Password Management

March 2022

The Necessity of Strong Passwords

- Who is after your password?
  - It isn't an individual, or even a room full of individuals who are trying to *crack* your password.
  - Rather, *banks of computers* are being used to perform the task … and computers do not sleep, eat, take smoke breaks, demand worker's rights, etc.
- Affordable hardware for hackers
  - The top video cards used in PCs to meet the demands of today's video games cost about *$1,500* and can process data at the rate of more than *30 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 *7 teraflops*.

How Strong is Strong Enough?

- Password length
  - Eight characters used to be good enough, but in recent years the minimum suggested password length has extended to at least *14-16 characters*.
    - Some sites suggest *16-32 characters*.
  - But length isn't the only metric by which password quality is measured.
    - After all, we could use *a string of 32 1's*.
  - The complexity of the password matters, as well.

- Password complexity
  - As cartoon artist XKCD puts it,

    Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
    (https://xkcd.com/936)

  - To put it another way

    If your password is easy to remember, it probably can be cracked easily.

    If your password is too complex to remember, you'll probably write it on a sticky note and put it under your keyboard.

Worst Practices

- Don't call me if you do these …
  - Short or predictable passwords
  - The same password on multiple accounts
  - Write it down and keep it with computer
  - Write it down, keep it elsewhere, but label what it is
- Common bad practices
  - Having different passwords for different accounts is a good thing, but then the temptation is to:
    - Write them in a notebook
    - Store them in a text file
    - Keep them in a spreadsheet

- Top 10 most common password 2022 (https://md5hashonline.com/most-common-passwords)

10. abc123	5. iloveyou
9. 12345678	4. password
8. rockyou	3. 123456789
7. 1234567	2. 12345
6. princess	1. 123456

Best Practices

- Finding the right balance (https://lastpass.com)
  - It is better to choose a *longer password* that is easy to remember than a shorter password that is too complex to remember.
  - But it still is the case that the password should be *complex enough* to make it difficult to guess or crack.
- Password generators
  - There are websites that provide you with strong, random passwords. For example:
    - https://www.lastpass.com/features/password-generator
    - https://passwords-generator.org
  - If you subscribe to a password manager product, it will generate passwords for you.
- Passphrases
  - Instead of a password, we can create a *passphrase* by appending together several random words, perhaps followed by a number or with special characters separating the words.
  - The LastPass website (https://lastpass.com) suggests that you, "tell a story unique to you like *Fidoate!my2woolsox*."

- Passphrase generators
  - There are several websites that will generate passphrases for you.
  - These passphrases were generated by https://useAPassphrase.com:
    - linoleum yeah fled demise
    - overdress clerk uncaring finished
    - radiant jacket reclaim refined
- Password managers
  - If you use different, strong passwords or passphrases on different accounts, keeping track of them can be painful.
  - A better alternative is to employ a *password manager*.
  - All password managers basically work the same way: they store all your usernames and passwords in an encrypted file, controlled by a master password.
    - They make it easy to copy usernames and passwords into browser fields.
    - A master password protects the *password vault*.
  - According to CNET (https://www.cnet.com/tech/services-and-software/best-password-manager), the best password managers for 2022 are:
    - Best free PM: *Bitwarden* (open source, $10/yr for premium version)
    - Best paid PM: *LastPass* ($36/yr)
    - Best paid PM for multiple platforms: *1Password* ($36/yr)
  - Most password managers are available on all common platforms:
    - Windows
    - macOS
    - Linux
    - iPhone/iPad
    - Android
- Forgotten master password?
  - Paid products provide a way to recover lost master passwords using biometric info (fingerprints or face ID).
  - Free products do not always provide this service, so you must decide how important this is to you.

Now the Bad News

- There is no risk-free solution
  - Keep your passwords in a notebook or unencrypted file and take the chance that this is destroyed, deleted, or stolen; or
  - Utilize a password manager and take the chance that you will forget/lose the master password and be unable to retrieve it.
- Risk mitigation strategies when using password manager
  - More secure: Store a printed copy of the master password in your safe deposit box.
  - Less secure: Store a printed copy of the master password at a trusted, off-site location.

Any Questions?

- You can reach me at blayne.mayfield@okstate.edu