication is the username and password combination (Cole 2011).

Passwords are the one security component an average user is able to control. The average college senior exercises this control for 13 websites (Gaw and Felten 2006) which is the same as for many technology professionals (RSA 2005). Once selected, the security of that password is typically beyond the user's control. For instance, users are not able to determine whether passwords are encrypted while being transmitted to websites that require their authentication. In addition, they seldom are able to determine how passwords are stored on each site. This is an issue that must be entrusted to an unknown website administrator or programmer. All too often this trust is misplaced.

In one example, the social entertainment site, rockyou.com, lost over 32 million of its users' passwords due to an SQL injection flaw. The site also stored all passwords as plain text making them easy to steal no matter how strong the password was when picked by the individual user (Imperva 2009). In another instance, Amazon.com truncated passwords to eight characters before encrypting and storing them. Though Amazon later encrypted the entire password, users were not forced to change their passwords, allowing attackers to focus on accounts where passwords had not been changed after the encryption functionality was updated (Murphy 2011). This would allow an attacker access to an account by entering the first eight characters, for example, "password," even if the true password was "password123" or even "password$ecur3".

In addition, some sites also allow many or unlimited logon attempts without locking user accounts. Presumably, this will keep their clients from becoming frustrated. The risk is that attackers are not limited in their attempts at guessing passwords (RSA 2005).

Users play a vital role in handling their own security in some critical areas. They are at least in partial control when selecting passwords. While some limitations are imposed by authentication

systems like minimum password length and character set selection requirements, the primary responsibility of choosing a good password falls on the user.

Many problems exist with password security. Some of these problems will be exacerbated in the years to come as the number of security breaches continues to rise. For example, the two techniques for cracking passwords include dictionary attacks and brute force attacks. Dictionary password cracking routines use all words in a preset list to identify passwords. Brute force attacks use all possible combinations in a selected character set for different length passwords to identify passwords.

There are several other ways for users to lose passwords. Users should be aware of shoulder-surfing, a technique which simply involves watching the user type in an attempt to discover a password or clues that might reveal information about it. Redirecting users to fake logon pages, known as phishing, can also be used to gain logon credentials fairly effectively as attested to by the loss and subsequent posting of about 34 thousand MySpace passwords (Schneier 2006). Writing down a password can also compromise security. Although written passwords might require an attacker to be close enough to see it, electronically stored passwords could be found remotely through the network. In one study, 25% of respondents admitted storing passwords in a spreadsheet or similar document (RSA 2005).

The dilemma facing the user is typically choosing a long/strong password which could be forgotten or a short one that could be easily attacked. One factor complicating this predicament is that most users have more than one password to remember. RSA (2005) found that more than a fourth of users surveyed had thirteen passwords or more needed during the course of their work In a 2007 a password habits study that used data collected from a browser toolbar component revealed users had an average of 25 online accounts where passwords are used but an average of only 6.5 different passwords which highlights the issue of password reuse (Florencio and Herley 2007). While using the same password for multiple accounts makes it easier for users to remember their passwords, it has an obvious flaw. Once the reused password is identified, perhaps on one of the weaker systems, attackers can attempt to authenticate as the user on other systems using the same password. Another potential setback for users is loss of access due to forgotten passwords. It is estimated that 1.5% of Yahoo users forget their passwords every month (Florencio and Herley 2007).

Many studies on passwords have separately explored how demographics including training (Weber, Guster et al. 2008), age (Schneier 2006), education (Weber, Guster et al. 2008), and system importance (Gaw and Felten 2006; Kaplan 2009) affect password selection. These factors were not studied within one study and thus the goal of this research is to determine if demographic factors including training, education, age, ethnicity, gender, computer experience, and prior secure password experience affect the individual's belief that system security and strong passwords are important. The study will provide organizations and security professionals with implications of how demographics and prior computer and password strength experience affect an individual's belief that the importance of a system's security and how selecting a strong password is impacted by this belief.

LITERATURE REVIEW

Dictionary attacks are often successful. Klein (1990) and Cazier and Medlin (2006b) found that roughly 25% of passwords were dictionary words in separate studies. This suggests that the problem of users picking weak passwords has not changed much over time. One possible misconception that leads to this continued practice is that slang, proper names, and keyboard sequences like "qwerty" are good passwords since they are not found in a standard dictionary. This could explain why nearly 50% of the passwords from the rockyou.com incident are often included in hacker dictionaries and 20% could be found in a dictionary created from only the 5,000 most popular passwords (Imperva 2009). As new practices are developed, like substituting letters in a word with similarly shaped numbers, so "password" might be represented as "pa55w0rd", dictionaries are also adapted to compensate (Cazier and Medlin 2006b). Another concern is that the use of the term "password" may influence users to select dictionary words since the word "word" is in the name "password".

Brute force attacks use all possible combinations of characters in a set to find passwords. So for a password containing only letters, the single letters "a" through "z" might be guessed first, followed by double letter combinations "aa", "ab", "ac" through "zz" is tried, followed by triple letter combinations, etc. Each letter added to a password increases the possible combinations exponentially. In addition to length, the number of different character sets used in a password increases the possible combinations. A lower case, letter only password containing 8 characters will provide 26 characters in 8 possible positions or 26^8 or a little less than 208 billion possible combinations. By adding 10 numerical digits to the character set, we get 36 possible characters for 8 possible positions or 36^8 or a little over 2.8 trillion possible combinations which represent a significant difference in the number of guesses and the amount of time that is needed to crack a password.

The only impediment to this process may be time. However, as processing speeds of computers continue to increase, the need for longer, more complex passwords increases in order to sufficiently ward off brute force password attacks. With the advent of distributed and cloud computing where processing is performed by a network of computers rather than a single machine, the issue of brute force attacks becomes compounded as demonstrated by the use of Amazon's cloud computing service to crack Wi-Fi Protected Access (WPA) encryption (Liebowitz 2011).

By the nature of computer systems, any penetration in one part of the system could expose other areas for possible exploitation. For example, an intruder used the word "happiness" as a password to gain access to a Twitter employee's account which granted the right to reset passwords to any other account on the system. This simple breach allowed the hacker to compromise many high-profile accounts, including President Barack Obama and some news sites (Carr 2009).

Most users are not doing a good job of selecting secure passwords. So what is a good or strong password? Most concepts of a strong password suggest that it is one that is hard to crack. Cazier and Medlin (2006b) used a human based rating scale for passwords consisting of 5 levels that

vary according to makeup, and used password cracking as a technique for testing. In another study, Cazier and Medlin (2006a) found that the majority of participants (59%) chose common words with over 43 percent using names of a significant other, pet, or child.

Actual cracking would seem to be a very good test of password strength but could be skewed depending on factors like what encryption method was used to hash the passwords. For example, using the Lan Manager Hash in Windows XP which contains a few well know implementation flaws, including splitting passwords into two 7 character hashes, may indicate that some passwords are less secure than they would be if implemented with a different hashing function. LAN Manger was replaced by NTLM in Windows NT SP4, replaced by Kerberos in Windows 2000, and completely disabled in Windows Vista.

Cracking results may also depend on the software used, the size and quality of the dictionary used, and to some extent the experience of the individual. Some, including Florencio and Herley (2007) use an entropy based method to rate the potential strength based on character set diversity and password length, specifically the rating is the base 2 logarithm of the alphabet size raised to the power of the length of the password. This is more of a theoretical password strength rating and gives a good indicator of how difficult a password would be to crack using a brute force attack. However, it does not fully take into account a dictionary style attack where a fairly long word would receive a good rating but for practical purposes could be guessed in a very short amount of time.

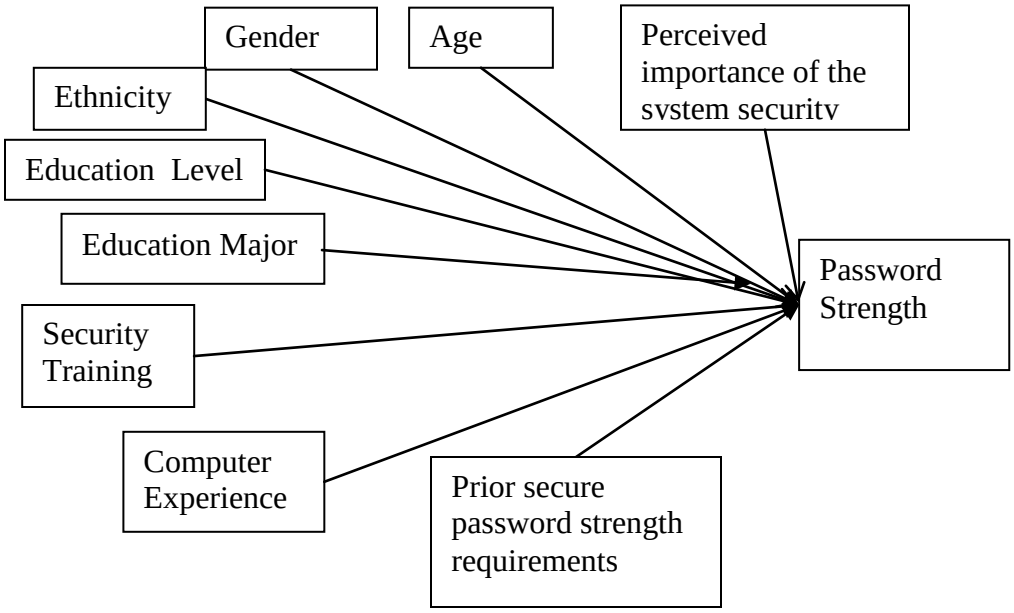
The question remains what determines whether a user is likely to select a strong password. Not surprisingly, one study finds that users who are information systems majors or users who receive training dealing with password selection create stronger passwords than those who do not receive training (Weber, Guster et al. 2008). The importance of the system to the user is related to the strength of the password chosen (Gaw and Felten 2006; Kaplan 2009). Password strength rules can certainly increase complexity but may force users into unsafe practices like writing down or storing electronic copies of passwords in plain text. The studies that worked with real world data captures do not appear to contain any demographic data or additional information to indicate user motivations. Schneier (2006) suggests the strength of passwords found in the MySpace data set indicates younger users select better passwords. Unfortunately, this evidence is only anecdotal since no demographic data was linked with password data.

In a study that explored mandatory password changes at a university, Belanger, Collignon, Enget, Negangard (2011) found that perceived security threat did not influence individual's decision to comply with a mandated password change requirement if they perceived they were vulnerable. Herath and Rao (2009) found that employees underestimated the threat of security breaches. LaRose, Rifon, and Enbody (2008) found that individuals are more likely to engage in safe behavior if they perceived they are personally responsible. Anderson and Agarwal (2010) found that individuals who were concerned with security threats positively affected their attitude toward security behavior.

MODEL

The goal of this study is to determine which demographic factors influence perceived importance of security for a system as well as the selection of strong passwords. Several factors will be explored including age, gender, ethnicity, educational major, and education level as well as computer experience, computer expertise, security training on passwords, and perceived importance of system. Data collection will be accomplished by completion of a survey. Individuals will be asked to self-rate their computer experience and expertise from beginner to expert as direct measurement of these factors is beyond the scope of this work. Security training will be evaluated with questions that determine whether password selection training was included and when the training took place. Perceived importance of the system to the user or perceived security threat was shown to be related to password selection and should be evaluated to separate it from other factors. The following model will be tested.

Figure 1. Demographic Affect on Perceived System Security Implications Model



RESEARCH METHOD

A survey will be used to collect the information needed for the study. While collecting actual passwords from live systems would be preferable, the privacy and security issues involved would create a significant challenge to finding potential sources. Individuals will be asked to provide passwords that they would consider using for several types of accounts including:

- Yahoo.com
- Amazon.com
- Their Bank
- Second Bank account
- Facebook

- LinkedIn
- Blog
- Personal email account
- Work email account (not working must be an option)
- Work database (no policy enforcement)
- Work database (password policy enforcement)

Questions will be included to determine computer expertise, recent security training, system importance, and password secrecy.

Passwords will be rated according to the formula:
$$\text{PasswordStrength} = \log_2(\text{AlpabetSize}^{\text{PasswordLength}}) \quad (1)$$

A password cracker will also be used as a practical measure of passwords. Differences of strength will be observed when using a standard dictionary, a larger dictionary, hybrid (where characters may be added to standard words), and brute force.

Password strengths will be compared for differences according demographic groups. Those with recent training may be treated separately if there seems to be significant influence. Numbers of forgotten and written down passwords will be compared against rule complexity.

CONCLUSION

Individuals are the weakest security link and passwords are the most common security decision individuals make in protecting systems. Organizations are vulnerable to system breaches based on the individuals who access their systems. Employees and other system users may believe that the organization's computer systems are not important or not vulnerable based on their password choice. They may not realize the need to protect the systems via the creation of strong passwords. This research will explore whether organizations can mitigate against this threat by offering training. It will also determine if individuals recognize the importance of securing certain systems. It also determines whether any demographics play a role in strong password selection.

Limitations

The limitations on this study include that the data will be gathered via a survey. While the goal of the research is to determine the individual's perception of the importance of securing different types of systems that they access, the data gathered is not in the real world and thus respondents can choose to provide realistic answers.

Contributions

This research will explore how a wide range of demographic factors affect password selection and perceived system security for different types of computer. For academic researchers, it is important because it adds to the password and security research basis by answering questions about what demographics influence a user's perception of system security importance.

This research will also contribute to the practical research by informing organizations of the individual's perception of importance of securing worksite databases and email accounts. It will give organizations a better understanding of what demographic factors influence an individual's choice of a secure password.

REFERENCES

Anderson, C. L. and R. Argawal (2010). "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions." MIS Quarterly **34**(3): 613-643.

Belanger, F., S. Collignon, et al. (2011). User Resistance to the Implementation of a Mandatory Security Enhancement. The Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13, Virginia Tech, Blackburg, Virginia.

Carr, J. (2009). "Twitter Trouble." Information Today: 2.

Cazier, J. A. and B. D. Medlin (2006a). "Password Security : An Empirical Investigation into E-Commerce Passwords and Their Crack Times." Information Systems Security **15**(6): 45-55.

Cazier, J. A. and B. D. Medlin (2006b). "How Secure Is Your Information System? An Investigation into Actual Healthcare Worker Password Practices." Perspectives in Health Information Management **3**(7).

Cole, E. (2011). Protecting Your Passwords. OUCH!, SANS Securing the Human.

Cole, E. (2011). "Protecting Your Passwords." OUCH!

Florencio, D. and C. Herley (2007). A Large Scale Study of Web Password Habits. International Conference on World Wide Web, New York, NY, ACM.

Gaw, S. and E. W. Felten (2006). Password Management Strategies for Online Accounts. Symposium On Usable Privacy and Security (SOUPS). Pittsburg, PA.

Gaw, S. and E. W. Felten (2006). Password Management Strategies for Online Accounts. Symposium On Usable Privacy and Security (SOUPS. Pittsburg, PA.

Greenemeier, L. (2011). Highway robbery: Car Computer Controls Could Be Vulnerable to hackers. Scientific American.

Greenemeier, L. (2011). "Highway Robbery: Car Computer Controls Could Be Vulnerable to Hackers: Scientific American." Science News, Articles and Information.

Hearth, T. and H. R. Roa (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations," European Journal of Information Systems **18**(2): 106-125.

Imperva (2009) "Consumer Password Worst Practices." The Imperva Application Defense Center (ADC). http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Kaplan, D. (2009). "IPhone Worm Plays Prank, but Signals Danger Ahead." SC Magazine.

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

LaRose, R., N. J. Rifon, et al. (2008). "Promoting personal responsibility for internet safety." Communication of the ACM **51**(3): 71-76.

Liebowitz, M. (2011). Your Home Wi-Fi Network Can Be Hacked in Minutes. Security News Daily.

Murphy, D. (2011). Change Your Older Password to Thwart Amazon Security Flaw. PC Magazine.
RSA. (2005, Sept 27). "RSA Security Survey Reveals Multiple Passwords Creating Security Risks and End User Frustration." Retrieved Apr 25, 2011, from http://www.rsa.com/press_release.aspx?id=6095.
Schneier, B. (2006). "MySpace Passwords Aren't So Dumb." Wired.com.
Schneier, B. (2006). MySpace Passwords Aren/t So Dumb. Wired.
Weber, J. E., D. Guster, et al. (2008). "Weak Password Security: An AEmpirical Study." Information Security Journal: A Global Perspective **17**(1).
Weber, J. E., D. Guster, et al. (2008). "Weak Passwords Security: An Empirical Study." Information Security Journal: A Global Perspective **17**(45-54).