Topic: Password Manager *Author:* Christian Robles *Date*:January 28, 2022

Problem Background

Privacy and security is something really important, most of the things this days ask you for personal information to fill in. At the same time they ask you for some kind authentication factors, like a password for instance, to keep everything private and ensure that you are the only one that can access it. The reality is that with the advancements of technology, keeping things private is become harder. People has so many accounts nowadays that they tend to use similar or the same passwords for securing their accounts, also they make them easy-to-remember, which most of the times means shorter, which at the same time means easier to guess by people who aren't supposed to. This is a problem because it absolutely violates the privacy of the account's owner. On the other hand, there is people who have a different password for each account, some of them probably even make them hard-to-guess. This time the problem isn't that privacy will be compromised, neither will security, but there is a high probability that some of them, if not most of them, will be forgotten with the pass of time, which might result in lost of information or having to go through the tedious process of reseting it.

According to IdentityForce: "In 2019, 14.4 million consumers became victims of identity fraud — that's about 1 in 15 people", "One in five victims of identity theft have experienced it more than once", and many other stats.

IdentityForce's Article - https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics

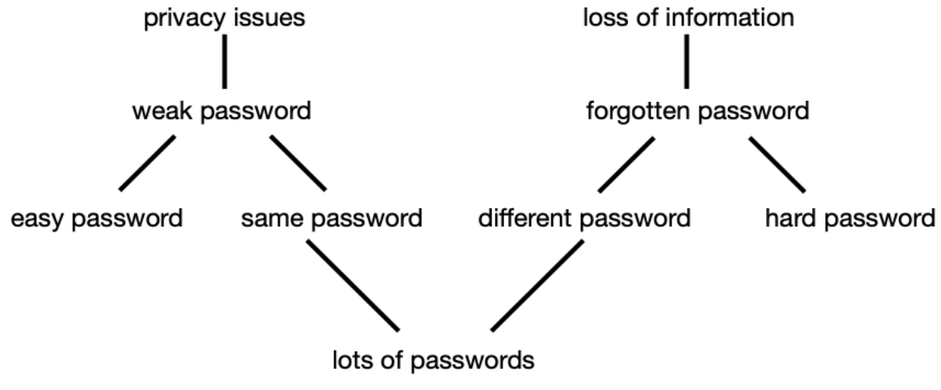
Countermeasures

Cause	Countermeasures	Why
weak password	- analysis of vulnerabilities - random password generator - two-factor authentication	By implementing these measures the complexity of accessing the information increases significantly.
forgotten password	- passwords will be stored	If passwords are forgotten, they can be recovered, no need to loss data or reset password.
lots of passwords	- all passwords will be stored in the same place - one global-unique password	there will be no need to memorize any password, but the global-unique one.

Target

Improve the privacy and security of all the people that have shared some kind of personal or private information with other services, or any other information that they want to keep private. Give them a more reliable, practical and safer way of accessing, managing, and controlling their information.

Causes



Check/Evaluate

- - Searching for vulnerabilities, creating a random password and/or adding a two-factor authentication increases the security of the information, and improves the reliability of the passwords.
- - Passwords are securely stored and well protected, granting access just to the owner.
- - No privacy violation or loss of information. Everything will be secured effectively, and will relieve the owner of the burden of memorizing every password.
- - If countermeasures doesn't work other types of security methods must evolve immediately so that a security improvement is guaranteed at all time.

Act/Standardize

If there is some kind of security vulnerability detected, the owner would be notified and recommended to change it. Other kinds of suggestions will also be able, so that the constant security of the information is ensured always.