Category: Concepts, Trends, and Challenges

Password Security Issues on an E-Commerce Site

B. Dawn Medlin
Appalachian State University, USA

Joseph A. Cazier
Appalachian State University, USA

Dinesh S. Dave
Appalachian State University, USA

INTRODUCTION

With the exponential growth of the Internet and e-commerce, the need for secure transactions has become a necessity for both consumer and business. Even though there have been advances in security technology, one aspect remains constant: passwords still play a central role in system security. The difficulty with passwords is that all too often they are the easiest security mechanism to defeat.

Kevin Mitnick, notably the most recognized computer hacker, made the following statement concerning humans and their passwords:

> *...the human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures addresses the weakest link in the security chain.* (Poulsen, 2000)

Without secure passwords, e-commerce sites invite online criminals to attempt fraudulent schemes that mimic the goods and services that legitimate e-commerce merchants offer. With increasing numbers of users on an increasing array of e-commerce sites, often requiring the use of passwords, users often choose to reuse the same simplistic password, and do so on multiple sites (Campbell, Calvert, & Boswell, 2003).

For most computerized systems, passwords are the first line of defense against hackers or intruders (Horowitz, 2001). There have been numerous published articles that have created guidelines on how to create better or safer passwords with the following recommendations:

1. passwords should be memorized and not written down;
2. passwords should be an eight- or nine-character word or phrase, and end users should randomly add
3. passwords should contain a mixture of letters (both upper- and lowercase), numbers, and punctuation characters; and
4. passwords should never be words that can be commonly found in a dictionary.

But if an individual adheres to security experts' suggestions about password authentication, it usually involves a trade-off. If a password is easy to create and remember, it is most likely that it is easy for others to guess or a hacker to crack.

Eventually, any password can be cracked. Password crackers use a variety of methods and tools that can include guessing, dictionary lists, or brute force attacks. Dictionary lists are created by using an automated program that includes a text file of words that are common in a dictionary. The program repeatedly attempts to log on to the target system, using a different word from the text file on each attempt. A brute force attack is a variation of the dictionary attacks, but it is designed to determine passwords that may not be included in the text file. In a brute force attack, the attacker uses an automated program that generates hashes or encrypted values for all possible passwords and compares them to the values in the password file (Conklin, White, Cothren, Williams, & Davis, 2004).

Unfortunately, many of the deficiencies of password authentication systems arise from the limitations of human cognitive ability (Pond, Podd, Bunnell, & Henderson, 2000). The requirements to remember long and complicated passwords are contrary to a well-known property of human memory. First, the capacity of human memory in its capacity 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, 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. Third, the human memory thrives on redundancy. In fact, studies have shown that individuals' short-term memory will retain a password for approximately 30 seconds, thereby requiring individuals to attempt to memorize their passwords immediately (Atkinson & Shiffrin, 1968).

BACKGROUND

Password security research has dramatically increased over the past 20 years (Ives & Walsh, 2004). Even though there has been an increased awareness surrounding the topic of password protection, password vulnerabilities remain significant. Most of today's e-commerce sites allow access to both data and the networked system by granting permissions based on password approval. The increased usage of passwords and logins has revealed several interesting issues associated with users' difficulty in developing and remembering passwords (Jones, 2002).

In order to combat the issue of having to remember so many different passwords, some users have resorted to selecting familiar terms such as a pet or family name, their own name, their phone number, or other common terms that could be found in a dictionary. British psychologist Helen Petrie, PhD, a professor of human/computer interaction at City University in London, analyzed the passwords of 1,200 British office workers who participated in a survey funded by CentralNic, an Internet domain-name company in 2001. She found that most individuals' choices of passwords fell into one of four distinct password "genres" or categories (see Table 1).

The first group, which she labeled as "family," comprised nearly half of the respondents. These individuals selected their own name or nickname; the name of a child, partner, or pet; birth date; or a significant number such as a phone or social security number. Further, Petrie found that these individuals chose passwords that symbolized people or events with emotional value or ties.

One-third of the respondents were "fans," using the names of athletes, singers, movie stars, fictional characters, or sports teams. Petrie also found that these individuals were generally young and wanted to align themselves with the lifestyle represented by or surrounded around a celebrity status such as Madonna and Homer Simpson.

Eleven percent of responses were "fantasists." Petrie found that their passwords comprised sexual terms or topics. Some of the examples included in this category were terms such as "sexy," "stud," and "goddess." The final 10% of participants were identified as "cryptics." These users were seemingly the most security-conscious, but it should also be noted that they were also the smallest of all of the four categories. These individuals selected unintelligible passwords that included a random string of letters, numbers, and symbols.

IMPACT

To assess the security level of the passwords selected by consumers at the online bookstore, the researchers reviewed current best practices for online password security (Ohio State, 2004; University of New Mexico, 2004; Department of Defense, 1985; Security Stats, 2004) and aggregated the guidelines into an instrument that was used to rate the security level of each password. The data set contained 520 customer profiles collected from an e-business site from the summer of 2003 until the summer of 2004, with the majority of the respondents being from the western United States. Also, it should be noted that the e-commerce site did not require a signed consent from the user, as the information was obtained via the owner of the site, nor was a password recommended or created by the system.

Using the five-point human rating system gathered from a review of the literature, a panel of three individuals familiar with the current literature related to password security developed the categories presented in Appendix A. To provide a greater degree of granularity for analysis, a series of dichotomous yes or no questions was developed that was both positive and negative. From these questions, a standardized scoring system was developed (see Appendix B). The scoring system included eight

Table 1. Petrie's category definition

Category #	*Name*	*Definition*
1	Family	Name or nickname; name of a child, partner, or pet; birthday
2	Fan	Names of athletes, singers, movie stars, fictional characters, or sports teams
3	Fantasists	Interest in sex is evident in passwords such as "sexy," "stud," and "goddess"
4	Cryptic	Unintelligible passwords or a random string of letters, numbers, and symbols, such as Jxa+157