Password Manager - Wikipedia Re-Print

Edits by Dovell Bonnett

Dovell Bonnett
Founder and CEO of Access Smart.

"It is cheap and easy to design a high security system poorly. It is expensive and hard to design a security system to protect against every possible attack. It requires forethought and insight to design a useful security system at a high degree of trustworthiness and at an affordable price".
-- Tom Austin

Recently I had the opportunity to update Wikipedia's listing for "Password Manager". While many others have also contributed over time to this entry, I wanted to do a simple PDF reprint of this topic to help inform others about the advantages and disadvantages of a password manager system. While I don't know who else has contributed to the writing of this entry in Wikipedia, I want to thank and acknowledge their contributions.

General

A password manager is software that helps a user organize passwords and PIN codes. The software typically has a local database or a file that holds the encrypted password data for secure logon onto computers, networks, web sites and application data files. Many password managers also work as a form filler, thus they fill the user and password data automatically into forms. These are implemented using a browser extension, smart card application or USB stick application that communicates to the browser.
The great advantage of passwords is that they are readily incorporated in most software, require no extensive computer/server modifications and users are very familiar with them. While passwords are secure, the weakness is how users choose and manage them:

- Simple passwords - short in length, uses words found in dictionaries, don't mix in different characters (numbers, punctuation, upper/lower case), etc.
- Write passwords down - sticky notes on monitor, notepads by the computer, document in computer, whiteboard reminders, smart device storage in clear text, etc.
- Same password - using the same password for multiple sites, never changing account passwords, etc.
- Sharing password - telling others the logon passwords, sending unencrypted emails with password information, contractors using same password for all their accounts, etc.

The added problem is that most users do more than one of these mistakes. This makes it very easy for hackers, crackers, malware and cyber thieves to break into individual accounts, SMB's, multi-international corporations, government agencies, institutions, etc. It is protecting against these vulnerabilities that makes password managers so important.

Password Manager - Wikipedia Re-Print

Edits by Dovell Bonnett

Password managers come in five basic flavors:

- **Desktop - desktop software storing passwords on a computer hard drive.**
- **Portable - portable software storing passwords and program on a mobile device, such as a PDA, smart phone as a portable application.**
- **Token - a security token with multi-factor authentication combines "something you have" (smart card or USB stick), "something you know" (PIN or password) and "something you are" (biometrics).**
- **Web based - Online password manager where passwords are stored on a provider's website.**
- **Stateless - Passwords are generated on the fly from a master passphrase and a tag using a key derivation function.**

Password managers can also be used as a defense against phishing and pharming. Unlike human beings, a password manager program can also incorporate an automated login script that first compares the current site's URL to the stored site's URL. If the two don't match then the password manager does not automatically fill in the logon fields to safeguard against visual imitations and look-alike websites. With this built-in advantage, the use of a password manager is beneficial even if the user only has a few passwords to remember. While not all password managers can automatically handle the more complex login procedures imposed by many banking websites, many of the newer password managers handle complex passwords, multi-page fill-ins, and multi-factor authentication prior to usage.

Password managers can protect against keyloggers or keystroke logging malware. When using a multi-factor authentication password manager that automatically fills in logon fields, the user does not have to type any user names or passwords for the keylogger to pick up. While a keylogger may pick up the PIN to authenticate into the smart card token, for example, without the smart card itself (something you have) the PIN does the user no good. Add a biometric finger scan with the smart card and then the risk from malware is practically none.

Vulnerabilities

Desktop password managers and browser based password managers are convenient but are considered the weakest means to protect your accounts. That's because most of these applications rely on no authentication or a single factor of authentication. If the computer is on, it is possible for another individual to simply click where they want to go and they are in. Some password managers typically use a single user-selected master password or passphrase to form the key used to encrypt the protected passwords. The single passphrase is referred to as "single factor authentication" and is one of the weakest ways to authenticate the user. This master password

must be strong enough to resist attack (e.g., brute force, dictionary attacks, etc.), but complexity drives poor user management.

A compromised master password renders all of the protected passwords vulnerable. This demonstrates the inverse relation between usability and security: a single password may be more convenient (usable), but if compromised would render all of the held passwords insecure.

As with any system which involves the user entering a password, the master password may also be attacked and discovered using key logging or acoustic cryptanalysis. Some password managers attempt to use virtual keyboards to reduce this risk - though this again is vulnerable to key loggers which take screenshots as data is entered.

Some password managers include a password generator. Generated passwords may be guessable if the password manager uses a weak random number generator instead of a cryptographically secure one.
A strong password manager will include a limited number of false authentication entries allowed before the password manager is locked down and requires IT services to re-activate. This is the best way to protect against the brute-force attack.

Password managers that do not prevent swapping their memory to hard drive make it possible to extract unencrypted passwords from the computer's hard drive. Turning off swap, or installing more memory can prevent this risk.

Online password manager

An online password manager is a website that securely stores login details. They are a web-based version of more conventional desktop-based password manager.

The advantages of online password managers over desktop-based versions are portability (they can generally be used on any computer with a web browser and a network connection, without having to install software), and a reduced risk of losing passwords through theft from or damage to a single PC - also the same risk is present for the server that is used to store the users passwords on. In both cases this risk can be prevented by ensuring secure backups are taken.

The major disadvantages of online password managers are the requirements that you trust the hosting site and a keylogger is not on the computer you're using. With servers and the cloud being a focus of cyber attacks, how one authenticates into the online service and that the passwords stored there are encrypted with a user defined key are just as important. Again, users tend to circumvent security for convenience.

The use of a web-based password manager is an alternative to single sign-on techniques, such as OpenID or Microsoft's Windows Live ID scheme (formerly Passport), or may serve as a stop-gap measure pending adoption of a better method.

Security token password managers

Security tokens like smart cards or secure USB flash devices are seen by security experts as the best way to authenticate users, since many require multi-factor authentication. The data stored in the token is usually encrypted to prevent probing and unauthorized reading of the data. Some token systems still require software loaded on the PC along with hardware (smart card reader) and drivers to properly read and decode the data. Some of the other advantages include: tokens can also be either contact or contactless smart card, stand-alone client based or tied into active directory. These tokens can be combined with RF ID badges for building access and use other security protocols like Single sign-on (SSO), One-time passwords (OTP) and Public Key Infrastructure (PKI) instead of passwords to establish the trust. These tokens can be thought of as the key to secure the virtual front door.

The disadvantages include the different costs of ownership. Some implementations require back end server modifications, extensive training, server-to-token synchronization, outside certificate authorities and expensive tokens. Others may be less expensive to implement and have a lower cost of ownership, but many not support Authentication, Authorization, Data integrity and Non-Repudiation. It's not that one token solution is better than another, but rather which is right for your environment, risk and budget.