Password managers

TG

Agenda

- What is a password manager?
- Benefits
- Possible issues
- Cloud-based or offline?
- Who is it for?
- Introduction to and showcase of KeePassXC

What is a password manager?

- An application that allows users to store, generate, manage, and retrieve complex passwords of online credentials
- Data is locally or remotely stored in an encrypted database file and unlocked by a single master password and possibly a key (token-based hardware devices or a file including a security token) for multi-factor authentication
- Typically using a industry standard encryption algorithm such as 256-bit AES (Advanced Encryption Standard) or other
- Open- or closed-sourced

Benefits

- Prevent simple and repeatably used passwords
- No need to memorize multiple passwords
- Store and organize credentials
- Secure credentials using encryption algorithms
- Prevent phishing or pharming (User may not know passwords to every site, Application may compare website URL)
- Prevents keystroke logging (keyloggers) through auto-fill scripts
- Prevents brute-force attacks by limiting the number of false authentications

Possible issues

- Requires taking backups regularly
- Risk of losing password access because of a single master password (preventable by using key or written down passphrase; depends on threat model)
- Theft or damage of hardware may result in losing access
- Can’t prevent man-in-the-browser attacks from malware or threat actors on the device
- Secuity of encrypted data depends on the master password or passphrase used
- Requires awareness of the user

Cloud-based or offline?

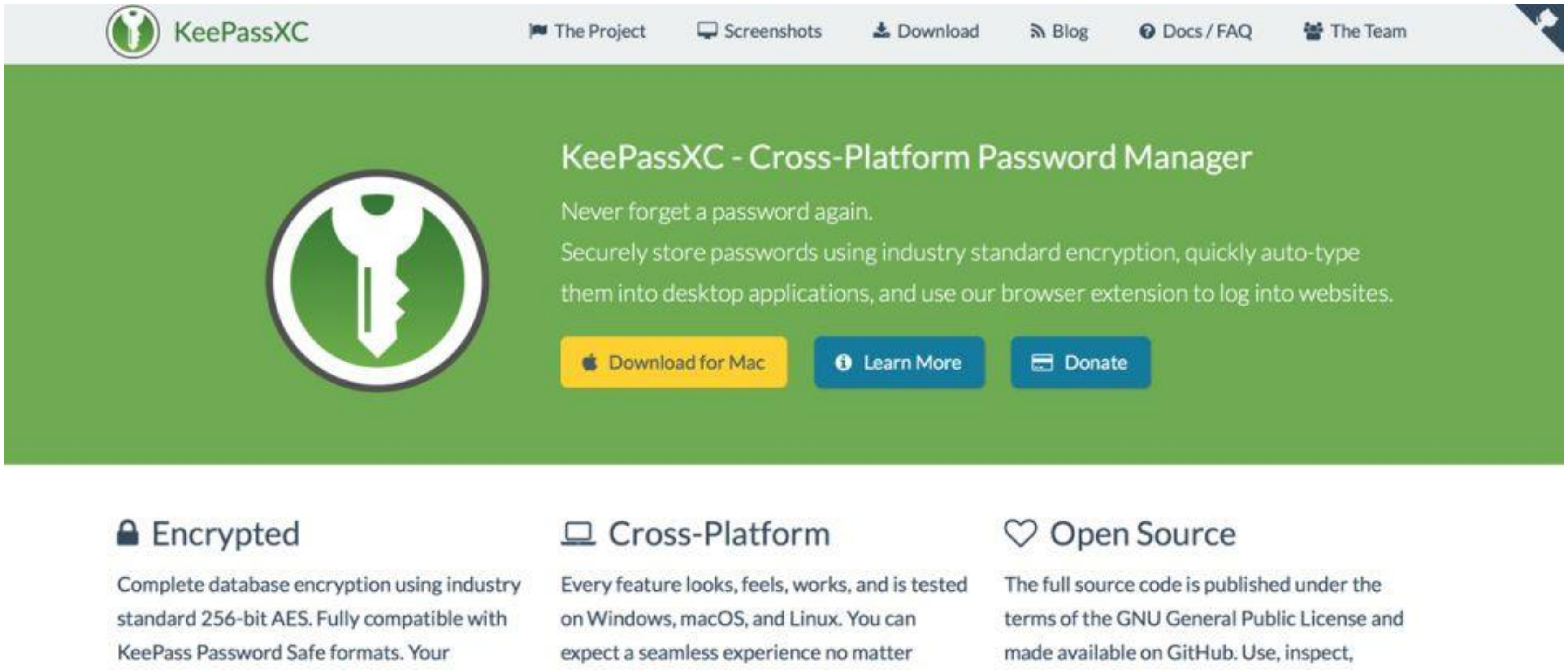
- Dependence on online file hosting service
- Application requires internet access permissions; may allow for possible leakage of data
- Offline is more secure as you don’t hand out the database file, but may be worse for convenience and offer less functionality (e.g. portability through synchronization across devices)
- User must trust the host of the web-based application to secure application and data sufficiently (prevent attacks from threat actors, keyloggers, bad encryption)
- Open-sourced or closed-source? What really happens with the data and in the background?
- Are additional features worth it?

Who is it for?

Questions to ask yourself

- Do I currently have strong and unique passwords?
- Do I value security above convenience?
- What type of attacks and threat actors am I worried about?
- Is a password manager available on the platform that I use?
- Do I trust a web-based solution and the host with its security practices?
- Does the password manager offer certain features and are they worth it? (e.g. data breach detection, password generation, auto-fill, synchronization, or other)

Introduction to and showcase of



KeePassXC - Cross-Platform Password Manager

Never forget a password again.
Securely store passwords using industry standard encryption, quickly auto-type them into desktop applications, and use our browser extension to log into websites.

Encrypted

Complete database encryption using industry standard 256-bit AES. Fully compatible with KeePass Password Safe formats. Your

Cross-Platform

Every feature looks, feels, works, and is tested on Windows, macOS, and Linux. You can expect a seamless experience no matter

Open Source

The full source code is published under the terms of the GNU General Public License and made available on GitHub. Use, inspect,

Passwordless future?

“We will continue to be vulnerable until change arrives”

“Until the passwordless future is here we need something to manage that for us”

Passkeys (Apple)

Windows Hello (Microsoft)

FIDO Alliance

Sign-in (Google)

Sources

- https://en.wikipedia.org/wiki/List_of_password_managers
- https://en.wikipedia.org/wiki/Password_manager
- https://blog.google/technology/safety-security/one-step-closer-to-a-passwordless-future/
- https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/
- https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy
- https://owasp.org/www-community/Threat_Modeling_Process
- https://developer.apple.com/passkeys/
- https://addons.mozilla.org/en-US/firefox/addon/keepassxc-browser/
- https://keepassxc.org

Thank you for listening!

Questions?