# The role of passwords in cybersecurity

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

***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.**

***Index Terms*—component, formatting, style, styling, insert**

## 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. 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

As mentioned earlier a password protects sensitive information that users don't want to be leaked. 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

The future of passwords is passkeys, which eliminates the need for username and password all together.

Passkeys are easier to use, securer, faster and work on most of the user's devices.

### D. Solutions to password managing

### E. Password Save

*1) Explanation:* A password save allows you to save a list of your usenames linked to the password. It has one master password that looks the save. Instead of remembering a ton of password at once users only have to recall one single pin. The rest is done by the app or rather the software.

*2) Providers:*

- **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 saves is that the data (password, account information and additional data such as URLs, attachments ans notes) is stored in an offline, encrypted file that can be stored locally. This prevents your data from getting leaked when the could gets hacked or breached.
  The program is customizable. It allows its user to customize literally everything to their needs.

- **1Passwort**
  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 you log into. It will only be saved on your devices and never saved with your other pins.
  Depending on what account type you choose your 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 creates strong passwords for accounts that are newly created.
- **Password Safe (MATESO)**

- **LastPass**

- **Dashlane**

## III. Concept and implementation for best practise

## IV. Conclusion