Shawn Cressler
ITS 695 Internship
Saint Joseph's University Summer 2013

The Importance of Secure Passwords

Passwords are your first line of defense on the Web ("Cyber security awareness," 2010.) Passwords protect larger and larger portions of our everyday lives examples include bank accounts, credit card accounts, social media sites, email, and retail websites. On a professional level strong passwords protect grades, email communications, student data, and are required to maintain required levels of confidentiality. A weak password is exploitable by hackers and con artists who would like nothing more than to have access to your private personal data.

From Microsoft.com (2013) some of the most common passwords attacks include:

- Guessing - The attacker attempts to log on using the user's account by repeatedly guessing likely words and phrases such as their children's names, their city of birth, and local sports teams. *This is why you should never use any personal information as a part of your password including family birthdates, social security numbers, home address, and maiden name. Basically, anything about you that is a matter of public record or easily researched.*
- Online Dictionary Attack - The attacker uses an automated program that includes a text file of words. The program repeatedly attempts to log on to the target system using a different word from the text file on each try. *Creating passwords that use common words in all upper or lower case letters without symbols or numbers are very vulnerable to this form of attack.*
- Offline Dictionary Attack - Similar to the online dictionary attack, the attacker gets a copy of the file where the hashed or encrypted copy of user accounts and passwords are stored and uses an automated program to determine what the password is for each account. This type of attack can be completed very quickly once the attacker has managed to get a copy of the password file. *This kind of attack indicates that your system is already compromised and the attacker must have high level access to copy files off your computer. Most passwords can be broken in this manner given enough time however weaker passwords are broken more quickly.*
- Offline Brute Force Attack - This is a variation of the dictionary attacks, but it is designed to determine passwords that may not be included in the text file used in those attacks. Although a brute force attack can be attempted online, due to network bandwidth and latency they are usually undertaken offline using a copy of the target system's password 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. *Much like a dictionary attack this kind of attack will eventually crack almost any password; however, stronger passwords will always take longer to break.*

The University of Texas at Austin (2010) also includes the following as common password attacks.

- Phishing - This is a common scam technique where a hacker will send out an urgent IM or e-mail message designed to alarm or excite users into responding. These messages will appear to be from a friend, bank or other legitimate source directing users to phony Web sites designed to trick them into providing personal information, such as their user names and passwords. *If you suspect a phishing attack the best course of action is to contact the company, organization, or person the message supposedly came from before responding to it.*
- Shoulder Surfing - Be careful when logging on to a computer in public, such as a computer lab, cybercafé or library. There may be hackers lurking around for the express purpose of watching people enter their user names and passwords. It's a good idea to have a password you can enter quickly without looking at the keyboard. *In addition to "Shoulder Surfing" many people make the mistake of sharing their passwords and login information. For the same reason teachers discourage students from sharing locker combinations it is important not to share your security information; you can never be sure others will be as careful with your passwords as you will be.*

Creating strong passwords isn't difficult if you follow a few basic rules. First, a password should be at least eight characters long, although using ten characters as a rule of thumb is better. Next use a combination of uppercase letters, lowercase letters, symbols and numbers (approximately 69 characters to pick from.) For example, if you use just uppercase or lowercase letters in an eight character password it will only take up to two hours to crack using modern computing technology. However, if you add numbers, symbols, and different cases to the mix the time possibly required to crack the same length password bloats to eight months! This is why most systems require the inclusion of at least one upper case, one lower case, a symbol and a number in a new password. If you increase your password size to ten characters a one case password can require a little over two months to compromise (Shaffer, 2012.)

Second, when creating passwords you should never use the same password for more than one account, service, or social networking site. If an attacker or hacker manages to crack one of your passwords they will inevitably try that password on your other accounts and services. A single password used for multiple logins can endanger your online security and put your personal information at risk.

Finally, it helps if you think of passwords in the same way people think of cat litter as in it needs to be changed regularly for obvious reasons. Luckily, unlike cat litter passwords do not have to be changed every week. Unfortunately the longer you use a password the less secure it becomes. So, to paraphrase Al Capone, "Change your passwords early and often." Changing your password every four to eight weeks will keep you relatively secure.

Things to remember when it comes to passwords are:

- Eight characters at least, more is better.
- A combination of cases, symbols, and numbers makes a stronger password
- Don't share your passwords, for any reason.
- One account, one password, never reuse passwords.
- Change your passwords regularly.

References:

Cyber security awareness - lock up - the importance of strong passwords. (2010, October 05). Retrieved from http://www.utexas.edu/its/secure/articles/importance_strong_passwords.php

The importance of using strong passwords. (2013). Retrieved from http://msdn.microsoft.com/en-us/library/ms851492(v=winembedded.11).aspx

Shaffer, G. (2012). Good and bad passwords how-to password cracking goals, techniques, relative merits, and times. Retrieved from http://geodsoft.com/howto/password/cracking_passwords.htm