How Secure Is Your Information System? An Investigation into Actual Healthcare Worker Password Practices

by Joseph A. Cazier, PhD; and B. Dawn Medlin, PhD

Abstract

For most healthcare information systems, passwords are the first line of defense in keeping patient and administrative records private and secure. However, this defense is only as strong as the passwords employees chose to use. A weak or easily guessed password is like an open door to the medical records room, allowing unauthorized access to sensitive information. In this paper, we present the results of a study of actual healthcare workers' password practices. In general, the vast majority of these passwords have significant security problems on several dimensions. Implications for healthcare professionals are discussed.

Key Words: privacy, passwords, user behaviors, information security

Introduction

Most healthcare computer systems require some type of password authentication. Unfortunately, there are numerous problems that can make this type of authentication a poor line of defense, including weak passwords, improper password storage, and passwords that are captured through social engineering techniques. These problems can lead to unauthorized access of computer systems and could potentially compromise a patient's information.

For security, employees must use both length and strength in their creation of good passwords. This includes the use of a combination of numbers, alpha characters, and special symbols. Weak passwords do not include the aforementioned character sets and are composed of commonly used words or phrases, which can be easily cracked.

In this paper, we will examine the passwords created by employees of a healthcare agency. Through an empirical analysis of the passwords, the factors of length and strength are observed.

Passwords

Passwords are the gatekeepers to a patient's information on many healthcare agencies' computerized systems. The use of short, self-selected passwords by employees is convenient but can soon create problems, such as making it easier for hackers to enter into the agency's computerized system. Unfortunately, the capacity of human memory to remember a sequence of items is temporally limited, with a short-term capacity of around seven items plus or minus two.[1] When humans remember a sequence

of items, those items cannot be drawn from an arbitrary and unfamiliar range but must be familiar "chunks," such as words or familiar symbols, as the human memory thrives on redundancy. In fact, studies have shown that an individual's short-term memory will retain a password for approximately 30 seconds, thereby requiring individuals to attempt to memorize their passwords immediately.[2] This attempt is often ineffective, leading to weak or redundant passwords.

Weak Passwords

The definition of a weak password includes any word that may appear in a dictionary or words that only utilize letters and no other type of special character. As an example, nouns or proper names are poor choices for passwords, including nicknames or the names of famous sports teams, movie stars, or popular cartoon characters. These passwords are weak because they can be easily cracked through the use of software or identified through a technique known as social engineering.

Social engineering is the process of using social skills to convince individuals to reveal facts that may assist the hacker in obtaining access to unauthorized systems.[3] Hackers can obtain information from the end user by pretending to innocently ask questions about hobbies, the date of birth of family members, or the user's telephone number or address. Social engineering therefore enables hackers to obtain enough information to make at least an educated guess of the employee's password.

New social networking sites, such as www.myspace.com or www.facebook.com, further compound the privilege of information problem. As individuals increasingly provide personal information on these types of searchable Web sites, hackers are able to learn a great deal more about their targets, thus increasing the chances of guessing their passwords.

Prior to the development of search engines, individuals who were interested in obtaining information about another person might do so by looking in the phone directory or by picking up an individual's mail. Today, hackers and social engineers can obtain information by "googling" someone. Google's search and information-retrieval capabilities enable hackers to easily obtain personal information, often from a comfortable and anonymous distance. Google is just one of the services that indexes web pages on the Internet, not only acquiring information but integrating it into databases, saving individuals' phone numbers and addresses, as well as directions to their homes.

Password Cracking

Passwords can be cracked through a variety of methods, with the simplest method being the use of a dictionary or word list. Electronic dictionaries exist currently for a variety of languages that include English, Spanish, French, and many other foreign languages. Dictionaries also exist that contain words from TV shows, movies, music, sports, and numerous hobbies.

Whereas dictionaries or word lists rely on speed, the second method of password cracking relies purely on power. The brute force attack method attempts to crack the password by simply comparing every possible combination and permutation of characters available until it finds a match for the password. Once a password is cracked, it could allow the hacker to assume the legitimate user's identity, thereby allowing access to all data that the legitimate user is authorized to view. Even worse, the hacker may be able to escalate those privileges and take control of the entire network.

The reason that most software cracking programs are so very effective is that they usually attack an institution's passwords en masse. No one may know which specific person at a company is a Michael Jordan fan, but among 1,000 people in the United States, the probability that at least one is a Michael Jordan fan and has a related password is fairly high. The same is true with other famous sports stars or teams.[4]

In contrast to weak passwords, governmental agencies such as the Department of Defense and organizations such as the Computer Emergency Response Team (CERT) have provided guidance on the

creation of good passwords. These found that passwords are made more secure by adding both length and strength.

Good Passwords

Good password practices can be effectively applied to health care agencies' computerized systems. One such practice is disallowing passwords that consist of common, everyday words and requiring the passwords to incorporate as many different characters as possible.[5] Users can achieve this through the mixing or mingling of characters from the various character sets such as A, B, C or a, b, c; special characters such as $, ?, &; alt characters such as µ, £, ϕ; and numbers such as 1, 2, 3.

As would be expected, a strong password requires a certain degree of complexity so that it cannot be easily cracked, and length is one of the ways of introducing complexity.[6] Length means that the longer a password, the longer the time it takes to crack. Simply put, longer is better.

Analysis

Data Collection

This study analyzed the passwords of 90 active employees that were obtained from the technology officer of a healthcare department in the spring of 2006. Employees are required to enter their user ID and password on a PC, which the system processes and compares to the entries it has stored. If it finds a match, the employee will be given access to the computer system, but if there is no match, the employee will not be allowed access and will have to contact the technology officer after three unsuccessful login attempts. Employees were not told that the dataset would be analyzed, therefore allowing the researchers to have access to their current password choices. This particular agency did not enforce any particular password rules or suggest password guidelines. Because of a lack of rules and/or guidelines, passwords collected are of particular interest, as they show current healthcare workers' password security practices when left to their own devices and without being required by a network or other administrator to create a "good" password.

Rating Instrument

To assess the security level of the selected passwords by employees at a healthcare agency, the researchers reviewed current best practices for password security.[7-9] Next, the researchers aggregated the guidelines into an instrument that was used to rate the security level of each password. A series of dichotomous yes or no questions were used around the guidelines, both positive and negative. From these questions, a standardized scoring system was used based on work developed and validated by Medlin and Cazier.[10]

For the scoring system, eight questions concerning the positive recommendation of what people "should be doing" according to best practices were identified, and an additional eight concerning negative "what not to do" practices were identified. Researchers then rated and cross-checked each actual password based on the scoring system. Next, an aggregate score was designed for the positive and negative practices by assigning a 1 or a 0 to the password for each question and summing the scores for each section. A final score was assigned by subtracting the overall negative score from the overall positive score. Since there were eight positive questions and eight negative questions, this provided a theoretical range of -8 and +8 for the overall score. It also allowed the researchers to both look at the overall password security level and identify specific strengths and weaknesses on each guideline.

Reviewing the results of the questions on positive and negative password practices in table 1 and 2, we see that a very small percentage of employees are using most of the best practices as recommended by governmental, educational, and private organizations. For example, most users (64.4 percent) did not use both upper- and lowercase passwords. Of those who do use upper- and lowercase passwords, the vast majority of those (78.2 percent) do so only in logical places, such as in capitalizing a name. Capitalizing the first letter of a name may in fact be worse than not capitalizing them at all, since the inclination for someone trying to guess the password would be to capitalize in logical places. To add maximum security,

passwords need to be capitalized in odd or differing places where someone would not expect them to be. Only a small percent (7.8 percent) of the healthcare workers sampled actually used this method of capitalizing letters.

In addition to using a mix of upper- and lowercase letters, most experts recommend having a combination of letters and numbers. In our case, less than a fourth (24.4 percent) used both letters and numbers. Of those who used letters and numbers, the vast majority (82.0 percent) only used numbers at either the beginning or end of the word. While this is better than having only letters or numbers, it is not as strong as the 4.4 percent whose password had letters and numbers commingled. Passwords with letters and numbers only at the end or beginning are easy to crack with a hybrid-dictionary attack, which takes common words and adds numbers before and after. They are also easier to guess than mixed-order alphanumeric passwords. On the upside, almost all the users (85 percent) had passwords of at least six characters long; however, only 32.2 percent had passwords with eight or more characters.

In relationship to the negative questions, the great majority of the employees, 58.9 percent, appear to be using common words that can be found in any English language dictionary, thus making them very susceptible to dictionary attacks or password guessing. Of even greater concern, 43.3 percent of all passwords appear to be the name of a person. These are usually the easiest of all to guess, as they are likely someone close to the person such as a significant other, pet, or child. Most of this information could be obtained fairly easily through social engineering techniques.

Another common threat is having the user name the same (4.4 percent) or similar (11 percent) to the password. This reduces the value by NOT requiring that the person know or remember two sets of characters. One added security problem with the aforementioned scenario is that a great majority of the time the username is displayed as text at login, which can be easily shoulder surfed or found by a hacker on the system.

Future Research and Recommendations

The present study offers opportunities for future research to more fully examine other variables and factors that may contribute to a safer environment for patient data. Since the study was restricted to a single agency, with 90 possible participants available for the study, a limitation was the small sample size of the above-mentioned criteria. Even thought the results sample is large enough to be statistically significant, future research could benefit from a broader sample that would produce more generalizable results. Second, the dataset was collected in a small rural setting that may vary from other agencies in larger more urban areas.

Through this study, the researchers were able to highlight the insecurities in relationship to passwords and computer data security, demonstrating that a password policy is necessary to provide a more secure system. Our recommendation would be for all healthcare agencies to institute a password policy that would provide the following guidelines: 1) how passwords should be constructed, 2) how user-level and system-level passwords are managed and changed and 3) how the agency will track employees' passwords.

Managers and administrators must enhance the security of their networks by setting strong password policies. Network administrators should require users to regularly change or update employee passwords, and those requirements should be incorporated into the organization's overall security policy. All employees should be taught good password practices and should be frequently reminded about how easily a security breach can occur. Additionally, employees need to be taught the resulting effect of weak password choices.

This study also shows the need to create a culture of security around sensitive data. It is easy to be lax about information with which one deals with on a daily basis, forgetting how damaging it could be in the wrong hands. It therefore appears that healthcare agencies may want to require that a password contain letters, numbers, and symbols; be a certain length; and not contain common words or personal identifiers. Additionally, this research reinforces the need for healthcare agencies to provide password education and training.

Conclusion

Unfortunately, most employees in this healthcare agency were not very security savvy when they created their passwords. It also appears that they do not completely understand the ramifications of a password breach (like possible access to patients' accounts by a hacker) and how their choice of a weak password could affect the security of their agency's system. It is apparent that healthcare agencies must institute password policies and training that will address the need for good passwords in order to protect patient and other sensitive healthcare information.

Joseph A. Cazier, PhD, is an assistant professor of computer information systems at Appalachian State University in Boone, NC.

B. Dawn Medlin, PhD, is an associate professor of computer information systems at Appalachian State University in Boone, NC.

Notes

1. "Login error trouble keeping track of all your sign-ons? Here's a place to keep your electronic keys, but you better remember the password." *San Jose Mercury News*. (2001). February 4, 2001
2. "Human Memory." Intelegen, Inc., Troy, MI, 2000. Retrieved November 12, 2005, from http://www.brain.web-us.com/memory/human_memory.htm.
3. Whitman, M. E. and H.J. Mattford. *Principles of Information Security*. Boston, MA. Thomson Course Technology, 2003.
4. Andrews, L.W. "Passwords Reveal Your Personality." *Psychology Today*. January/February 2002. Retrieved February 1, 2005, from http://www.psychologytoday.com/articles/pto-20020101-000006.html.
5. University of New Mexico. "Password Methodology: How to Make, Remember and Change Good Passwords." 2004. Retrieved October 10, 2004, from www.unm.edu/cirt/accts/psswrdmethodology.html.
6. Donovan, C. SANS Institute "Strong Passwords." SANS Institute, Bethesda, MD. June 2, 2000. Retrieved October 12, 2005, from http://www.giac.org/certified_professionals/practicals/gsec/0043.php.
7. Georgetown University Information Security. Retrieved September 2005 from http://security.georgetown.edu/documents/brochure_netid.pdf.
8. University of New Mexico. "Password Methodology: How to Make, Remember and Change Good Passwords."
9. Department of Defense. *Password Management Guideline*. Department of Defense Computer Security Center, 1985. Fort Meade, MD. Retrieved September 2004 from www.alw.nih.gov/Security/FIRST/papers/password/dodpwman.txt.
10. Medlin, B.D. and J.A. Cazier. "Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times." *Information Systems Security: The (ISC)^2 Journal*. Vienna, VA. Accepted for publication summer 2006.

References

1. MOREnet. "Internet Security Best Practices, Best Practices in General." University of Missouri, Columbia, MO. 2000. Retrieved April 2006 from www.more.net/security/best/index.html.

Table 1

Password Scores

PW Score	Number	Percent
-2	5	5.6%
-1	15	16.7%
0	20	22.2%
1	26	28.9%
2	10	11.1%
3	7	7.8%
4	4	4.4%
5	1	1.1%
6	1	1.1%
7	1	1.1%

Table 2

Positive and Negative Dichotomous Scoring Questions

Positive Questions	Yes (percentage)
1. Does the password have both upper- and lowercase letters?	35.6
2. Does the password have both upper- and lowercase throughout the password, not just the beginning?	7.8
3. Does the password have both letters and numbers?	24.4
4. Does the password have both letters and numbers throughout, not just at the beginning or end?	4.4
5. Does the password have any special characters?	14.4
6. Does the password have at least 6 characters?	85.6
7. Does the password have 8 or more characters?	32.2
8. Does the password appear to be random?	11.1
Negative Questions	Yes (percentage)
9. Is the password the same as the username, e-mail, or name?	4.4
10. Does the password resemble the username, e-mail, or name?	11.1
11. Does the password appear to be the name of a person (real or in a book)?	43.3
12. Does the password appear to be the name of a place (real or in a book)?	5.6
13. Does the password appear to be a word that could be found in an English dictionary?	58.9
14. Does the password appear to be a word in a foreign dictionary?	2.2
15. Does the password appear to have a discernible pattern to it? (i.e., 123321, 8888888 or aabbccbbaa)?	2.2
16. Does the password appear to be a date?	3.3