SE 3XA3: Problem Statement
PasswordProtectionProgram

Team 28, Tuples1
Suhavi Sandhu, sandhs11
Shabana Dhayananth, dhayanas
Joseph Lu, luy89

September 25, 2017

What is the problem?

Online security is becoming more relevant than ever. Strong passwords are often easy to forget and therefore, it is much easier to opt for weaker passwords usually containing simple word or number combinations. The problem that we are trying to solve pertains to the difficulty people have with deciding on, remembering and storing their passwords. Furthermore, users have a tendency to use duplicate passwords for different services and the same password for years, according to a survey conducted by TeleSign, a mobile identity company[1]. This makes them more susceptible to security threats. Overall, the biggest issue with online security is human fallibility.

Why is this problem important?

We are in an age where almost all services provided to consumers, including banking, health records and social media, have a website or app that requires the creation of a password protected account. Many of these accounts store sensitive personal information that if compromised, could lead to identity theft, and risk other individuals associated with the account (for example the victims email contacts). According to a guide released by The Office of the Privacy Commissioner of Canada, in order to safeguard information online, it is best to create unique, strong passwords and change them often[2]. However, most people do not do this as it is difficult to keep track of updating passwords and remembering the new ones. We hope to facilitate this issue by creating a

[1]Password Statistics: The Bad, the Worse and the Ugly (Infographic), Carly Okyle, 2015, https://www.entrepreneur.com/article/246902

[2]Identity Theft and You, Public Works and Government Services Canada, 2014, https://www.priv.gc.ca/media/2034/guide_idt_e.pdf

password manager where one can safely store and access all of the passwords they use while only having to remember one strongly encrypted password.

What is the context of this problem?

The stakeholders in this case are users of online services that want a place to store their passwords safely and also want a means of generating stronger passwords. The services for which the passwords are created are also affected by the problem as they have to deal with security threats and users that forget their passwords. Identity thieves play a role as they are able to breach users personal information due to weak passwords and weak encryption methods. Lastly, the development team is a stakeholder as programmers attempting to solve the problem at hand. Padlock is an open-source password management application that is available for desktop and mobile, running on Windows, Macintosh, Unix, iOS and Android environments. We will be re-implementing this application to learn more about encryption and password security, developing an offline version for desktop, suitable for Windows, Macintosh or Unix environments.

Bibliography

1. Okyle, Carly. "Password Statistics: The Bad, the Worse and the Ugly (Infographic)." Entrepreneur. June 03, 2015. Accessed September 24, 2017. https://www.entrepreneur.com/article/246902.

2. Identity Theft and You, Public Works and Government Services Canada, 2014, Accessed September 24, 2017. https://www.priv.gc.ca/media/2034/guide_idt_e.pdf