Lab – Create and Store Strong Passwords

Objectives

Understand the concepts behind a strong password.

Part 1: Explore the concepts behind creating a strong password.

Part 2: Explore the concepts behind securely storing your passwords?

- Background / Scenario

Passwords are widely used to enforce access to resources. Attackers will use many techniques to learn users' passwords and gain unauthorized access to a resource or data.

To better protect yourself, it is important to understand what makes a strong password and how to store it securely.

- Required Resources
- PC or mobile device with Internet access
- Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

- The user can easily remember the password.
- It is not trivial for any other person to guess a password.
- It is not trivial for a program to guess or discover a password.
- Must be complex, containing numbers, symbols and a mix of upper case and lower case letters.

Based on the list above, the first requirement is probably the most important because you need to be able to remember your password. For example, the password **#4ssFrX^-aartPOknx25_70!xAdk<d!** is considered a strong password because it satisfies the last three requirements, but it is very difficult to remember.

Many organizations require passwords to contain a combination of numbers, symbols, and lower and upper case letters. Passwords that conform to that policy are fine as long as they are easy for the user to remember. Below is a sample password policy set for a typical organization:

- The password must be at least 8 characters long
- The password must contain upper- and lower-case letters
- The password must contain a number
- The password must contain a non-alphanumeric character

Take a moment to analyze the characteristics of a strong password and the common password policy set shown above. Why does the policy set neglect the first two items? Explain.

It neglects the first two requirements because adding variations to the password such as mixing numbers with uppercase/lowercase letters make the password difficult to remember but also difficult to guess. If a person follows a certain set of rules in making passwords, that person will most likely reuse those rules for other passwords as well.

A good way to create strong passwords is to choose four or more random words and string them together. The password **televisionfrogbootschurch** is stronger than **J0n@than#81**. Notice that while the second password is in compliance with the policies described above, password cracker programs are very efficient at guessing that type of password. While many password policy sets will not accept the first password, **televisionfrogbootschurch**, it is much stronger than the second. It is easier for the user to remember (especially is associated with an image), it is very long and its random factor makes it hard for password crackers to guess it.

Using an online password creation tool, create passwords based on the common company password policy set described above.

1. Open a web browser and go to http://passwordsgenerator.netLinks to an external site.
2. Select the options to conform to password policy set
3. Generate the password.

Is the password generated easy to remember?

No, the password generated is not easy to remember.

Using an online password creation tool, create passwords based on random words. Notice that because the words are appended together, they are not seen as dictionary words.

1. Open a web browser and go to http://preshing.com/20110811/xkcd-password-generator/Links to an external site.
2. Generate a random word password by clicking **Generate Another!** at the top portion of the webpage.
3. Is the password generated easy to remember?

Yes, it is quite easy to remember but also very vulnerable.

- Securely Storing Passwords

If the user chooses to use a password manager, the first strong password characteristic can be dropped because the user has access to the password manager at all times. Notice that some users only trust their passwords to their own memory. Password managers, either local or remote, must have a password store, and it can be compromised.

The password manager password store must be strongly encrypted and access to it must be tightly controlled. With mobile phone apps and web interfaces, cloud-based password managers provide anytime, uninterrupted access to its users.

A popular password manager is Last Pass.

Create a trial Lastpass account:

1. Open a web browser and go to https://lastpass.com/Links to an external site.
2. Click **Start Trial** to create a trial account.
3. Fill out the fields, as instructed.
4. Set a master password. This password gives you access to your LastPass
5. Download and install the LastPass' client for your operating system.
6. Open the client and log in with your LastPass master password.
7. Explore LastPass password manager.

As you add passwords to Lastpass, where are the passwords stored?

My passwords are most likely stored on their company servers which is basically cloud storage.

Besides you, at least one other entity has access to your passwords. Who is that entity?

Lastpass company

While having all your passwords stored on the same place can be convenient, there are drawbacks. Can you think of any?

Since Lastpass is a company that stores passwords, then possibly they would become targets of hackers who steal information. I basically placed my risk onto the company to protect my passwords for me which can never be a complete guarantee.

- What Is a Strong Password Then?

Using on the strong password characteristics given at the beginning of this lab, choose a password that is easy to remember but hard to be guessed. Complex passwords are OK as long as it does not impact more important requirements such as the ability to easily remember it.

If a password manager is used, the need to be easily remembered can be relaxed.

Below is a quick summary:

Choose a password you can remember.

Choose a password that someone else cannot associate with you.

Choose different passwords and never use the same password for different services.

Complex passwords are OK as long as it does not become harder to remember.