Technical University of Denmark

Project Agreement

Daniel Schougaard
s103446

November 24, 2015

1 List of Existing Solutions

- Rattic (https://rattic.org)
- KeePass / Other Local Stored Password Managers(https://keepass.org)
- LastPass (https://lastpass.com/)
- Encryptr (https://encryptr.org/)
- VAULT (https://vaultproject.io/)
- Vault (https://www.zoho.com/vault/application-security.html)
- TeamPasswordManager (http://teampasswordmanager.com)
- Secret Server Express (http://thycotic.com/products/secret-server/express/)
- Simple Safe (https://www.simplesafe.net/)
- PassWork (https://passwork.me/)
- SimpleVault (http://simplevault.sourceforge.net)
- PasswordState (http://www.clickstudios.com.au/)

2 KeePass & Other Locally Stored Password Managers

Since the breach of LastPass, KeePass and the like have been the go-to tools, for storing, generating and retrieving passwords. While most of these tools are very user-friendly, very intuitive, and very secure, they do lack one very important aspect: Accessibility. All of these tools store the passwords, in an encrypted file on the disk of the local machine.

While there exists a plethora of similar solutions, I will focus on KeePass for this section.P

KeePass' organisational options are brilliant. Its tree structure, enables you to easily organise your passwords.While one could argue, that this is "enough", we also have to face that we live in the age of electronics. Almost everybody has at least *two* devices, both of which would need access to passwords. Hence, KeePass and the like suffer from the fact, that you would need a 3rd party way to distribute these files. One option to this is Dropbox. But again: This just destroys the user-friendliness of the workflow.

KeePass uses AES-256, compressed with GZIp

3 Rattic

Rattic is almost what a good password manager should be: Simple, lightweight, and easy to use. That is, except that it is obviously aimed at teams. The most apparent indicator of this, is the fact that a newly created password needs to be assigned to a "Group". This would be fine, had Rattic taken a hint from Unix, creating a personal group for each user. But alas, no. You'd need to manually create a new group, for each user, to be able to store private passwords in Rattic.

Additionally, Rattic suffers from lack of a tree stucture. You have *two* options of sorting passwords: Groups and tags. Neither of which is presented in a manner, that gives a quick overview of the contents of the databse, or allows for more than a single level of hierarchy. Supports export in KeePass format.

While this software could essentially suffice, in order to meet the requirements, it would be lacking heavily in the user experience department.

4 LastPass

The infamous LastPass was the cause of a major scandal, in June 2015 [1], where they discovered, that users – granted salted and encrypted – passwords could have been leaked. Post this event, a lot of professionals lost trust in their services.

Generally, LastPass offers *great* usability. Their user experience is unparalleled, with browser integration making it a joy to use. However, you *do* need to store your password on their servers. While LastPass only encrypts and decrypts locally [2], on the user's machine, it is *still* storing sensitive data, on someone else's machine.

LastPass employs AES-256 as encryption algorithm.

5 Encryptr

Encryptr is a very interesting piece of software. Developed by SpiderOak, it offers zero-knowledge encrypted password storage, using the Crypton backend. However, per default it uses SpiderOaks servers, running Crypton. This puts Encryptr basically in the same overall category as LastPass: You need to trust someone else with your sensitive information.

Luckily, you *can* run the Crypton backend at home. Unfortunately, getting this Crypton to work is not as straight forward as one could've hoped. Ontop of

[1] https://blog.lastpass.com/2015/06/lastpass-security-notice.html/
[2] https://lastpass.com/whylastpass_technology.php

that, getting Encryptr to work with your own Crypton server, requires editing code, to change the target server. Hence, for this purpose Encryptr is *very* bad, when it comes to usability.

6 Vault

ZOHO's Vault software is yet another piece of software that falls under the same category as LastPass: You upload your passwords to their servers. While they – much like LastPass – have a delightful UI and good user experience, it is *still* hosted on a machine, someone else hosts.

7 VAULT (vaultproject.io)

Vault markets itself as a tool for "securely accessing secrets". This tool differs greatly from the previously covered. Vault is *only* a CLI / HTTP API tool. There is no graphical interface as such.

8 TeamPasswordManager

TeamPasswordManager aims itself at – as the name implies – teams, much like Rattic. This choice, is very apparent in the work flow. For instance, a password is tied to a "project", instead of a user. Security wise, TeamPasswordManager dons some impressive features. Using the standard AES-256, with the twist of a Bcrypt approach, and two-factor authentication.

While this software could essentially suffice, in order to meet the requirements, it would be lacking heavily in the user experience department.

9 Secret Server Express

Thycotic's Secret Server Express is yet another one of those pieces of software, clearly aimed at the Enterprise. Their feature list is surely impressive, but most of them are clearly aimed at larger corporations.

Giving no demo or screenshots of the software they're selling, it is impossible to determine the user experience of the software, however I would go as far as to wager, that it would be very focussed on enterprise workflows.

10 Simple Safe

Simple Safe markets itself at teams, which is not necessarily evident at a first glance. However, based on their own user experience – and poor description – it appears that all users have access to all passwords. This results in, that a single user can not have a private password, for their use only.

As seen before, Simple Safe allows passwords to be organised in "groups", much like Rattic. When you switch between groups, it is very "clonky", with a grey'ed over screen, showing it's loading – and it takes a while. From a user experience point of view, their solution is less than optimal.

From a encryption perspective, there isn't a lot to be told. Their rather vague description of their software, only states that they use 256 bit encryption [3], omitting their algorithm choice.

11 PassWork

Yet another solution, that markets itself at the enterprise, and has password data stored on a remote server. Same comments goes for this, as for LastPass, Vault (ZOHO), and Secret Server Express.

Their user experience seems fine, and at first glance they – per default – have created a private group for each user, to store private passwords in.

12 Simple Vault

While Simple Vault is *clearly* not aimed at enterprise use and is actually self-hosted, it does come with a bunch of downsides. First of all, it does not appear that it has the possibility for several users. Secondly, there is absolutely *no* organisation: Passwords are stored single level, sorted lexicographical. Each individual password, can be protected by a passphrase, "sort of" enabling multi-user access. However, other users will be able to see the password exists for a given website, which can be considered unfortunate.

User experience wise, it is horrible. The design and colours are a pain to work with, the position of buttons and menus are not intuitive. Not to sound too harsh, but the design looks like it was made by a 7th grader: It does *not* inspire confidence, in the developers ability to sufficiently protect my data.s

13 PasswordState

While PasswordState does market itself at enterprise customers, they offer a free version of their software, for teams of up to five people. Their UI is wonderful, if you are a tech geek and/or love graphs. It is very advanced since you're immediately presented with a lot of information, leading to believe it would easy scare off not-so-super-users.

Sporting a tree level structure, PasswordState manages to create the organisation there have been lacking from the previously examined tools.

Unfortunately, PasswordState is limited to the Windows platform, making it less than optimal for the purposes of this project. It would render it unable to be executed, from a Raspberry Pi, for instance.

[3] https://www.simplesafe.net/faqs/