3XA3 Problem Statement

Group 20 (2020Vision)
Mullen, Thomas - mullentc
Pavlich, Phillip - pavlicpm
Bauer, Ivan - bauerim
L02

The average person uses multiple passwords to access a wide range of services on a day-to-day basis. In order to be secure, these passwords must be difficult to guess. If they are easy to guess, unauthorized users may be able to obtain sensitive information or execute dangerous actions. Password security is achieved by making passwords long and highly unpredictable. Unfortunately, these requirements can make it difficult for users to remember multiple passwords. In response to this, users tend to use weak passwords, the same password across multiple services, or store their passwords in insecure locations (ie sticky notes).

One method of dealing with this problem, is to store multiple passwords in a secure database (a ”key-store”) that is accessed through a single ”master password”. This is often called a ”password manager”. The master password is not submitted to any service, but instead is used to decrypt the other passwords. This allows large, complex passwords to be used without the user needing to remember them. Although an encrypted key-store can work for most situations, if the system containing the key-store becomes compromised by an attacker, it may be possible to guess the master password and obtain all passwords contained within, compromising a large number of services.

There is an alternative method that avoids storing any data and instead generates passwords from the master password when they are required. This prevents the key-store from being compromised by avoiding any key-store at all. However, it opens a new vulnerability by allowing the master password to be determined from the generated passwords that are submitted to the service. This method shifts the security requirement from the local system to the remote service.

In conclusion, it is clear that both approaches to this common problem have vulnerabilities and a more secure solution is required. Our stakeholders consist of every user that logs into a service with a password, the owners of these services, and people who rely on the integrity of these services on a day-to-day basis. These services exist in nearly every environment, especially web-based environments.

Our goal is to develop a system that will manage passwords, increase the password strength, and avoid the known vulnerabilities that are within existing software.