An Empirical Investigation: Health Care Employee Passwords and Their Crack Times in Relationship to HIPAA Security Standards

B. Dawn Medlin, Appalachian State University, USA
Joseph A. Cazier, Appalachian State University, USA

ABSTRACT

The purpose of this article is to examine the passwords selected by health care professionals and the security and privacy standards in relationship to those passwords as addressed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Examinations of these passwords have illustrated the connectivity between password length and strength and the need to educate employees as to the importance of their password choices. Through an empirical analysis, this article examines whether the passwords created by employees of a health care agency followed “strong” or “weak” password practices. The results should indicate to health care agencies the importance of comprehensive password policies and employee training.

Keywords: IS security; HIPAA; passwords; user behavior

INTRODUCTION

Every health care agency in the United States that handles protected patient health information is required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA security standards require health care agencies to adopt policies and procedures that will show how security methods will be implemented that are “reasonable and appropriate.”

Like most organizations, health care agencies who want to protect their information have employed processes, such as password authentication methods, that act as barriers between the “outside world” and most of their computer systems. If a hacker is able to determine a valid userid and password, then it is likely that they can impersonate the employee and have admittance into the agencies’ computerized system. Unfortunately, if valid credentials are presented, this intrusion often goes unnoticed.

In this article, we examined the passwords that were created by employees of a health care agency. There are numerous problems...
that can make password 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 computerized systems and could potentially compromise a patient’s information and privacy.

Through an empirical analysis of the passwords, the factors of length, strength, and crack times were observed. Examination of these passwords illustrates the need for good password practices, especially because they are included both directly and indirectly within the HIPAA security standards. The analysis is both interesting and important, as it analyzes employees’ actual self-selected passwords in an organization that has implemented no password rules or restrictions.

**Literature Review**

HIPAA consists of three sets of standards which include: 1) transactions and code sets, 2) privacy, and 3) security. The objectives of these standards are to simplify the management and administration of health insurance claims, lower costs, and give patients more control and access to their medical information while protecting their information from real or potential threats of disclosure or loss.

HIPAA also requires that health care organizations take reasonable and appropriate steps to limit the disclosure of an individual’s personal health information, including training employees to follow privacy procedures, designating an individual to oversee the organization’s privacy initiatives, and securing access to electronic patient records. The privacy deadline for HIPAA was April 2003, and the security deadline was April 2005.

There are distinct differences between privacy and security. Privacy is the patient’s control over the use and disclosure of their own personal health information (PHI), whereas security is defined as the “policies, practices, and technology that must be in place for an organization to transact business electronically via networks with a reasonable assurance of safety” (Volonino & Robinson, 2004, p. 1).

Personal health information, or PHI, is the HIPAA term for health information in any form (i.e., paper, electronic, or verbal) which personally identifies a patient. This includes individually identifiable health information in paper records that have never been electronically transmitted (http://www.medstarsystems.com/hipaa.html). Privacy may also include the right to determine when, how, and to what degree PHI is shared with others. The HIPAA privacy rules grant new rights to patients to gain access and control of the use and disclosure of their personal health information (United States Department of Health and Human Services, 2003).

HIPAA addresses security and privacy measures in relationship to passwords, either directly or indirectly, in the following standards (http://www.hhs.gov/news/facts/privacy.html). These standards, as listed below, include management processes, user education and training, and access control.

**Security Management Process** (161.308(a)(1)) Healthcare organizations must show that they have a consistent set of internal processes, with implementation that is widespread and institutionalized. Processes range from establishing criteria for who has access to what, and who can request certain resources; to ensuring that access rights are revoked immediately upon employee termination. Also required are security policies that should be established and implemented.

**Security Awareness and Training** (161.308(a)(5)) HIPAA requires that staff members be trained and educated concerning the proper handling of PHI. This basic-level security training should include measures such as password management.

**Access Control** (161.312(a)) HIPAA security regulations require a definition of who has access to PHI within the organization, as well as the rules determining an individual’s right of access, and the reasons for denying access to some individuals.
Passwords

Self-created computer passwords are generally personal, as they reflect the personalities of individuals who may attempt to summarize their life through a few keyboard entries. According to Grudin (1994), psychologists have found that people and personalities are often very predictable in the aggregate, as may be their choices of passwords.

To counter the problems associated with short and guessable passwords, systems were invented that changed passwords on a regular basis and that forced the enduser to create a new password different from any other password that had been previously created. Systems that were more sophisticated enforced rules requiring passwords to be structured using letters and digits in nonrepeating patterns. Requiring employees to create new and different passwords often results in some employees violating security policies and rules, such as never writing down their passwords. Employees who are required to remember multiple passwords have often found it necessary to write their passwords on a piece of paper and then tape it to their computer.

Psychologists have found that humans can store only five to nine random bits of information in their short-term memory, thus making it difficult to remember long and complicated passwords (Andrews, 2004). In order to deal with this memory shortcoming, employees will often choose passwords with personal meanings so that they can associate them with something in their long-term memory (http://brain.webus.com/memory/human_memory.htm).

For all humans, there are several problems with short-term memory. First, 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 (Kanaley, 2001). Second, it has been found that when humans attempt to recall a sequence of items, those items are not drawn from an arbitrary or unfamiliar range but must be familiar words or symbols. Third, the human memory increases with the use of redundancy (Atkinson & Shiffrin, 1968). Consequently, all of these aforementioned weaknesses add to the problem of creating strong passwords.

Strong Passwords

In order to create strong passwords, it may be helpful to define and describe what makes a strong password. An effective password does not consist of common, everyday words but incorporates different characters such as the incorporation of letters (both upper and lower case), numbers, and special symbols. This can be achieved by mixing or mingling characters from the five different character sets, which include:

- uppercase letters such as A, B, C;
- lowercase letters such as a, b, c;
- numbers such as 1, 2, 3;
- special characters such as $, ?, &; and
- alt characters such as μ, £, φ

Strong passwords can also be created by replacing letters with other characters so that they form memorable words but not necessarily dictionary words (Merkow & Breitnauer, 2006). For example, the word “password” may become “Pa55w0rd.” Unfortunately, this step is already outdated, as dictionaries or wordlists have already been created to combat this mixing of characters and numbers technique. In response to this problem, some individuals have chosen to use combinations of two or more unrelated words, each of which consist of characters from each of the five character sets.

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. (Donovan, 2000). Length simply means that a password that is longer is more difficult to crack.

There are also other behaviors that employees should practice to maximize the effectiveness of their passwords. Employees should avoid using the same password on multiple accounts, because doing so can create a single point of failure, and if a hacker or intruder gains...
access to one account, they will almost certainly have access to most or all of the employees’ other accounts. If an employee repeatedly uses the same password and that password is a weak password, then the time needed to crack that password can be as fast as a few seconds.

**Weak Passwords**

Most employees create passwords containing a family name, pet name, birthday, or anniversary because these are generally easier to remember rather than random sequences. These passwords are weak because they can be easily cracked through the use of software cracking programs 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 (Whitman & Mattord, 2003). Hackers can obtain information from the employee by pretending to innocently ask questions about hobbies, the date of birth of family members and pets, or the birth location of the employee. Social engineering therefore enables hackers to obtain enough information to make at least an educated guess of the employee’s password.

The definition of weak passwords also includes any words that may appear in a dictionary, that is, 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 name of a spouse or pet.

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 can obtain information by “googling” someone. Google’s search and information retrieval capabilities have made it the first stop for many hackers in their quest to 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, such as individuals’ phone numbers, addressees, and directions to their homes.

The easiest way for some employees to remedy the weak password problem is to use a program such as a random password generator that provides the enduser with a ready-made password. Random password generator programs can be downloaded from the Internet sites like http://www.wincatalog.com/pasgen.html. Other types of software programs are available on the Internet (http://www.angel.net/~nic/passwd.html) that will convert a current password into a generated password that is not recognizable. However, due to the random nature of these passwords, they are difficult to remember. Sometimes employees will record the password on a sticky note and place it on their monitor, allowing any and all passers-by to see their “secret” password. Again, the solution is to create a password that is memorable but difficult to decipher. But adherence to security experts’ suggestions about password authentication usually involves a tradeoff - passwords that are easy to create and remember are also easy for others to guess or for a hacker to crack.

**Cracking and Hacking**

It is important to distinguish between “cracking” and “hacking.” Essentially, “codes are cracked” and “machines are hacked.” If a password is cracked, it could allow the hacker to assume the legitimate employee’s identity, thereby allowing access to all data that the legitimate employee is authorized to view.

Five main techniques hackers can use to identify a password include stealing it, guessing it, brute force attack, dictionary attack, and the hybrid method. Each of these methods requires different skills. To steal means looking over one’s shoulder when typing it, or finding the piece of paper on which it was written. To guess means the hacker tries familiar passwords, usually consisting of the names of spouses or favorite sports team. A brute force attack is where every possible combination of letters, numbers, and symbols is used in an attempt to guess the password (Cliff, 2001). While an
extremely labor intensive task, with modern fast processors and software tools, this method should not be underestimated. The next method, a dictionary attack, uses combinations of words. In the first attempt, words available in a general dictionary are chosen. Dictionaries with hundreds of thousands of words, and specialist, technical, and foreign language dictionaries also are available, as are lists of thousands of words that are often used as passwords such as “qwerty,” “abcdef,” and so forth. The last method is a hybrid attack, which mixes the aforementioned two attack techniques by using dictionary type words as a base and then using brute force to check for permutations of that word. Essentially, it combines the best of both methods and is considered to be highly effective against passwords where little or no imagination was used.

Cracking Software
Essentially, any password that is stored on a computerized system can be cracked. Passwords are stored on the system in an encrypted form that has been run through an encryption algorithm, which converts it into a mathematical formula. It should be noted that there is no algorithm that will take a password in encrypted form and give it back in its original password form.

The software cracking program works by taking the strings of characters and encrypting them, and then comparing the encrypted text against the password that was stored in an encrypted form. If the two encrypted versions are the same, then the string of characters is the password. It would take a long time to try every combination of letters that an employee could have as their password, even on a reasonably fast machine. So cracking software tries the most likely combinations. First, the software attempts to find out everything it can about the employee on the system, like a login name, an employee’s full name, address, social security number, and so forth. All of these attempts may only take a few minutes.

The program then progresses to a large “dictionary” containing words from many languages, place names, people names, names of characters in books, jargon, slang, and acronyms. It makes an attempt to crack each password, and after the cracking program has completed that task, it tries variations on words, such as any word written backwards, any word with a punctuation character at the end, any word with a punctuation character at the beginning, any word capitalized, and any two words put together with a number between them. It tries every combination possible to try and guess or crack the password. Not all attempts are successful, but given enough time, most passwords can be cracked. In fact, most of these attempts can be completed between a few seconds to a few minutes.

Recommendations for Organizations and Network Administrators
As required by HIPAA, security and privacy administrators, and management must enhance the security of their networks by setting strong password policies. Password requirements, such as length and strength, should be built into every health care agency’s security policies. Network administrators should institute a requirement to regularly change or update employee passwords. Employees should also be frequently reminded about how easy it is for hackers to get passwords through social engineering. New employees should be taught good password practices. Providing intranet resources on network security and password security may also be helpful. Finally, the organization’s password policy should be integrated into the overall security policy, and all employees should be required to read the policy. Systems administrators should implement safeguards to ensure that people on their systems are using adequately strong passwords. They should set password expiration dates on all programs, keep a password history to prevent reuse, and lock out accounts after 3-5 password attempts. Additionally, the organization should keep the number of people in the organization who have access to these passwords as low as possible. Finally, when
installing new systems, they should ensure that default passwords are changed immediately. This article addresses the issues surrounding password length and strength in an effort to educate both health care organizations and their employees. Obviously, passwords are just one piece of the puzzle. Other pieces are increasing physical security, plugging network holes, and installing strong firewalls. These elements provide much more global protection in the networked environment than passwords alone, but if the only method of control employees have is a password, they must be aware of security risks and take the very best precautions available to them.

RESEARCH METHODOLOGY

Data Collection
Most of today’s health care agencies allow access to both data and the networked system by granting permission based upon password authentication and approval. The increased usage of passwords and logins has revealed several interesting issues associated with users’ difficulty in developing and remembering passwords (Jones, 2002).

The data set was collected from a health care agency in the spring of 2006, and consisted of 90 active employees. Employee passwords were given to the researchers after approval by the director of the health care agency. Names of the employees, as well as their passwords, were provided by the network administrator and without the knowledge or consent of the employee.

In addition, this particular agency did not enforce any particular password rules or suggest password guidelines, and employees were free to choose passwords of varying lengths and strengths. Because of a lack of rules or guidelines, passwords collected are of particular interest, as they show current health care workers’ password security practices when left to their own devices and without being required by a network or other administrator to create a “strong” password.

Rating Instrument
To assess the security level of the selected passwords by employees at a health care agency the researchers reviewed current best practices for password security (Department of Defense, 1985; Georgetown University, 2005; University of New Mexico, 2004). Next, the researchers aggregated the guidelines into an instrument that was used to rate the security level of each password.

To provide a greater degree of granularity for analysis and in order to recommend specific guidelines, 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 that had previously been developed and validated by Medlin and Cazier (2006). These questions are presented in Table 1. Building on prior research with a standardized methodology allows for a better opportunity to gauge practices over time and across disciplines.

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. 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. Because 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.

Analyzing the results of the questions on positive and negative password practices, 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 employees (64.4%) did not use both upper and lower case passwords. Of those that do
Table 1. Dichotomous password scoring sheet

<table>
<thead>
<tr>
<th>Positive Questions</th>
<th>Yes %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the password have both upper and lower case letters?</td>
<td>35.6 %</td>
</tr>
<tr>
<td>2. Does the password have both upper and lower case throughout the word, not just the beginning?</td>
<td>7.8 %</td>
</tr>
<tr>
<td>3. Does the password have both letters and numbers?</td>
<td>24.4 %</td>
</tr>
<tr>
<td>4. Does the password have both letters and numbers throughout, not just at the beginning or end?</td>
<td>4.4 %</td>
</tr>
<tr>
<td>5. Does the password have any special characters?</td>
<td>14.4 %</td>
</tr>
<tr>
<td>6. Does the password have at least 6 characters?</td>
<td>85.6 %</td>
</tr>
<tr>
<td>7. Does the password have 8 or more characters?</td>
<td>32.2 %</td>
</tr>
<tr>
<td>8. Does the password appear to be random?</td>
<td>11.1 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Negative Questions</th>
<th>Yes %</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Is the password the same as the username, e-mail or name?</td>
<td>4.4 %</td>
</tr>
<tr>
<td>10. Does the password resemble the username, e-mail or name?</td>
<td>11.1 %</td>
</tr>
<tr>
<td>11. Does the password appear to be the name of a person (real or in book)?</td>
<td>43.3 %</td>
</tr>
<tr>
<td>12. Does the password appear to be the name of a place (real or in book)?</td>
<td>5.6 %</td>
</tr>
<tr>
<td>13. Does the password appear to be a word that could be found in an English dictionary?</td>
<td>58.9 %</td>
</tr>
<tr>
<td>14. Does the password appear to be a word in a foreign dictionary?</td>
<td>2.2 %</td>
</tr>
<tr>
<td>15. Does the password appear to have a discernible pattern to it?</td>
<td>2.2 %</td>
</tr>
<tr>
<td>16. Does the password appear to be a date?</td>
<td>3.3 %</td>
</tr>
</tbody>
</table>

use upper and lower case passwords, the vast majority of those (78.2%) 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, because 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%) of the health care workers sampled actually used the method of capitalizing letters.

In addition to using a mix of upper and lower case letters, most experts recommend having a combination of letters and numbers. In our case, less than a fourth (24.4%) used both letters and numbers. Of those that used letters and numbers, the vast majority (82.0%) only used numbers at either the beginning or end of the word. While this is better than having only letters and numbers, it is not as strong as the 4.4% whose password had letters and numbers comiled. Passwords with letters and numbers only at the end or beginning are easy to crack with a hybrid 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 employees (85%) had passwords of at least

Copyright © 2007, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
six characters long; however, only 32.2% had passwords with eight or more characters.

In relationship to the negative questions, we see that the great majority of the employees, 58.9%, appear to be using common words that can be found in a Standard English language dictionary, thus making them very susceptible to dictionary attacks or password guessing. Of even greater concern, 43.3% 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 username the same (4.4%) or similar (11%) 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. Not many foreign words were found in this dataset, which may attest to the lack of diversity in rural health care workers.

In Table 2, almost a third of the passwords (31%) were cracked in less than one minute. These percentages specifically address password strength. From a security standpoint, the passwords that took the longest to crack had the highest scores, indicating greater security. Those passwords that were cracked in less than one minute were dictionary words, and the longer passwords were cracked using the brute force method. In the category of 1 to 5 minutes, the hybrid method that incorporates letters and numbers was used.

The type of method used to crack the passwords should be noted. In less than one minute, almost 30% of the passwords were cracked with the dictionary method, another 33% were cracked by brute force from 1 to 10 hours, and 20% required at least 10 hours to crack. The five passwords that were not cracked included special characters, symbols, and numbers and were comprised of six or more characters in length, thus adding to their level of security. The average length for the uncracked category was 10.4 letters long and had the highest password security score, with an average of 3.60.

**CONCLUSION**

The introduction of HIPAA has created the legal responsibility of health care agencies to focus on policies related to the security standards and the technical controls that must be developed, implemented, and later tested. Weak passwords created by employees provide easy access and could ultimately result in a potential violation of HIPAA.

Unfortunately, most employees in this health care agency did not appear to be very se-

---

**Table 2. Password crack time by category**

<table>
<thead>
<tr>
<th>Crack time by Category</th>
<th>N</th>
<th>Percent</th>
<th>Mean Length</th>
<th>Mean Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 Minute</td>
<td>28</td>
<td>31.1%</td>
<td>6.57</td>
<td>-0.04</td>
</tr>
<tr>
<td>1 to 5 minutes</td>
<td>2</td>
<td>2.2%</td>
<td>6.00</td>
<td>1.50</td>
</tr>
<tr>
<td>5 to 60 minutes</td>
<td>7</td>
<td>7.8%</td>
<td>5.14</td>
<td>-0.29</td>
</tr>
<tr>
<td>1 to 10 hours</td>
<td>30</td>
<td>33.3%</td>
<td>6.37</td>
<td>0.60</td>
</tr>
<tr>
<td>More than 10 hours</td>
<td>18</td>
<td>20.0%</td>
<td>8.00</td>
<td>2.22</td>
</tr>
<tr>
<td>Not Cracked</td>
<td>5</td>
<td>5.6%</td>
<td>10.40</td>
<td>3.60</td>
</tr>
<tr>
<td>Overall</td>
<td>90</td>
<td>100%</td>
<td>7.08</td>
<td>1.27</td>
</tr>
</tbody>
</table>

Copyright © 2007, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
curity savvy when they created their passwords. It also appears that they do not completely understand the ramifications of a password breach (e.g., possible access to patients’ accounts by a hacker) and how their choice of a weak password could affect the entire security of their agency’s system.

We believe that this investigation makes a unique contribution to the literature because the passwords studied are currently in use in a health care agency setting. As noted previously, there were no enforced rules relating to password creation, nor does the site require or suggest password guidelines. It therefore appears that health care organizations may want to require that a password contain letters, numbers, symbols, a certain length, and uncommon words or personal identifiers. Additionally, this research reinforces the need for health care agencies to provide password education and training as required by the HIPAA security standards.

REFERENCES


Kanaley, R. (2001, February 4). Login error trouble keeping track of all your sign-ons? Here’s a place to keep your electronic keys, but better remember the password. San Jose Mercury News, 3G.


B. Dawn Medlin is currently serving as an associate professor in the department of computer information systems in the John A. Walker College of Business at Appalachian State University in Boone North Carolina. She earned her doctorate at Virginia Polytechnic Institute and State University. Her teaching and research activities have been in the area of information technology, specifically in security, outsourcing, and e-commerce. Dr. Medlin's research articles have appeared in journals such as the Information Systems Security: the (ISC)2 Journal and the Journal of Information Privacy and Security, Int. J. Information Technology Management, Journal of Computer Information Systems, Int. Journal of Management, among other refereed journals.

Joseph A. Cazier is an assistant professor in the department of computer information systems in the John A. Walker College of Business at Appalachian State University. He received his PhD from Arizona State University in Boone North Carolina. He actively does research in information security, trust and ethics. Dr. Cazier has also published in Information & Management, the Journal of Information System Security, Information Systems Security: the (ISC)2 Journal and the Journal of Information Privacy and Security, among others. He has also published a book relating to business ethics and privacy, Value Congruence and Trust Online: Their Impact on Privacy and Price Premiums.