Home

Home › My courses › Network Attacks: Detection, Analysis & Counter... › 17 Password And Password Managers › Lesson Proper for Week 17

# Lesson Proper for Week 17

## PASSWORDS & PASSWORD MANAGERS

A **password** is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in tandem with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website. Passwords can vary in length and can contain letters, numbers and special characters.

A **password** is sometimes called a passphrase, when the password uses more than one word, or a passcode or passkey, when the password uses only numbers, such as a personal identification number (PIN).

A **password** is a simple application of challenge-response authentication, using a verbal, written or typed code to satisfy the challenge request. The order and variety of characters are often what determines the difficulty, or security strength, of a given password. That is why security systems often require users to create passwords that use at least one capital letter, number and symbol. For a password to be an effective security mechanism, its details must be kept secret. Otherwise, unauthorized users could gain access to the files and securities one is trying to protect.

## IMPORTANCE OF PASSWORD

The true importance of an account password is to protect against unauthorised network access. The user password does not actually prevent somebody from accessing any data on the device at all (unless the password is used in conjunction with some additional protection such as encryption)

Strong passwords consist of a combination of uppercase and lowercase letters, numbers and special symbols, such as punctuation. They should be at least 12 characters long, although we'd recommend going for one that's even longer. ... The longer your password is – the better.

## GUIDELINES FOR USERS CREATING OR UPDATING PASSWORDS

1. Length: The number of characters in the password.

Make passwords at least seven (7) characters long, and remember that longer is better.

2. Width: The variety of characters used in the password.

Passwords should contain at least one uppercase letter, lowercase letter, number, and symbol.

If allowed, ASCII characters can increase the security of a password.

3. Depth: How conceptually challenging is the meaning of the password?

Do not use your company name, username, or real name in the password.

Do not use a dictionary word.

4. General Guidelines

a. Remember: The best passwords are easy to remember but hard to guess.

b. Do not increment passwords (password1, password2, password3, etc.) Each new password should be significantly different from the ones before it.

c. If you do write your passwords down, ensure that they are stored in a secured place and are destroyed as soon as possible.

d. Never share your password with anyone.

e. Use a different password for every account (and a different user name when possible).

f. Stay vigilant. If you suspect a password has been compromised, change it immediately.

g. If given the option to save a password, remember that it may pose a security threat.

5. Examples of excellent passwords:

ü J*p2ba4>H! (Joyful star played tuba for more than an hour!)

ü Fl#sw33t>OH (Florida – hashtag sweet – is greater than Ohio)

ü D0gsrm!fav (Dogs are my favourite)

ü F4NS!Nu$a (Big fans in the USA!)

## PASSWORD MANAGERS

A **password manager** is essentially an encrypted vault for storing passwords that is itself protected by a master password. In order to gain access to the passwords stored in the manager, a user has to know the master password; in many cases, a second authentication factor is required as well.

*Password vaults* can be used to simply store passwords for easy recall, but one of the best features of most password managers is their ability to generate passwords. A longer password is more secure and harder to crack, and the passwords generated by password managers are combinations of random numbers and letters that are very secure.

Another important feature of most **password managers** is the ability to automatically fill in passwords to stored sites. By using that feature you won't have to type anything but the master password, and it's also a good way to avoid having passwords stolen by keylogging malware.

***A good password manager*** will allow you to sync your data between devices so you won't have to worry about losing data stored on your desktop if you're using your smartphone.

In short, password managers should take the hassle out of your digital life by putting all your sensitive information into one secure, easy-to-access location.

*Most password managers worth using utilize AES (Advanced Encryption Standard)-256, which is generally considered one of the strongest forms of encryption available--so strong that the US government uses it to transmit top-secret information*

***AES encryption, or advanced encryption standard****, is a type of cipher that protects the transfer of data online.*

## BENEFITS OF USING A PASSWORD MANAGER

§ **You don’t have to memorize all your passwords anymore.** You only need to remember the master password that unlocks your password vault. And if you opt for a cloud-based password manager, you can access your password vault anywhere, from any device.

§ **They can auto-generate highly secure passwords for you.** Password managers will typically ask you if you’d like to use an auto-generated password whenever you create a new account with a website or application. These random passwords are long, alphanumeric, and essentially impossible to guess.

§ **They can alert you to a phishing site.** Here's a quick gloss on phishing scams. Spam emails are spoofed or faked to look like they're coming from a legitimate sender, like a friend, family member, co-worker, or organization you do business with. Links contained within the email direct to similarly spoofed malicious websites designed to harvest login credentials. If you're using a browser-based password manager, it will not auto-complete the username and password fields since it doesn't recognize the website as the one tied to the password.

§ **They can help your beneficiaries when you pass away.** This is called a digital inheritance. In the event of your death, your family or whoever you designate to administer your estate will gain access to your password vault.

§ **Password managers save time.** Beyond just storing passwords for you, many password managers also auto-fill credentials for faster access to online accounts. In addition, some can store and auto-fill name, address, email, phone number, and credit card info. This can be a huge timesaver when shopping online, for example.

§ **Many password managers sync across different operating systems (OSes).** If you're a Windows user at work and a Mac user at home, jump on your Android Monday through Friday and turn to iOS on the weekends, you'll be able to quickly access your passwords regardless of which platform you're on. Ditto for all the most popular web browsers; i.e., Chrome, Firefox, Edge, Internet Explorer, and Safari.

§ **They help protect your identity.** In a roundabout way, passwords managers help protect against identity theft, and here's why. By using a unique password for every site, you're essentially segmenting your data across each website and application you use. If a criminal hacks one of your accounts, they won't necessarily be able to get into any of the others. It's not foolproof, but it's an additional layer of security that you'll certainly appreciate in the aftermath of a data breach.

## TYPES OF PASSWORD MANAGERS

a. **Desktop-based password managers** store your passwords locally on your device, like your laptop, in an encrypted vault. You can't access those passwords from any another device, and if you lose the device, then you lose all the passwords stored there. Locally-installed password managers are a great option for people who just don't want their data stored on someone else's network. Some locally-installed password managers strike a balance between privacy and convenience by allowing you to create multiple password vaults across your devices and sync them when you connect to the Internet.

b. **Cloud-based password managers** store your encrypted passwords on the service provider's network. The service provider is directly responsible for the security of your passwords. The primary benefit of cloud-based password managers, 1Password and LastPass being good examples, is that you can access your password vault from any device as long as you have an Internet connection. Web-based password managers can come in different forms—most commonly as a browser extension, desktop app, or mobile app.

c. **Single sign-on (SSO).** Unlike a password manager that stores unique passwords for every application you use, SSO allows you to use one password for every application. Think of SSO as your digital passport. When entering a foreign country, a passport tells the officials at customs and immigration that your country of citizenship vouches for you and that you should be allowed to enter with minimal hassle. Likewise, when using SSO to log into an application, you aren’t required to verify your identity. Instead, the SSO provider vouches for your identity. Businesses favour SSOs over password managers for a few reasons. Chiefly, SSO is a secure and convenient way for employees to access the applications they need to get their jobs done. SSOs also reduce the amount of time IT spends troubleshooting and resetting forgotten passwords.

## THE MOST WELL-KNOWN AND POPULAR PASSWORD MANAGERS

### 1. LastPass

· A robust password management tool available on most computing platforms and as a browser plugin. If installed in multiple locations it will sync, allowing for secure and easy password management.

· A digital vault where you can safely store passwords without fear of their being discovered. Plenty of people are in the bad habit of keeping a notebook in their desk drawer or sticky notes on the underside of their keyboard with passwords on them; LastPass is the cure for that incredibly dangerous practice.

All of the data you store in LastPass is encrypted using the AES-256 standard. This level of encryption is used by the US government to protect top secret information; a 2013 paper said there is no computationally feasible way to brute force crack it, and as of 2021 nothing has changed. That means your passwords are safe.

### 2. 1Password

· 1Password is a password management app that stores all your login information behind one master password. It is available for iOS, macOS, Android, and Windows.

· 1Password is an app used for managing the multitude of passwords each of us has nowadays. Put simply, it's a secure vault where you can put passwords, credit card numbers, and other sensitive personal information.

· 1Password uses a single logon for access to all stored passwords, and users can also use their fingerprints to log in on applicable devices.

Users who want to share information among family members will find 1Password particularly useful: it has a family sharing system built right in. Administrators can share select information with certain family members, enabling parents and children to access shared accounts.

### 3. Dashlane

- Dashlane, a fully-featured password manager and secure digital wallet app, helps hundreds of thousands worldwide manage and secure their digital lives. Dashlane aggregates passwords, credit cards, IDs, notes, and other important information in secure place that no one else can access, and enables automatic logins, smart autofill, and express checkouts on any website - no integration required.

**4. RoboForm**

- RoboForm is a password manager that enhances online security by using a master password to gain access to websites and apps. ... RoboForm also offers accounts for business and personal use, making it easy to manage passwords for anywhere from a single user to hundreds of users.

- RoboForm securely stores all of your passwords and logs you in with a single click (or tap). Save time entering personal and billing information with AutoFill for long web forms.

- RoboForm is a top-rated software used to store and manage your passwords and other personal information securely. It can remember your passwords, log you into websites, fill out your forms, and much more — all with the simple click of a button.

**5. Keeper**

- Keeper is a password manager application and digital vault created by Keeper Security that stores website passwords, financial information and other sensitive documents using 256-bit AES encryption, zero-knowledge architecture and two-factor authentication

- With Keeper, your passwords, logins and other personal information are saved in a private, digital vault. It is here where you can view and edit all of your website login credentials and details, as well as store important files and photos.

◀ Preliminary Activity for Week 17

Jump to...

Analysis, Application, and Exploration for Week 17 ▶

Navigation

Home
Dashboard
Site pages
My courses

- Capstone Project 1
- Network Attacks: Detection, Analysis & Counter...
  - Participants
  - General
  - 12 - Midterm Examination
  - 16 Multi-Factor Authentication (Mfa)
  - 17 Password And Password Managers
  - Preliminary Activity for Week 17
  - **Lesson Proper for Week 17**
  - Analysis, Application, and Exploration for Week 17
  - Generalization for Week 17
  - Evaluation for Week 17
  - Assignment for Week 17
- Ojt/Practicum 1
- Social And Professional Issues
- System Integration And Architecture 2

Courses

## Fair Warning

**NOTICE**: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

**PROSECUTION**: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION**: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

## Activities

- Assignments
- Forums
- Quizzes

Resources

Bestlink College of the Philippines
College Department

Powered byeLearning Commons