The role of passwords in cybersecurity

1st Lilo Zobl
Botball Team HTL Anichstraße
HTL Anichstraße
Innsbruck, Austria
lzobl@tsn.at

2nd Matteo Reiter
Botball Team HTL Anichstraße
HTL Anichstraße
Innsbruck, Austria
mareiter@tsn.at

3rd Niclas Prantl
Botball Team HTL Anichstraße
HTL Anichstraße
Innsbruck, Austria
nprantl@tsn.at

4th Lukas Krahbichler
Botball Team HTL Anichstraße
HTL Anichstraße
Innsbruck, Austria
lkrahbichler@tsn.at

***Abstract*—This document is part of the ECER 2023 conference on educational robotics. It follows the topic of cybersecurity and will focus on the role of passwords.**

I. Introduction

This paper will focus on the wide use of passwords or passphrases in IT-security. It will focus on the security aspect of passwords, especially on weak passwords due to user (human) laziness.
It will cover state of the art password technologies (2 factor authentication with passkeys) and possible future technologies. Additionally it will try to highlight alternatives for effective password management and introduce a choice of selected password managing software.
Finally the paper includes a best practice guide to:

- check if user's passwords have already been breached
- create an easy to remember but secure master password for a password managing software

II. State of the art

Passwords are used to protect sensitive information or access to hardware.
For example users need to key in a user-name and password before they can access any network device over SSH. This is also the case if a client wants to access the Raspberry Pi inside the Wombat controller remotely.

A. The problem with passwords

[1] [2] As mentioned above a password protects sensitive information or access to hardware like a robot. That's why it's so important to have a good, secure password. However users often are too lazy to create a strong password for every account they own. This is understandable, because as a study from NordPass shows, the average user has around a 100 accounts that require a unique password. Remembering a hundred unique passwords or more is really beyond a users capability.
Yes, the main problem is laziness but there are many other reasons why users tend to create weak passphrases.
Every year long records gets published by different providers revealing the most used passwords. Here are the top ten used passwords of last year: [3]

1) 123456
2) 123456789
3) qwerty
4) password
5) 12345
6) 12345678
7) 111111
8) 1234567
9) 123123
10) 1234567890

Other common password are locations, names, birthdays, etc.

B. Current state of art

[4]In recent years there was a massive increase in cyber-crime. To prevent data-leaks, companies started integrating 2-factor-authentication.
2-factor-authentication adds an extra layer of security to passwords. First the user has to key in the username and password, which is the same as always. Then the user has to answer an additional question to verify it's really him/her.
The second factor has different types of categories:

- **Something the user knows.** This might be a personal question the user had to configure beforehand, a personal identification number (PIN), ect.
- **Something the user has.** This could be a small hardware token or smart-phone.
- **Something unique to the user.** This might be a biometric pattern like a fingerprint, an iris scan, or a voice print.

A common type of the 2-factor-authentication is the SMS Text-Message. After entering the password and user-name the user receives a unique one time passcode (OTP) via text message. They need to key in the passcode during a limited time (for example one minute). After both the first factor and second factor are correct the user gains access.

C. Future state of art

[5] In the future passwords will likely be replaced by passkeys because they are easier to use, securer, faster and work on almost every device.
A passkey is similar to the 2-factor-authentication but without the first factor. The second and only factor is the users device's security method such as a pin or a biometric sensor (fingerprint, face scan).
The passkey is hardware specific, which means the user always needs to carry the device (that the passkey is installed on) with them. If the user wants to use passkey on their laptop they need to verify their identity with their smartphone. This eliminates phishing, credential stuffing and other remote attacks.
In conclusion when a user is asked to sign-in to an app or website, he/she approves the sign-in with the same biometric or PIN that he/she uses to unlock the device (phone, computer or security key). The app or website can use this mechanism instead of the traditional (and insecure) username and password.

D. Solutions to password managing

If users don't want to or can't use passkeys there are different options how they could protect their sensitive information. Users can write their passwords with account info into a booklet. The passwords would be unique and strong. It's a really simple idea but also has a lot of drawbacks. For example:

- Users need to carry the booklet with them everywhere. If not they can't always access their accounts.
- Users can lose the booklet. If that happens they can't access any of their accounts any more.
- It's not a really clear way of organizing passwords. Once something is written down user can't change the position in the booklet. So users would have to search for each password for indefinite time before they find it.

The other and better option is a password safe.

E. Password Safe

1) Explanation: A password safe allows you to save a list of your user-names and passwords for all your accounts. It has one master password or passphrase that unlocks the safe. Now users only have to recall one single master passphrase instead of a huge amount of passwords.

2) Examples:

- **KeepassXC** [6]

Fig. 1: KeePassXC Logo

This software is developed for users with extremely high demands of secure personal data management.
KeePassXC uses Advanced Encryption Standard (AES) encryption algorithm with a 256-bit key to secure the password database.
The biggest difference to other password safes is that the data (password, account information and additional data such as URLs, attachments and notes) is stored in an offline, encrypted file that can be stored locally. This prevents user's data from getting leaked when a server gets hacked or breached.
The XC stands for Cross-Plattform. It is possible to use it on Linux, Windows, macOS and Android.
The program is customizable. It allows the user to customize literally everything to their needs.

- **1Password** [7]

Fig. 2: 1Password Logo

This password safe is known for its easy to use interface and high security encryption.
1Password uses an uncommon encryption known as dual-key encryption. If the server gets breached it's impossible for the hacker to decrypt the user's sensitive information because of its two keys. The first key is the user's master-key. The second key is a secret key, which is a 128-bit, machine-generated code. The secret key is generated on every device the user logs into. It will only be saved on the user's devices and never saved together with the other pins.
Depending on what account type users choose their data is stored differently. However in only one version users have the option to save their data locally. In every other option the user's data gets saved in a cloud-based vault.
The interface is very user-friendly. It even generates strong passwords for accounts that are newly created.

3) Benefits and drawbacks of password safe software: [8]

Benefits:

- **Security:** Password safes use advanced encryption algorithms to protect the user's passwords. This makes it extremely difficult for hackers to steal the passwords and gain access to the user's online accounts.
- **Convenience:** Password safes store all of the user's passwords in one place, which makes it easy for them to access their accounts without having to remember

multiple passwords.

- **Auto-fill feature:** Many password safes have an auto-fill feature that automatically enters the user-name and password for the user, saving them time and reducing the risk of typing errors.
- **Multi-device access:** Many password safes allow user to access their passwords from multiple devices, including smartphones, tablets, and computers.
- **Password strength:** Password safes often include a password generator feature, which creates strong passwords. This helps to ensure that the passwords are not easily guessable.

Drawbacks:

- **Single point of failure:** If a user's password safe is hacked or compromised, all of their passwords are at risk. It is important to choose a password safe that has a strong encryption algorithm and to use a strong master password.
- **Dependency:** Using a password safe can make a user dependent on it for remembering passwords, which may make it difficult to remember passwords if a user is not able to access their password safe for some reason.
- **Learning curve:** Some password safes have a steep learning curve, and it can take some time to get used to using them effectively.
- **Cost:** Some password safes charge a fee for their services, which can be a disadvantage if user are looking for a free solution.
- **Compatibility:** Some password safes may not be compatible with all websites or devices, which can limit their usefulness.

III. Concept and implementation for best practise

It can be very overwhelming to start with a secure option to manage passwords. So here is a best practise guide everyone can follow.

1) First you should check if your password has already been breached. There is a website that let's you easily check just that. It's called **"haveibeenpwned.com"**. Haveibeenpwned is open source and secure. If someone searches for a breach it doesn't store the data that was typed in (an email address or phone number). It only ever retrieves the data from storage then returns it.

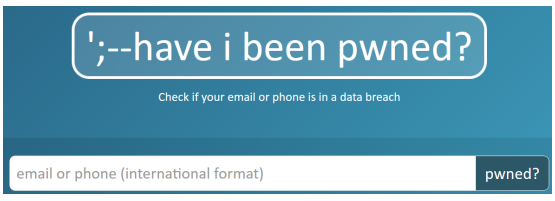

Fig. 3: Have I been pwned? Homepage

If you have already been pawned, change that password. If not you can rest assured.

2) Pick a password safe that fits best for your needs. You can choose one of the ones mentioned above or do your own research.
3) Create a good master password or even better a master passphrase. Here is a easy way to do it:
   - First think of something which is easy to remember. For example "I love apples and bananas" or "Ich komme aus der Stadt Wien" if you want to use your native language.
   - The second step is to transform the sentence in dialect or slang form. For example "I luv appls and bananas" or "I komm aus da Stadt Wien".
   - Third, you can change letters into numbers and remove spaces. A "s" gets changes into a "5", an "e" gets changed into a "3" and an "o" gets changed into a "0". For example "Iluvappl5andbanana5" or "Ik0mmau5da5tadtWi3n".
   - The fourth step is to add symbols to your password. Change characters that look like a symbol into one such as "a" to "@" or "s" to "?". For example "Iluv@ppl5@ndb@n@n@5" or "Ikomm@u5d@5tadtWi3n".
   - The fifth step is to make all words start with a capital letter. This is only needed if the language you choose does not have a grammar rule for that (It's needed in English but not in German for example).

   In the end you would end up with a passphrase like "ILuv@ppl5@ndB@n@n@5" or "Ikomm@u5d@5tadtWi3n". This is a really secure passphrase because it has numbers, upper case and lower case letters, symbols and more that 8 characters. This would make a strong master password that is nearly impossible to crack.

IV. Conclusion

Passwords remain a widely used and convenient method of authentication, but they have significant weaknesses that make them vulnerable to attacks. While there are emerging alternatives to passwords, such as biometric authentication and passkeys, there are also challenges associated with their adoption, such as cost, compatibility, and user experience.
As the cybersecurity landscape continues to evolve, it is important to explore new, innovative and especially creative approaches to authentication and access control, that are both secure and user-friendly.

List of Figures

REFERENCES

[1] Proof for Research, URL:https://tech.co/password-managers/how-many-passwords-average-person

[2] Information for "The problem with passwords", URL:https://www.nomios.com/news-blog/password-problem/

[3] List for most used passwords, URL:https://www.passwordmanager.com/most-common-passwords-latest-2022-statistics/

[4] Information for "Current state of art", URL: https://authy.com/what-is-2fa/

[5] Information for "Future state of art", URL: https://fidoalliance.org/passkeys/ https://developer.apple.com/passkeys/ https://www.passkeys.io/ https://developers.google.com/identity/passkeys?hl=de

[6] KeepassXC, Open source password manager, URL: https://keepassXC.org

[7] 1Password, Paid password manager, URL: https://1password.com/de/

[8] Information for "Benefits and drawbacks of password safe software", URL: https://expert.services/blog/managing-your-website/security/password-managers; https://www.orangecountyscu.org/stories/pros-and-cons-of-using-a-password-manager/; https://www.passwordboss.com/pros-and-cons-of-using-a-password-manager/; https://www.trustworthy.com/blog/pros-and-cons-password-manager/