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
email address or ORCID

4th Lukas
Botball Team HTL Anichstraße
HTL Anichstraße
Innsbruck, Austria
email address or ORCID

***Abstract*—This document is part of the ECER 2023 confrence 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 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 username 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

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. But that's not the only reason. A study from NordPass conducts that the average user has around a 100 accounts that require a unique password.
Yes, the main problem is laziness but there are many other reasons why users tend to create weak pins.
Every year long record gets published by different providers reviling the most used passwords. Here are the top ten used passwords of last years:

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

Also common password are locations, names, birthdays, ect.

B. Current state of art

In recent years there was a massive increase in cybercrime. To prevent data-leaks companies started integrating 2-factor-authentication.
2-factor-authentication adds an extra layer of security to your password. 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 the user is.** This might include a biometric pattern of 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 username the user receives a unique one time passcode (OTP) via text message. They need to key in the passcode in a limited time (for example a minute). After both the first factor and second factor are correct the user gains access.

C. Future state of art

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 user always need to carry the device (that the passkey is installed on) with them. If user want 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, the user approves the sign-in with the same biometric or PIN that the user has 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 user don't want or can't to use passkeys there are different options how they could protect their sensitive information. User 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:

- User need to carry the booklet with them everywhere. If not they can't always access their accounts.
- User 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 usenames linked to the associated password. It has one master password that locks the safe. Now user only have to recall one single password instead of a huge amount.

2) Examples:

- **KeepassXC**
  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 program is customizable. It allows its user to customize literally everything to their needs.

- **1Password**
  This password save 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 users sensitive information because of its two keys. The first key is the users 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 log into. It will only be saved on user's devices and never saved with the other pins.
  Depending on what account type user 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: Benefits:

- Security: Password safes use advanced encryption algorithms to protect user's passwords. This makes it extremely difficult for hackers to steal the passwords and gain access to user's online accounts.
- Convenience: Password safes store all of a 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 username and password for 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 for user. This helps to ensure that their 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.
   If you have already been pawned change that password. If not you can rest assured.
2) Pick a password safe that fits best to your needs. You can choose one of the ones mentioned above or do your own research.
3) Create a good master password. Here is a easy way to do it:
   - First make a sentence that 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 but the sentence in dialect or slang. For example "I luv appls and bananas" or "I komm aus da Stadt Wien".
   - Thirdly you can change letters into numbers. 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 fourth 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 password like "ILuv@ppl5@ndB@n@n@5" or "Ikomm@u5d@5tadtWi3n". This is a really secure password 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 as well as authentication and access control, that are both secure and user-friendly.