Assessing password threats: Implications for formulating university password policies

Melissa Walters
The University of Tampa

Erika Matulich
The University of Tampa

ABSTRACT

Weak passwords are often cited as one of the most serious threat to university system security; however, password vulnerabilities go beyond weak password construction. This paper explores password vulnerabilities and threats in a university context, including best practices for password syntax, security, and policy.

Keywords: passwords, university policy, system security, threat assessment

Introduction

Weak passwords are often cited as one of the most serious threat to system security; however, password vulnerabilities go beyond weak password construction (Culp, 2000, 2003). Consider the following three scenarios. First, a visitor to a university enters an employee's unlocked office, sits down at the employee's computer, and then signs on to the university network using the password written on a yellow sticky note posted on the computer monitor. Second, a former student writes a program to repeatedly attempt unauthorized logons using known usernames (consisting of university email addresses) and incorrect passwords, ultimately forcing the system to reset user passwords to "1234." Third, a faculty member receives a fraudulent email apparently from the university information technology department asking users to click a provided link and then enter their logon data to update their account; because the email appears to come from a legitimate source, the faculty member dutifully follows the instructions in the email inadvertently revealing their password to an unauthorized party. The "phisher" of passwords then uses the university accounts to send so much spam that the university is blocked by many internet service providers, and university members cannot send out legitimate emails. These are not uncommon password breaches, and furthermore, the breaches have nothing to do with password syntax.

Passwords and Logical Access Control

Logical access control generally involves a logon procedure whereby a user both claims (user identification) and validates (user authentication) their identity to the system. Passwords are a common form of authentication whereby users validate their identity based on something they know (a password) as opposed to something they have (tokens or swipe cards) or something they are (biometrics such as fingerprints or retinal scans) (Tipton & Henry, 2007). A password is usually a string of alpha, numeric, and/or special characters used to individually authenticate identity and establish accountability for a specific user within a system. Because usernames are frequently common knowledge (e.g., the first part of a user's email address), passwords are typically the first line of defense against unauthorized access to information systems resources. Moreover, as many systems do not require multiple forms of authentication, passwords may also be the last line of defense, making user passwords extremely valuable to someone (a "cracker") seeking unauthorized access to a system. University IT practices must evaluate password authentication as part of logical access control to ensure the confidentiality, integrity, and availability of university information system resources. But as the scenarios above illustrate, assessing the effectiveness of password practices means going beyond considerations of basic password syntax.

Password Vulnerabilities and Threats

A cracker needs only a single valid password to infiltrate a university system, and once in, is in an ideal position to mount additional attacks (Culp, 2000, 2003). As a consequence, passwords are routinely subjected to a number of different attacks (Tipton & Henry, 2007; Gregory 2009). University IT policymakers should be aware of common password weaknesses and attacks so they can assess the effectiveness of password practices relative to their ability to mitigate the risk associated with such vulnerabilities and threats.

Low Hanging Fruit: Weak Passwords

Passwords are considered "low-hanging fruit" because most users choose weak passwords from a security standpoint (Culp, 2000). Left to their own devices, users will invariably choose something easy to remember (and as such, easy to guess or crack) and use it for everything. Moreover, users dislike changing their passwords and if forced to do so, will use simplistic recycled variations of the same password (such as "password01," "password02," "password03"). If required to use a more complicated password or change their password regularly, many users will write their password down and post it in a conspicuous or easy to find location, sometimes referred to as the "dreaded yellow sticky note vulnerability" (Culp, 2000). Top desk drawers, pullout writing tables, the undersides of keyboards, and the fronts, sides, or backs of computer monitors are usual favorites. In addition, poor password management such as unenforced change requirements, failure to deactivate inactive accounts, or weak password resets can also make systems more vulnerable to logical access breaches (Allen, 2009; Gregory, 2009).

Know Thy Enemy

Awareness of common tactics used to illicitly acquire or "crack" passwords is central to evaluating the effectiveness of university password practices. There are numerous methods used to crack passwords including scavenging trash, password guessing, social engineering, and software-based attacks. Password cracking might simply involve exploiting the yellow sticky note vulnerability (a savvy cracker will know where to look), watching someone input their password (referred to as "shoulder surfing"), or ferreting through the trash in an attempt to extract written-down passwords or other information that might provide hints to user passwords ("dumpster diving"). Another common low-tech method might involve intuitive guessing based on commonly used passwords (e.g., "password" or "admin"), default passwords (e.g., "Guest," "1234," or blank passwords), consecutive numbers/letters or common keyboard sequences (e.g., "1111," 1234," or "qwerty"), and logical deduction based on knowledge about a user (e.g., children's names, pet's names, birthdates, addresses, etc.). Garry McKinnon, accused of illegally accessing numerous U.S. military computers, claimed he gained access to these high-profile systems by writing a simple program to search for blank default passwords (Kelly, 2006).

Users may also be duped into revealing their password to an illicit party masquerading as an authorized or otherwise trustworthy party (referred to as "social engineering"). Infamous hacker Kevin Mitnick, arrested by the FBI in 1995 for various computer hacking offenses, claims he gained unauthorized access to numerous systems exclusively through the use of passwords acquired via social engineering (Mitnick, 2002). Phishing, an electronic form of social engineering, involves the use of falsified emails designed to dupe individuals into sharing passwords or other sensitive information (Dhillion, 2007; Fraudwatch International, 2009). Phishing emails use forged source addresses, copied images, reproduced font styles, and disguised hyperlinks to imitate notices from authorized parties and will often direct individuals to a falsified web page to change their password or otherwise "update/verify account information" (Fraudwatch International, 2009). Although users may be aware of phishing scams with bank accounts or online auctions, for some reason these same users fall prey to emails that appear to be from their university IT department requesting password information.

In addition to low-tech password guessing and social engineering, there are a number of readily available software tools that may be used to illicitly acquire passwords. A "password cracker" is a software application used to recover unknown passwords (NetLingo, 2009; Tipton & Henry 2007). These applications may be used legitimately by security administrators to recover or test the integrity of system passwords or illegitimately by crackers to identify unknown passwords (Gregory, 2009; Tipton & Henry, 2007). Password cracking programs generally employ an amalgam of strategies to identify valid passwords, the most common being dictionary attacks and brute force attacks. Dictionary attacks involve systematically trying ordinary words or common slang found in dictionaries whereas brute force attacks iteratively generate possible combinations of characters based on known rules for acceptable passwords. Password crackers may also look for common number and special character substitutions often employed by users in an attempt to satisfy complex password requirements (e.g., "password" might become "password01," "Pa55w0rd," or "pa$$w0rd").

Spyware is another prevalent software-based method for illicitly acquiring passwords. Spyware is a form of malicious software designed to monitor computer activity and then transmit information to a third party without user knowledge. A keylogger is a form of spyware that records keystrokes (such as usernames and passwords), saves them in a log file and then transmits the log file to a third party (Online Cyber Safety 2009). In addition, passwords transmitted in cleartext (unencrypted form) are susceptible to electronic eavesdropping and may be captured by sniffer software. A sniffer is a program that monitors and analyzes network traffic by intercepting and reading network packets (Tipton & Henry, 2007; Mitchell, 2009; NetLingo, 2009). Used illegitimately, sniffers are capable of capturing sensitive information as it passes into, out of, or through a network. Sniffer programs are often used to collect passwords or view sensitive information transmitted in unencrypted form. Wireless networks are particularly vulnerable to sniffers (Online Cyber Safety, 2009).

Best Practices

Best password practices have evolved in response to common password threats and generally consist of what are believed (by industry consensus) to be the most effective and efficient strategies for ensuring adequate access control. As such, best practices have become a standard against which due diligence is measured (Allen, 2009; Dhillon, 2006). University IT policymakers should be familiar with best password practices so they can assess password authentication relative to what would generally be considered due diligence in ensuring an adequate level of protection for information resources of the university.

Best password practices include considerations of password syntax for the construction of strong passwords in addition to a well-communicated university password policy to facilitate user awareness (Hitachi, 2009; ISACA, 2009; Microsoft, 2009). Moreover, security practices to ensure the confidentiality and integrity of passwords are necessary to maintain the effectiveness of such password practices and policies (ISACA, 2009). Best password practices have been widely integrated into business system security, but universities need to adapt these practices to fit the needs of the university environment (McDowell, Rafail, & Hernan, 2004). Password syntax considerations, university password policy recommendations, and elements of password security in a university environment are described in further detail below.

Password Syntax

Weak passwords are labeled as such because the manner in which they are constructed makes them highly susceptible to common password threats such as password cracking software. Passwords based on insufficient length, single character-types, ordinary words, common number or keyboard sequences, or user specific information are easily compromised by such tactics. Strong passwords will possess characteristics designed to thwart common password attacks (Allen, 2009; Culp, 2003; Microsoft, 2009).

- Sufficient Length. Passwords should be at least 6 to 8 (preferably 8) characters. As a general rule, the longer the password, the more difficult it is to crack (Microsoft, 2009).
- Different Character Types. Passwords should use a combination of (at least three) alpha, numeric, upper and lower case, and if allowed, special characters (Allen, 2009). As general rule, the more possible combinations of characters, the more difficult and time consuming a brute force attack will become. An eight-character password using only upper case letters would require 8^{26} (302,231,454,903,657,293,676,544) combinations. With the addition of upper and lower case, the number of possible combinations jumps to $8^{52,}$ and with the addition of numeric characters, 8^{62} (Campbell, Calvert, & Boswell, 2003).
- Cryptic Construction. Passwords should not be based on ordinary words, common number or letter combinations/sequences, or user-specific identifiers (e.g., names) (Culp, 2003). The strongest passwords are cryptic; however, cryptic passwords are difficult to remember so users are more likely to write them down and keep them in an insecure location. A good password is one that is meaningful to the user (easy to remember) but nonsensical to others (difficult to guess). A passphrase can be used to construct a memorable but cryptic password by first creating an easy to remember phrase such as "most users have a difficult time remembering passwords" and using the first letter of each word ("muhadtrp"); the password can be further strengthened by using upper/lower case and substituting numbers/special characters for some of the letters (e.g. "mU4ad+rp") (Microsoft, 2009).

Password Policy

Password policy provides the foundation for developing, establishing, and implementing effective and efficient password practices. We recommend that University IT departments ensure that appropriate password polices have been developed, implemented, and communicated to users.

- Awareness. Password policies should be formalized and well communicated to users so they are aware of acceptable password practices (Gregory, 2009). University users should be made aware of common threats (e.g., phishing) so they are in a better position to thwart such attacks. Users should also be made aware of the impacts of logical access breaches so they understand the reasons for password policies and required practices.
- Individual Authentication. All user accounts should require logins and passwords that should provide individual authentication for accountability (Gregory, 2009; ISACA, 2009). Policy should clearly state that it would be considered a breach of policy to log in with someone else's password and stipulate responses to violations of policy. University administrators should also be willing to enforce those policies on faculty, staff, and students alike.

- Minimum Requirements. Minimum password requirements (syntax) should be established based on best practices and formalized as policy (Culp, 2000). Users should be required to use complex, cryptic passwords; blank or simplistic passwords should not be allowed (McDowell, Rafail, & Hernan, 2004).
- Change Management. Users should be required to change default passwords immediately and then change their selected passwords regularly (Hitachi, 2009). Change schedules should reflect the sensitivity of information access; once every 90 to 180 days is fairly common practice although once every 30 days is warranted for sensitive information access (ISACA, 2009). Change policy should also address reuse of previous passwords and histories of previously used passwords should be maintained by the system (ISACA, 2009). Reuse policy should also reflect the sensitivity of information access; disallowing reuse of the last three passwords is fairly common practice, although more sensitive data access may warrant disallowing reuse for an extended period of time or alternatively, prohibiting reuse of previously used passwords entirely (ISACA, 2009). Change policy should also establish a minimum period of time before a user can change their password again and a maximum number of times a user can change their password within a given period of time (to keep users from repeatedly changing passwords to circumvent password histories) (Hitachi, 2009). Care should be taken that password change does not happen during critical parts of a university calendar (e.g. during final exams) and the schedule of password changes coincides with semesters or quarters and keeps in mind university holidays (McDowell, Rafail, & Hernan, 2004). For example, our university sent out an email to students after final exams requiring them to change their passwords, but the students had already left the university for their winter break. Because the students did not change their passwords during the break within the designated time period, when they returned, their accounts had been disabled. The University IT help desk was overwhelmed at the beginning of the semesters, professors could not communicate with students, and faculty and staff were unable to perform work tasks. These issues could have been averted by changing the timing of the password change requirement to better match the calendar of the university.

Password Security

Password syntax is important, but even the strongest, most cryptic password is worthless if it is compromised (Mitnick, 2003). As such, we recommend that university IT departments also consider strategies designed to protect the security of user passwords.

- Confidentiality. Password verification files should not be stored in cleartext form; password files should be encrypted using a one-way cryptographic hash function (with passwords entered for authentication subjected to the same function for comparison) (Hitachi 2009, Tipton & Henry, 2007). In addition, passwords should be masked when input for authentication to avert electronic eavesdropping and should never be transmitted in cleartext form (e.g. via email, instant messaging). Moreover, passwords should not be written and kept in an insecure location (e.g., posted to a user's monitor). For users who must manage multiple passwords, readily available password management utilities provide a convenient and secure alternative to yellow sticky notes (Hitachi, 2009; Top Ten Reviews 2009). For highly secure data, universities should also consider biometric authentication such as a

fingerprint scanner, which are readily available on many laptop systems (Technovelgy, 2009).

- Login Failures. Account lockouts should be implemented for repeated login failures and users should be required to contact a security administrator to resolve a lockout (Culp, 2000). Account lockouts are generally preferable to automatic resets as reset functions can be exploited to force a system to reset passwords to common defaults that are easily guessed or cracked (Hitachi, 2009). This solution assumes that a university security administrator is available at all times, not just business hours.
- Forgotten Passwords. Users who have forgotten their password should be required to contact a security administrator to have the password reset (Gregory, 2009; ISACA, 2009). Reset passwords generally do not satisfy minimum password requirements, so once reset, users should be required to change the reset password within a stipulated time period. It is fairly common practice to allow users who have forgotten their password to have their password automatically emailed to them; this practice is not secure as passwords are generally emailed to users in cleartext form making them vulnerable to compromise (Hitachi, 2009, Tipton & Henry, 2007). Again, this solution would require a university security administrator to be always on call. If this is not possible, then automatic password resets should be set up to revert to a temporary password that is specific to the user but not commonly known (e.g., the last four digits of the employee number) (ISACA, 2009).
- Malware. The security administrator should require anti-virus and anti-spyware software along with regular scans of all systems to mitigate the risk of malware that might be used to steal passwords (ISACA, 2009). Such software should be easily accessible to users and if feasible, should be provided to university users free of charge (University of Tampa, 2009). Universities should also implement software that scans all computers attached to the network to verify use of appropriate anti-virus and anti-spyware software (University of Tampa, 2009).
- Spam. Universities should also make use of anti-spam filters as malware and phishing frauds are typically disseminated via spam (FraudWatch International, 2009). Spam filters will significantly reduce the number of illicit emails that users are exposed to and as such, will mitigate the risk that users will inadvertently compromise the confidentially of passwords (Tipton & Henry, 2007).
- Penetration Testing. Penetration testing provides an effective way to test the adequacy of password practices against common password threats by simulating attacks using the same tactics a cracker might use (Gregory, 2009; ISACA, 2009). When utilized to evaluate password authentication, penetration tests might involve common cracker tactics such as attempts to guess user passwords, walkthroughs to check for passwords posted in common places, discretely looking through trash to check for written down passwords, attempts to persuade users to reveal their passwords, and/or use of one of a number of available password auditing and recovery programs (e.g., L0phtCrack) (Boismenu, 2003; Culp, 2000).
- Multifactor Authentication. In addition to strengthening and testing password practices, university security administrators should also consider implementing stronger forms of authentication (Culp, 2000). Multifactor authentication involves combining different forms of authentication (passwords, tokens, and/or biometrics); a common form of multifactor authentication utilizes one-time session passwords generated by a smart device in addition to traditional static passwords (Tipton & Henry, 2007).

Conclusion

Evaluating the adequacy of password authentication requires university IT security administrators and policymakers to go beyond considerations of password syntax. It is important for universities and their user community to be familiar with common password threats and best password practices so they may assess the effectiveness of password strategies in terms of their ability to mitigate risks and satisfy expectations of due diligence with respect to logical access control.

References

Allen, C. (2009). Password Best Practices. http://www.lifewithalacrity.com/2009/09/password-best-practices.html

Boismenu, P. (2003). Password Cracking with L0phtCrack. SANS Institute Infosec Reading Room.

Campbell, P. Calvert, B., and Boswell, S. (2003). *Network Security Fundamentals*. Boston, MA: Thompson Course Technology, p. 73.

Culp, S. (2003). *The Ten Immutable Laws of Security*. Microsoft Corporation. http://technet.microsoft.com/en-us/library/cc722487.aspx.

Culp, S. (2000). *The Ten Immutable Laws of Security Administration*, Microsoft Corporation. http://technet.microsoft.com/en-us/library/cc722488.aspx.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, NJ: John Wiley & Sons.

FraudWatch International (2009). *Phishing email methods*. FraudWatch International Pty Ltd., http://www.fraudwatchinternational.com/ .

Gregory, P.H. (2009), *CISA Certified Information Systems Auditor All-In-One Exam Guide*, McGraw Hill.

Hitachi ID Systems Inc. (2009). Password Management Best Practices. http://www.psynch.com/docs/password-management-best-practices.pdf

Information Systems Audit and Control Association (ISACA) (2009). *Certified Information Systems Auditor (CISA) Review Manual 2009*. ISACA: Rolling Meadows, IL.

Kelly, S. (2006). Hacker fears UFO cover-up. BBC News Click Online, http://news.bbc.co.uk/2/hi/programmes/click_online/4977134.stm.

McDowell, M, Rafail, J, and Hernan J. (2004). Choosing and Protecting Passwords. Carnegie Mellon University. http://cns.esf.edu/Sec_Rec/PW_rec1.htm

Microsoft (2009). Create Strong Passwords. Microsoft Online Safety. http://www.microsoft.com/protect/fraud/passwords/create.aspx

Mitchell, B. (2009). A-Z Networking Terms. http://compnetworking.about.com/od/networksecurityprivacy/g/bldef_sniffer.htm

Mitnick, K. D. (2002). *The Art of Deception: Controlling the Human Element of Society*. Wiley Publishing.

Netlingo (2009). Netlingo The Internet Dictionary. Netlingo, http://www.netlingo.com/index.php.

Online Cyber Safety (2009). http://www.bsacybersafety.com/threat/keylogger.cfm

Technovelgy (2009). Biometric authentication: what method works best? http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16

Tipton, H. F. and Henry, K. (2007). *Official (ISC)^2 Guide to the CISSP CBK*. Boca Raton, FL: Auerbach.

Top Ten Reviews (2009). *Password Management Software Review*. Top Ten Reviews, Inc., http://password-management-software-review.toptenreviews.com/.

University of Tampa (2009). How to Protect Your Computer. http://www.ut.edu/detail.aspx?id=6688