Password Managers

December 2013

Why do we need strong passwords?

- It isn't an individual, or even a room full of individuals who are trying to guess your password.
- Rather, computers are being used to do the task.
- Computers do not sleep, eat, demand worker's rights, etc.
- The top video cards used to meet the demands of today's video games can process information at the rate of about 4.5 teraflops (trillion floating-point operations per second).
    - To put that in perspective, in the year 2000 the world's fastest supercomputer, a cluster of linked machines costing $110 million, operated at slightly more than seven teraflops. [http://www.gtri.gatech.edu/casestudy/Teraflop-Troubles-Power-Graphics-Processing-Units-GPUs-Password-Security-System]

What makes a password strong?

- Password length
    - Eight characters used to be good enough, but in recent years the minimum suggested password length has changed to twelve characters.
    - The Georgia Tech study cited earlier classifies seven character passwords as "hopelessly inadequate", while estimating (in 2010) that it would take 17,000 to crack a good, twelve-character password.
- Complexity
    - In 2010, Imperva posted a study named "Consumer Password Worst Practices". Here are the top 20 most popular passwords:

        1. 123456
        2. 12345
        3. 123456789
        4. Password
        5. iloveyou
        6. princess
        7. rockyou
        8. 1234567
        9. 12345678
        10. abc123
        11. Nicole
        12. Daniel
        13. babygirl
        14. monkey
        15. Jessica
        16. Lovely
        17. michael
        18. Ashley
        19. 654321
        20. Qwerty

        [http://www.imperva.com/docs/wp_consumer_password_worst_practices.pdf]

    - According to the Imperva study, NASA recommends the following rules regarding password complexity:
        - A password should contain a mix of four different types of characters: uppercase letters, lowercase letters, digits, and special characters (~, @, #, $, %, ^, etc.)
        - If there is only one letter or special character, it should be neither the first nor last character of the password.
        - The password should not be a name, a slang word, or any word in the dictionary. It should not contain your name or email address.
        - Here is an interesting, recent article named *Crack This: How to Pick Strong Passwords and Keep Them That Way:* http://www.digitaltrends.com/mobile/crack-this-how-to-pick-strong-passwords-and-keep-them-that-way
(or http://tinyurl.com/83vrn5b)

<u>Should passwords be changed frequently?</u>

- Many experts believe that passwords should be changed on some periodic basis.
    - In this way, if a hacker cracks a password, they will be locked out again after the password is changed.
- Other experts believe that forcing users to change passwords on a regular basis may not help.
    - Suppose a current password is My!password01.
    - If this password is cracked and then changed, it might now be My!password02, My!password03, or so forth. (Sound familiar? ☺) This gives the hacker a limited pool of alternate passwords from which to choose.
- OSU requires O-Key passwords to be changed every 120 days or more frequently.
- OSU also prohibits the reuse of the four most recent passwords.
    - This is to reduce the likelihood that hackers who have compromised an account simply can try old passwords again in a short period of time.

Should passwords be reused?

- Best practices dictate that each account should have its own unique password.
    - Otherwise, when a hacker has one of your passwords, he or she can get into several of your accounts.

Password Generators

- There are websites that provide you with strong, random passwords. For example:
    - http://strongpasswordgenerator.com
    - http://random.org/passwords

How do you keep track of passwords?

- Sticky notes
- Text files
- Excel files
- TrueCrypt and its cousins (We have discussed TrueCrypt in a previous session.)

Password Managers

- A better alternative might be to use a *password manager.*
- All password managers basically work the same way: they store all of your account IDs and passwords in an encrypted file, controlled by a *master password.*
- One distinction between different password managers is the same one we see with many software products:
  free vs. commercial.
    - In general, commercial products will be more full-featured than their free counterparts.
    - Further, some commercial products charge a yearly subscription fee for all of your devices, while others charge a one-time fee per device.

- Another distinction between password managers is: single vs. multiple computers.
    - If you manage passwords on only one computer, then just about any password manager will do.
    - But, if you manage passwords on several computers (all of the same operating system, say MS Windows or Apple OS X), then you might want to look at a password manager that stores its information in the cloud. That way, you will have access to your passwords on different computers.
    - However, this also means that the computers must be on the Internet (at some time) to retrieve the passwords.
- One final distinction between password managers is: single vs. multiple operating systems.
    - If you manage passwords on only one operating system, then you have more products from which to choose.
    - But, if you manage passwords on several operating systems (MS Windows, Apple OS X, Apple iOS, Android, etc.), then you probably will want to choose a solution that works on all of these operating systems.
- Here are a couple of useful websites where you can learn about some popular password managers:
    - *10 of the best multi-platform password managers for iOS, Android and the desktop* (http://thenextweb.com/apps/2013/10/06/10-of-the-best-multi-platform-password-managers-for-ios-android-and-the-desktop/#!pAWmL)
    - *Five free and secure password management apps* (http://www.techrepublic.com/blog/five-apps/five-free-and-secure-password-management-apps)

KeePass

- In our session today, let's take a look at some members of the KeePass family of open source software:
  - *KeePass* (http://keepass.info) – A cross-platform password manager.
  - *MiniKeePass* (http://minikeepass.github.io/) – A version of KeePass for iOS (iPhone/iPod/iPad).
- KeePass features:
  - Cross-platform.
  - Portable version (for flash drives) available for Windows.
  - Includes customizable generator for strong passwords.
  - Mouse button can be used to bring up a URL in your browser, copy your account ID to the clipboard, and copy your password to the clipboard.
  - The account ID or password is erased from the clipboard after a number of seconds (12 seconds, by default).
  - Each entry has a note area in which one can store such info as answers to security questions.
- MiniKeePass features:
  - View, edit, and create KeePass files.
  - Import/export KeePass files between your device and either Dropbox or iTunes.
  - Optional PIN to keep others from using MiniKeePass on your device.
  - You can store database passwords in the device's secure keychain.