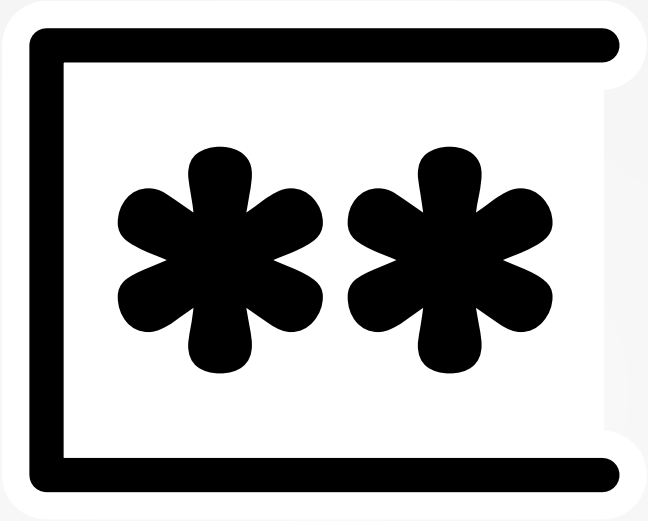
Password Managers



Adam Bolte
abolte@systemsaviour.com

The problem: Too many passwords!

- Each website account requires a password.
- Users have to think something up!
- Strong memorable passwords take time, so what to do?
  - Choose simple passwords that are easier to remember!
  - Reuse passwords wherever possible!
  - Save them in plain text files on the computer, a nearby notebook, or even just sticky notes stuck to the monitor bezel.

Pitfalls of bad security

- Passwords for one account compromised mean all accounts are compromised where accounts are shared.
  - You must assume passwords are not salted and rainbow tables are available, as it's impossible to know how secure your credentials are on any given server you do not have privileges for.
  - You cannot expect to always know when one of your accounts has been compromised (the service provider's machines may have been compromised without their knowledge), and there is often strong incentive to not tell.
  - You would have to remember all accounts using the same password, if you ever hope to reset all passwords in the event of a reported breach.
- Compromising one account may provide an attacker details to compromise other accounts (eg. Accounts that show security questions in the clear that may be used elsewhere, e-mail accounts which can reset passwords).

The End

- Thanks, and good luck! :)

- Oh hold up, there is actually a solution!

The solution: Password managers!

- Generates passwords for you.
- Specify how complex you want them to be.
- Only need to remember a single passphrase – it is now practical and easy to have a unique password for every account.
- All passwords are encrypted (and ideally restricted to personal hardware).
- No need to set security questions.

Password Managers

- Programs I have personally used extensively include:
  - Revelation
  - KeepassX 0.4.X
  - KeepassX 2.0-alphaX
  - pass
  - Firefox Sync
  - Gpgsea
- However, I have also tested many other programs.

Revelation

- http://oss.codepoet.no/revelation/wiki/Home
- GPL2
- Easy to use
- Release tag line examples include “*You drive, I think there's something wrong with me*” and “*Too weird to live, and too rare to die*”
- No longer maintained
- History of concerning security vulnerabilities
  - http://knoxin.blogspot.com.au/2012/06/revelation-password-manager-considered.html
  - Max 36 character master password!
- Implemented in Python, but slow with many passwords

KeePass

- http://keepass.info/
- GPL2+ (mostly, some MIT and LGPL code also)
- 1.x written in C++
- But the current 2.x is written in c# (so requires Mono on GNU/Linux)!
- Includes an interesting “Trigger” system, a password strength meter, basic security policy options, various interface customisation options, and support for key files.
- Provides the option to store files, and add custom fields.
- File dialog boxes are not well suited for GNU/Linux.
- Supports plug-ins, but many do not appear GNU/Linux compatible, and there are questions concerning licensing.

KeePassX

- https://www.keepassx.org/
- GPL2 or (at your option) GPL3
- Unlike KeePass 1.x, KeePassX has always been cross-platform compatible.
- Version 2.0 almost ready – a rewrite from scratch due to 0.4.x being difficult to maintain, wanting KeePass 2 .kbdx file-compatibility, wanting a GUI compatible with smaller displays such as that on the N900 (doing away with pop-up windows), etc.
- Not as feature-full as KeePass 2.x, but it's based on Qt instead of Mono so runs better.

Pass

- http://www.passwordstore.org/
- GPL2+
- Written in Bash
- Unix philosophy
- Import scripts from many different password managers.
- CLI-only
- Essentially just a wrapper around *xclip*, *gpg*, *pwgen, git* and *tree* commands.
- Very active community (3rd-party support for GUIs, Android, Firefox extensions, etc.)

Password Gorilla

- https://github.com/zdia/gorilla
- GPL2+
- Written in Tcl/Tk
- And looks it too. :)
- Yet has all the essential functionality you would expect, so is actually not bad.
- Last commit to master was last year.

Others (no longer maintained)

- fpm2 (GTK2 port of the ancient and very dead Figaro's Password Manager)
  - GPL2+ (and compatible)
  - http://als.regnet.cz/fpm2/
  - Supports a key file option
  - Buggy (easy to segfault, long delays to collect entropy)
- Ked Password Manager
  - GPL2+
  - http://kedpm.sourceforge.net/
  - Quite primitive GUI
  - Interesting CLI interface (but no ability to auto-clear passwords after a timeout period)
  - Last updated 2005

Others (no longer maintained)

- Gpass
  - GPL2+
  - http://projects.netlab.jp/gpass/
  - Interesting “password expiration” field
- GPassword Manager
  - Apache License V2.0
  - http://sourceforge.net/projects/gpasswordman/
  - Not very professional – difficult to build, source provided by zip file (and doesn't extract to a sub-folder), some program directories have spaces... too scared to try it! :)
- ...and many many more

Browser Built-in Password Managers

- Firefox
  - Optionally encrypts locally
  - Firefox Sync
    - Can sync to ownCloud
- Chrome/Chromium
  - Local passwords stored in the clear (no encryption option)
  - Syncing requires a Google Account
    - Privacy? Probably not!

Browser Password Manager limitations

- No password generator.
- Doesn't work well with passwords for things other than websites.
- Difficult to sort (no categorisation, etc.)
- No password change history.
- Greater security risks present.

Group password sharing

- Proprietary
  - LastPass: https://lastpass.com/
  - PassPack: https://www.passpack.com/
- Free software
  - Mortimer: https://github.com/aiaio/mortimer
  - Pass

Other security considerations

- Two factor authentication.
- Password manager browser integration via extensions?

Summary

- Always use a password manager.

- Thanks for watching!