Password Management

Eugene Davis
UAH Information Security Club
January 10, 2013

Password Basics

- Passwords perform service across a broad range of applications
  - Can act as a way to authenticate a user to a system
  - Can serve to seed a key for encryption
  - Can simply be made to unlock system regardless of who they are
- Good password storage for a website should see the password stored as a hash, meaning that the original password cannot be directly retrieved
  - Unfortunately, often this is not the case
  - In systems that store plaintext passwords, your password may be leaked should the system be hacked

Password Creation
Best Practices

- A good password should be at least 15 characters, using upper- and lower- case letters, numbers and symbols
- A password should never be repeated between two systems
  - If the system stores the password incorrectly and is compromised, then both systems are compromised
- No predictable pattern should exist relating different passwords together
- Passwords should be updated every few months, and remain distinct from current and past passwords

Password Management

- Given the sheer number of systems the average person must maintain passwords for, memorizing everything soon becomes untenable
- As a result, password management schemes must be created. Two basic types exist:
  1. The use of a non-deterministic algorithm to aid the memorization of the passwords
  2. The use of software to track, create, and maintain passwords meeting the specifications

Keeping It In Your Head

Non-Deterministic Algorithms for Password Memorization

1. **Pass phrases** – long, memorable phrases that take the place of a password
2. **Replacement of characters** – take a memorable password and replace it with symbols and numbers
3. **Password Haystacks** – select a fixed password and generate a random number of a selected character to pad the password in one or more locations

Keeping It In Your Head Cont.
Pass Phrases

- A pass phrase is a password composed of a lengthy, nonsensical phrase
  - Pros:
    1. Easy to remember, similar to a mnemonic
    2. Done correctly they present a high degree of entropy
    3. Assuming they are unrelated between systems, they are hard to guess (“crack”)
  - Cons:
    1. Become overwhelming if you require many pass phrases
    2. Require you to come up with random phrases every time you need to create a new password, or update an old one
    3. Require you to memorize many pass phrases

Keeping It In Your Head Cont.
Replacement of Characters

- With this scheme, you replace characters in a weak password with similar in appearance symbols or numbers
  - Pros:
    1. Easy to remember
    2. Slight improvement over the original password
  - Cons:
    1. Many cracking dictionaries already contain most variants of password
    2. For shorter passwords, still very vulnerable
    3. Still requires the memorization of distinct passwords for every system

Keeping It In Your Head Cont.
Password Haystacks

- In this password generation algorithm (created by Steve Gibson), a single password is used and padded with many, easy to remember, symbols until a long length is reached
  - Each system has the same password, with a different number of symbols
  - Example: cat could become c@@@@@@a@@@@t@@
  - Pros:
    - Easy to remember
    - Increases the length of the password rapidly
  - Cons:
    - Has a low amount of entropy
    - If an attacker figures out the pattern, the protection is further reduced
    - Requires you to remember the number and locations of the symbols for each site

Password Management Software

- A better alternative exists to attempting to memorize all your passwords in password management software
- Good password management software should:
  - Be encrypted with the current best encryption algorithms
  - Generate random passwords seeded by collected entropy
  - Be portable across multiple platforms and devices

Password Management Software
KeePass

http://www.Keepass.info

- KeePass is a free and open source password manager
- Available on Windows, Linux and Android
  - A portable version exists for Windows
  - An app (not official Keepass) exists for iPhones
- Database is encrypted by 128-bit AES (or Twofish)
  - Both are secure, government-used and approved encryption algorithms
- Generates random passwords, optionally using user input to collect entropy
- Stores the sensitive data used while running encrypted in process memory
- Newer versions (2.x) include protection against key loggers

Password Management Software
KeePass – Pros/Cons

- Pros:
  1. Portable across three major platforms (Android, Linux, Windows)
  2. Secure against many attacks
  3. Requires the memorization of only one password
  4. Windows versions integrate with web browsers
- Cons:
  1. Requires you to keep the database file with you if you need it
  2. Is not compatible with multi-factor authentication
  3. Linux, Android and iPhone versions remain in the 1.x line

Password Management Software
LastPass

https://lastpass.com

- LastPass is commercial software similar to Keepass, but with additional features
  - The database file is stored “in the cloud”
  - Operates over a far larger range of devices (including Apple)
- A free version exists, as well as a $12 a year version
- Functions as a browser plugin to all major browsers
- Database encrypted with 256-bit AES
- Master password is turned into the encryption key only after many rounds of hashing
- Premium version can generate one-time keys (use once, then throw away) that decrypt the database for access at public terminals without compromising your master password
- Premium version supports Yubikey, a multi-factor authentication device

Password Management Software
LastPass – Pros/Cons

- Pros:
  1. Portable across all major platforms
  2. Allows access from any location without carrying the physical file
  3. Heavily encrypted (better than KeePass)
  4. Supports multi-factor authentication for accessing the database
  5. Is developed by a very security conscious company
- Cons:
  1. Stores password online, making it easier for attackers to get it (mitigated somewhat by the degree of encryption employed)
  2. Does not work well with applications outside of the web browser

Alternatives to Passwords
Using Other Forms of Authentication

- Two other forms of authentication exist
  - Biometrics – authenticating based on a physical attribute of the users
  - Possession – authenticating based on an item in the users possession
- Additionally, two or three forms of authentication may be used together to further increase security

Conclusion

- Unless you have a small number of passwords, select a software password manager
- Ensure that the password manager you select encrypts your password database well
- Select a strong master password