Sufyaan's Website

sufyaan.me/kpst

KeePass + Syncthing

23 June 2023

Category: Software

I have decided to switch from a self-hosted Vaultwarden (Bitwarden) instance to using KeePass along with Syncthing to sync it to all my devices. There are numerous reasons why I decided to make this change.

Security

The offline nature of KeePass makes it so that it is nearly impossible to crack. Connecting things to the internet makes it trivial for a script kiddie thousands of kilometers away from you to attempt to crack your passwords. A password manager is a place where all of your passwords are stored. Due to this very reason, I decided to upgrade my security by moving to a reputed piece of software.

It has a plethora of security features. Firstly, it has the ability to generate passwords of any length. It allows you to choose what characters are allowed. Its generation is so complex and liberating that even foreign characters like Æ, É, or even mathematics symbols and arbitrary symbols that no one would care about can be used. For example, the division sign (÷) or the copyright symbol (©) are included in password generation. Since most hackers try alphanumeric character cracking, KeePass password generation can make your passwords practically impossible to crack.

The encryption algorithm used for your password database is AES-256, commonly known as 256-bit encryption. It is a form of encryption that is so difficult to crack that the only way you can actually hope to obtain someone's password is by phishing them or using external methods. For more information, please watch this video by 3Blue1Brown. It is extremely interesting.

In fact, KeePass is so secure that even the passwords that are stored in your memory while you are viewing your database is encrypted. That way, even a management engine attack will not work. If you want to try viewing the cleared memory sectors to find remnants of your passwords, good luck. The passwords which are stored in your memory are first overwritten to the point of unrecoverability before being cleared.

You can even setup a keyfile (a file you need to use to login), a security key, or both.

View. The. Code.

KeePass is open-source under the GPLv2 license, which is the best open-source license for people's freedom. That makes it free software.

The Encryption Never Stops

Along with KeePass, I use Syncthing to sync my database. Syncthing also uses cryptographic encryption. This makes it so that anyone who wants to brute-force my database needs access to both my Syncthing password and my KeePass password.

To Conclude...

I use KeePass along with Syncthing for three reasons.

1. KeePass is extremely secure. It has industry-standard protection methods and algorithms and its offline nature makes it practically uncrackable.

2. It is fully free software under the GPLv2 license
3. Syncthing is also encrypted, which means that an attacker who wants to attack me using the internet needs to crack both my Syncthing password and KeePass password which would take billions of years.

I am probably never going to switch back because this system works extremely well. Syncthing is very fast at staying up-to-date.