

openHPI course "Digital Identities
Protective measure: Secure passwords

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

Choice of "good", i.e. secure passwords (1/3)

Passwords are good when they are hard to guess or crack

Some **advice** for choosing good passwords:

- Passwords **should be case-sensitive**, even **combinations of** several words are useful.
- Password should contain **letters** as well as **numbers** and **special characters** (\$%&:;_-_?§!...)
- **Minimum length of** 12 characters
 - The longer the character length, the higher the security (because the complexity increases exponentially with each position).
- **No** passwords from the **user context** or a **dictionary**
- **No old** passwords that have been used before

Choice of "good", i.e. secure passwords (2/3)

- Choosing good passwords
 - makes brute force or dictionary attacks very time-consuming
- Secure storage
 - unattainable for data thieves
 - encrypted memory -> password manager
- Never pass on to third parties

Choice of "good", i.e. secure passwords (3/3)

Passwords should still be easy to remember ...

- so that they do not have to be written down.
- e.g. by using abbreviations

Donkey bridge:

- Difficult passwords can be remembered if you remember a complete sentence whose first letters of the word form the password, e.g:
- Where there's a will, there's a way. - **W1Wi,jdia1W.**

Use of password manager (1/3)

Problem with secure passwords

- Each account has its own secure password
- Many have >20 Internet accounts/identities
- No one can remember all passwords

A solution

- password manager
 - Service or program in which all passwords are managed/encrypted with a single, very strong password.
 - There are offline and online variants of password managers
 - A new password can be generated for each service.
 - Automatic entry of passwords on websites

Use of password manager (2/3)

Offline Password Manager

- Are basically more secure, since no third party has access to the passwords.
- Backups must be made by yourself
 - Database can be outsourced to Cloud
- The free KeePass is recommended for trying it out.



Use of password manager (3/3)

Online Password Manager

- Storage of the password database online
 - Passwords are available on all devices
 - It is uncertain whether the provider will save the clear passwords after all.

LastPass ****



iCloud Keychain



Summary: Secure Passwords

- Secure passwords...
 - ...contain upper and lower case letters, numbers and special characters.
 - ...are at least 12 characters long.
 - ...can't be found in the dictionary.
 - ...cannot be derived from the user context.
 - ...will not be reused.

- Password managers help to generate and store passwords

Summary: Secure Passwords

- Secure passwords...
 - ...contain upper and lower case letters, numbers and special characters.
 - ...are at least 12 characters long.
 - ...can't be found in the dictionary.
 - ...cannot be derived from the user context.
 - ...will not be reused.

- Password managers help to generate and store passwords