

Problem Solving (A3) Report

Christian Robles - January 20,2021 - Virtual Safe / Password Manager

Identify the Problem

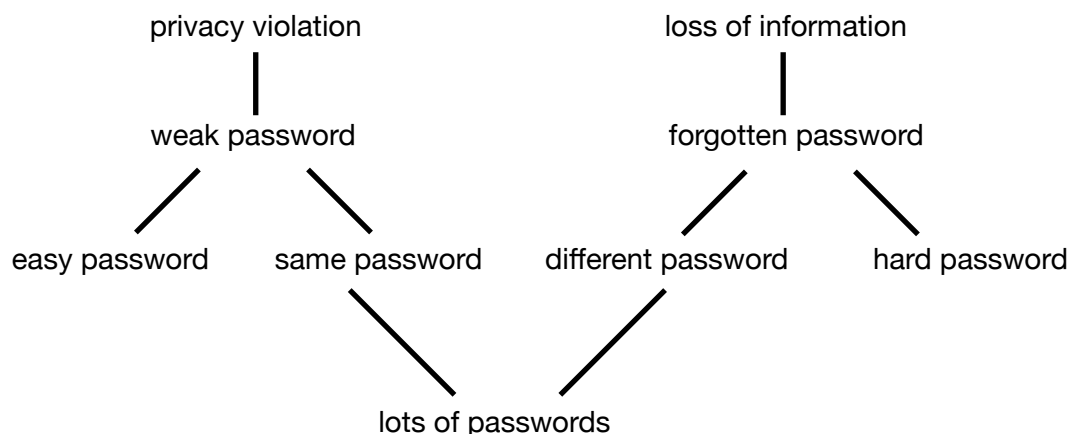
Privacy and security is something really important, most of the things this days ask you for personal information. At the same time they ask you for some kind authentication factors, like a password for instance, to keep everything private and ensure that you are the only one that can access it. The 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 make them also hard-to-guess. This time the problem isn't that privacy will be compromise, 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.

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.

Set the 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 information at all that they want to keep private. Give them a more reliable, practical and safer way of accessing, managing, and controlling their information.

Analyze the Causes



Purpose and Implement Countermeasures

| Cause | Countermeasures | Why |
|--------------------|--|---|
| weak password | use a password generator to create a random hard guess password add two-factor authentication | By implementing one or both of this measures the complexity of accessing the information increases significantly. |
| forgotten password | passwords will be securely saved | If passwords are forgotten, they can be recovered easily |
| lots of passwords | passwords will be all kept in some sort of virtual safe, protected by a global-unique password | there will be no need to memorize every password because they will be all secured in the same place. |

Check/Evaluate

- Creating a random password or adding a two-factor authentication increases the security of the information.
- Passwords are securely saved and protected, granting access just to the owner.
- No privacy violation or loss of information. Everything will be secured effectively, and will make relieve the owner of the burden of memorizing every password.
- If countermeasures doesn't work other types of security methods must evolve so that a security improvement is guaranteed.

Act and/or Standardize

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