Password Manager Software

Identity & Access Management Office

Information Technology at Purdue
Office of the Vice President for Information Technology
Purdue University

Abstract

This document discusses a type of software application called a Password Manager. Several Password Manager offerings for the Windows operating system are reviewed and a recommendation is presented.

Contents

Introduction....3
Security Features....4
Recommendation.... 4
  Password Safe (FOSS)....5
Runner up....6
  KeePass (FOSS)....6
Honorable Mention....8
  Oubliette (FOSS).... 8
Other Password Managers.... 11
  Password Gorilla (FOSS)....11
  PINs (FOSS).... 11
  RoboForm (Commercial)....11
  Any Password (Commercial)....11
  Turbopasswords (Commercial)....12
Conclusion.... 12

Password Manager Software

Introduction

There are currently many password manager software applications available. These provide a central, secure location to store account passwords, PINS and other sensitive information and lock it all up with a single master password. The need for these applications, also referred to as "password vaults" or "password databases", is expressed in the following quote:

> Over time, managing a plethora of logins becomes near impossible. Few people can remember more than a handful of passwords. This inevitably leads to either a proverbial yellow sticker on your desk, with all the passwords written down, or to the reuse of the same few passwords over and over again. Neither approach is very secure. In the first case, a co-worker could spy on your passwords, in the second, if an attacker manages to guess or intercept your passwords, many of the services you use can be accessed.
>
> Adding to the confusion is the multitude of password policies that different services enforce. E.g., some services require passwords to contain mixed case and non-alphabetic characters, or to be shorter or longer than a certain number of characters. Other services require you to change passwords every month, quarter, or year.
> - http://www.fpx.de/fp/Software/Gorilla/

This document attempts to provide an evaluation and brief overview of some of the password manager software available for the Windows platform. Some are free and open source software (FOSS) and some are commercial products which require a license and fee.

Security Features

The best of these software applications all share similar security characteristics. For instance, they all encrypt the passwords using a strong symmetric encryption algorithm such as AES or Blowfish. They all mask the password from the view of prying eyes and shoulder surfers. They support a method of entering the password at login prompts without the need to type them. This prevents shoulder surfing as well and also thwarts key loggers. If the clipboard is used to copy a password from the application it automatically clears the clipboard afterword. The best of them keep passwords encrypted even in the memory of the running application. This prevents the contents of the computer's memory or pagefile from divulging plaintext passwords.

Another characteristic that many of the best share is being open source. This allows other programmers the ability to read and audit the program code to ensure that it does what it claims, and correctly implements encryption and other security characteristics. A noted cryptography expert had the following to say:

> As a cryptography and computer security expert, I have never understood the current fuss about the open source software movement. In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice.
> - Bruce Schneier, Crypto-Gram, September 15, 1999

Summary of Security Features

- Masks passwords by default
- Clears clipboard
- Encrypts contents of memory
- Doesn't require typing the password - thwarts keyloggers
- Open source

Since the encryption of the password database is built into the software, it does not matter where the software is installed or where the password database is stored. Some password manager software comes with an installer and will install to the usual Windows location. Some do not require installation at all; the executable is simply moved to a location of the user's choosing. It does not matter where it is located. It can be placed on a USB flash drive for convenience, or in the Windows "My Documents" folder.

The master password for the password manager must be complex and strong. It should be at least as strong as the most sensitive password stored inside. If the password manager stores any passwords that are subject to the requirements of a password policy, then the same requirements should be observed for the master password.

Recommendation

Since the top password managers all share similar security characteristics, the criteria for choosing one to recommend comes down to convenience and ease of use. Two password managers stand out; "Password Safe" and "KeePass". Both are very capable, feature rich and secure. But Password Safe slightly nudges past KeePass as the password manager recommended here.

Password Safe (FOSS)

Password Safe is a password manager originally created by noted cryptography expert Bruce Schneier's Counterpane Labs. While it has always been free, it eventually became open source.

It has a very simple and intuitive user interface. A very nice feature first noticed upon launch is the ability to open the password database read-only. This prevents accidental modifications to the password database when the intent is merely to retrieve a password rather than to modify one. Password Safe requires no installation. It can run self-contained from a USB flash drive and is also available for the new USB technologies called PortableApps and U3.

Password Safe has many convenient security features, one being that after a certain configurable timeout period it locks and minimizes to an icon in the task tray where it sits ready for a double-click when needed. Another nice feature is that it warns if the master password chosen is too weak.

Usability features are nice as well. Password Safe has a password generation feature. It also automatically keeps a history of all previous passwords. It allows an expiration to be set on certain passwords; when the password is about to expire a warning is generated alerting the user that the password needs to be reset. It also allows a password policy to be set; new passwords will be checked against the requirements of the policy and auto-generated passwords will automatically be compliant. This is very convenient in settings where it is important that passwords adhere to certain requirements. Other notable features are a convenient backup function and a nice automatic form filler.

Password Safe just slightly nudges past KeePass as the recommended Password Manager. It has a slightly cleaner user interface and also currently appears to have more active developers.

Password Safe Features

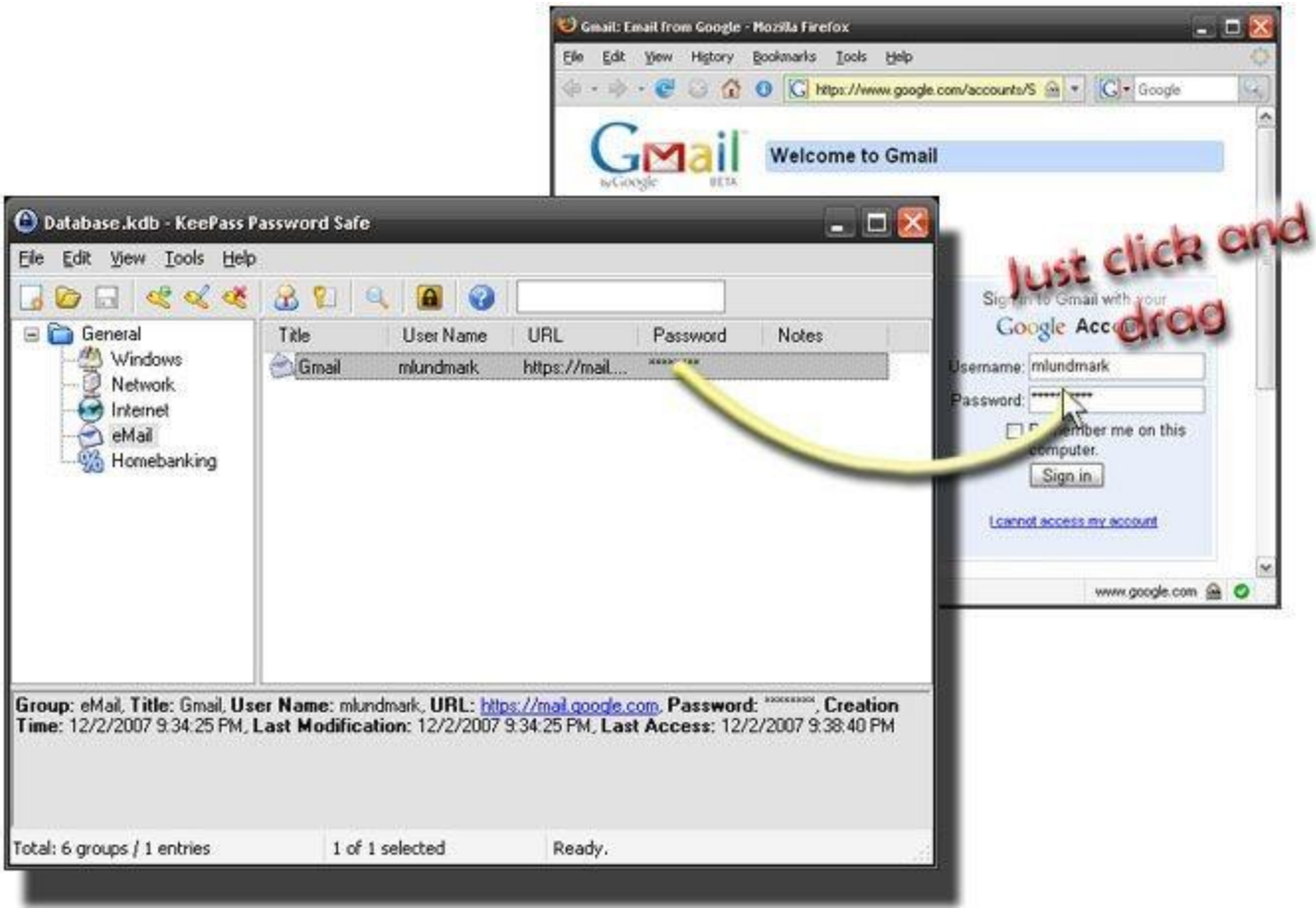
- FOSS
- Can open the password database read-only
- No install, can run from USB flash drive, U3, PortableApps
- Random password generator
- Minimizes to Task tray and locks, has timeout period
- Warns if master password is weak

- Maintains password history
- Configurable password expiration warning
- Can set a password policy
- Backup function
- Nice auto form filler
- Blowfish Encryption
- Website: http://passwordsafe.sourceforge.net/
- See also link: http://en.wikipedia.org/wiki/Password_Safe

Runner up

KeePass (FOSS)

Another very good password manager is KeePass. It has a rather refined and well organized user interface. Its best feature is probably the ability to easily drag the username and password into the form fields on a login page. This a strong feature for those who use various online accounts on a daily basis.



The drag and drop feature must be used with care, however. The password must be dropped with accurate aim into the password field and not accidentally outside it! As the author found out, bad things can happen if the aim is a little off!

Like all good password managers it organizes passwords for accounts into categories and offers a search function. It tracks information for each such as the time that the password was last changed, account related notes, and password expiration date if applicable. All of the account information is easily viewable in a convenient pane at the bottom of the application window. KeePass has a timeout feature that automatically locks and minimizes its window after a certain period of inactivity. It minimizes to a nice padlock icon in the Windows task tray.

KeePass has a couple of nice features that could probably be considered overkill for most non-NSA applications but are really cool to security geeks. Similar to other Password Managers, the master password for the password database can be a typed password, but with KeePass it can also be a key file, or a combination of key file and typed password. In password manager software the master password is used as the key that encrypts the database. So a longer key makes for an exponentially more secure password database, consequently using a key file can potentially make your passwords more secure.

Another feature where KeePass goes way beyond most password managers to the level of truly paranoid is with its password generator. A password generator is a feature that will automatically create a new random password. Random passwords tend to be stronger because they are harder for someone else to guess. Computer Science types may point out, however, that the randomness of most computer programs is not truly random and with some (significant) skill can be predicted. This is not so with KeePass. When it generates a random password it first asks the user to create entropy. Entropy is used to make computer generated randomness more random. KeePass appears to be the only popular password manager with this feature.

Unfortunately, there are some features lacking in KeePass that are found in most other top password managers. One is a built in password policy checker such as the one found in Password Safe. There are other features lacking as well. KeePass does not warn when the master password is weak. It does not maintain password history. With KeePass you could manually keep your password history in the notes section, but that is not very convenient. KeePass does have a version that maintains password history, but as of this writing it is in alpha development and not recommended for daily use.

KeePass comes in a few different versions. The version evaluated here is "KeePass 1.09 (ZIP Package)" from http://KeePass.info/download.html. It does not require installation. It can simply be unzipped into a directory and remain totally self contained or run from a USB flash drive for portability. KeePass also has versions specifically made for the new USB technologies called PortableApps and its commercial cousin, U3.

Despite a few missing features, KeePass is still a highly capable password manager. It is convenient, secure, and trustworthy. It happens to be free and open source, but is better than some non-free commercial products.

KeePass Features

- FOSS
- Minimizes to task tray and locks, has timeout period
- No install; can run from USB flash drive, PortableApps and U3
- Random password generator

- Intuitive user interface
- Account info pane at bottom of application
- Very convenient drag and drop functionality
- AES Encryption
- Website: http://KeePass.info/
- See also link: http://en.wikipedia.org/wiki/KeePass

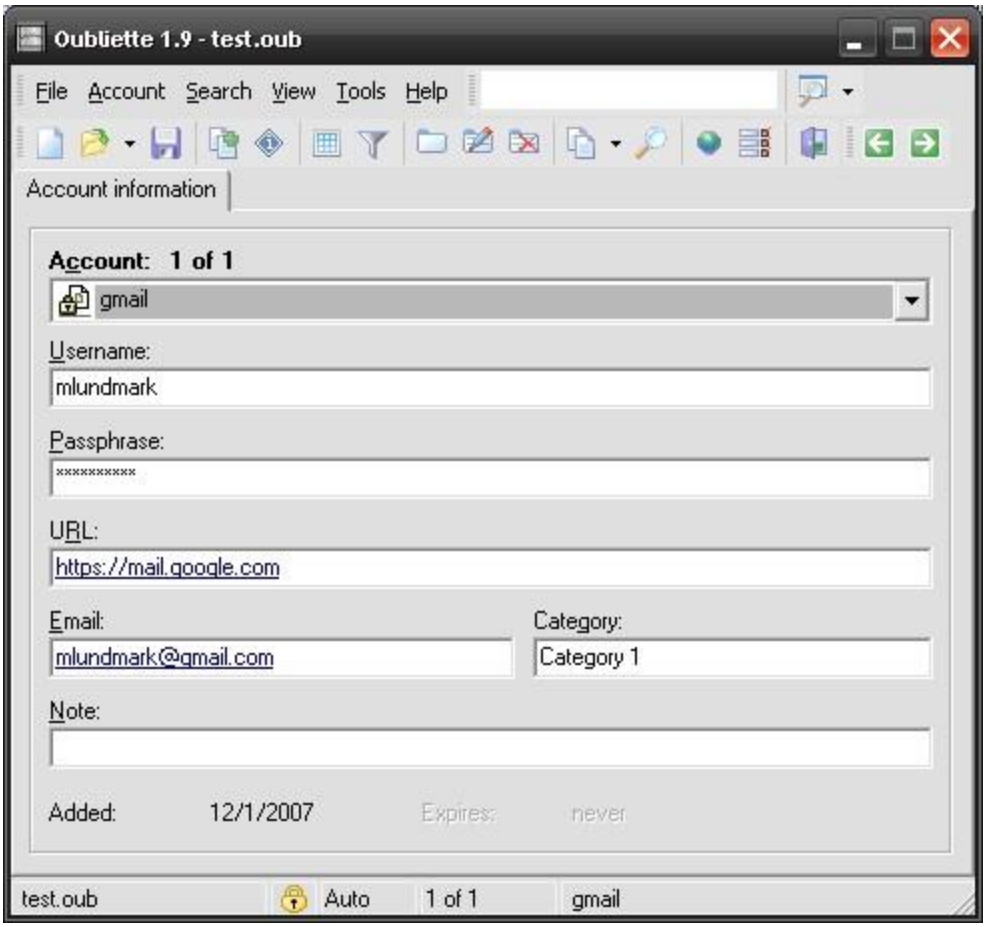
Honorable Mention

Oubliette (FOSS)

A very capable and feature rich password manager is Oubliette. Its interface is a bit different than the rest. Rather than presenting the accounts (and passwords) as a list or tree view like many do, it instead provides navigation via a drop down list or a search box. Some users may find this handy, while others may not. It has a nice website and very good documentation. This password manager is no longer under development due to the programmer's time constraints. This very likely does not matter as it appears to be a very complete and feature-rich password manager. Just don't expect any bug fixes or updates.

Similar to many other password managers, getting the password out of Oubliette and into the password form field when logging into an account can be accomplished several different ways. The clipboard with a copy/paste operation can be used or a convenient drag and drop feature can be employed. If the clipboard is used, Oubliette will clear the clipboard afterword. It also has a nice automated form filling feature. Some of these features can improve not only convenience but also security. Since these features prevent the actual typing of a password, any potential keyloggers that could be maliciously installed on the computer are rendered useless. Oubliette has many configuration options to tailor its behavior. A bonus feature of Oubliette that is not often found in password managers is the ability to encrypt files on disk.

One unfortunate design decision is that by default passwords are not masked. This is a setting that can be configured, but it is peculiar that this is not the default.



Oubliette Features

- FOSS
- Good website, good documentation
- Does not mask passwords by default (unfortunately) but can optionally
- Project not currently under development; current version is 1.9.5, last updated 2003
- Random password generator
- Encrypts/decrypts files on disk
- Has space for encrypted notes for each account
- Uses/clears clipboard and has a very nice drag to web page feature
- Automated form filling
- Highly configurable
- Blowfish or IDEA encryption
- Website: http://www.tranglos.com/free/oubliette.html

Other Password Managers

Here is a brief survey of some other password manager software. Some are better than others. Their noted advantages and disadvantages are listed below.

Password Gorilla (FOSS)

- FOSS
- Based on the "Password Safe" password manager, but extended to be crossplatform (not Windows only)
- Stand alone executable
- The look and feel is almost identical to Password Safe
- Twofish encryption
- http://www.fpx.de/fp/Software/Gorilla/
- "Password Safe" is better on a Windows platform because it has more features

PINs (FOSS)

- FOSS
- Does not require installation
- Nice password generator; by default meets standard best practices for password complexity and are reasonably easy to remember
- Has secure file deletion feature
- Has character map feature so you can have characters in your password that don't exist on the keyboard
- Character map feature allows entering password using mouse, password never has to be typed, not even the first time - thwarts key loggers
- Nice auto form filler thwarts keyloggers
- User interface needs some polish
- Locks periodically, even when in use – very inconvenient
- Passwords not masked by default, but can be optionally
- Nice list type layout with note section displayed at bottom
- http://www.mirekw.com/winfreeware/pins.html

RoboForm (Commercial)

- Rave reviews, lots of features
- Enterprise and mobile (USB/U3) versions
- Free version is very limited
- Pro version $30
- Has mobile version that works with USB Key and U3.
- AES Encryption
- http://www.roboform.com/
- Older Freeware version still exists that has full functionality: http://www.321download.com/LastFreeware/page7.html#AI%20RoboForm

Any Password (Commercial)

- Commercial product with confusing license; free for personal use, otherwise $19 including for edu, $25 for pro, free trial period

- Can run from USB key
- Password generator
- Password not masked by default; can set to mask all, but then cannot unmask - very inconvenient
- Multi-user
- Stores files as well
- Can open in read-only mode
- CSV import/export of account information
- Documentation is limited
- Inconvenient user interface
- IDEA Encryption

Turbopasswords (Commercial)

- Commercial, from Chapura, makers of software that runs on Palm handhelds, $30, free trial
- Passwords not masked by default (can be optionally)
- Works with Windows and synchronizes to any Palm OS handheld
- Integrates with IE & Firefox; setup program installs a Firefox plug-in; this is inconvenient; the others integrated suitably without needing browser plug-ins (some, less tech-savvy users, may find this convenient, however)
- Auto-fill feature is bad; too automated; after signing out of a site it immediately auto-fills the username/password box again automatically even if not needed
- Does not take advantage of the Windows task tray
- No way to locate or move the password database after initial creation
- Saves files in the "My Documents" folder with no way to change locations

Conclusion

Even though these evaluations were made regardless of the cost of the software, it just so happened that the FOSS password managers blew away the commercial ones. You can't go wrong with password manager such as "Password Safe" or "KeePass".