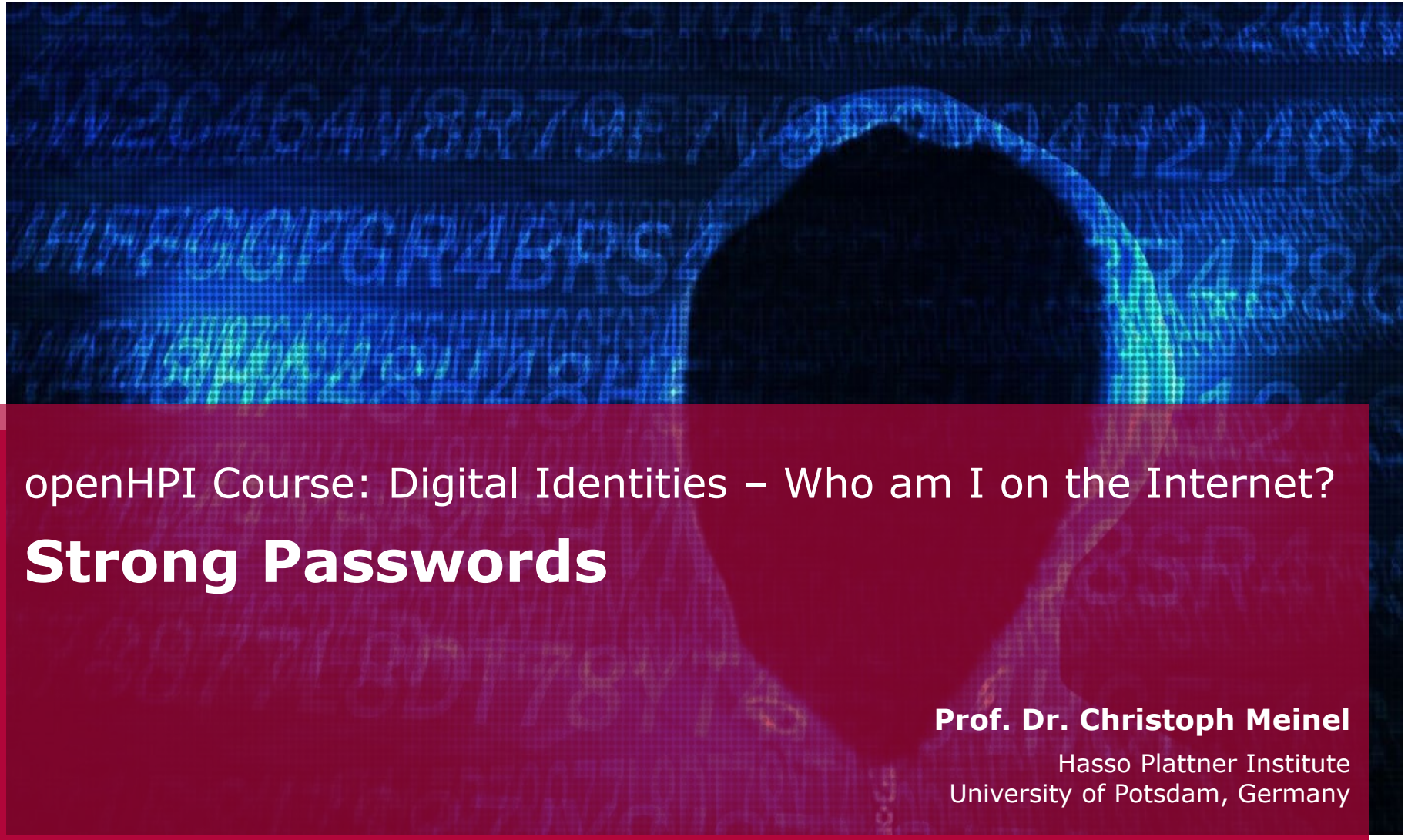


openHPI Course: Digital Identities – Who am I on the Internet?

Strong Passwords

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Strong Passwords (1/3)

Passwords are “strong" when they are complex and difficult to attack

Some advice for choosing strong passwords:

- Passwords should be **case-sensitive** and should contain both uppercase and lowercase letters
- **Combinations** of multiple words are also useful (*Passphrase*)
- In addition to letters, passwords should contain digits and special characters ($% &:; -_? §! ...)
- **Minimum length 12**
  - The longer the password length, the higher the security (because with each additional character the complexity increases exponentially)
- **No** passwords from user context or dictionary
- **No old** passwords that have already been used

Strong Passwords (2/3)

Passwords should still be **easy to remember** so that they **do not need to be written down**, e.g. use of

- **abbreviations**
- initial letters of words in a sentence

Mnemonic

- Difficult passwords can be recalled if you remember a complete sentence, the (case sensitive) initials and punctuation marks of whose words form the password, e.g.
  - Where there is a will, there will be a way. – Wti1W,tWb1W.

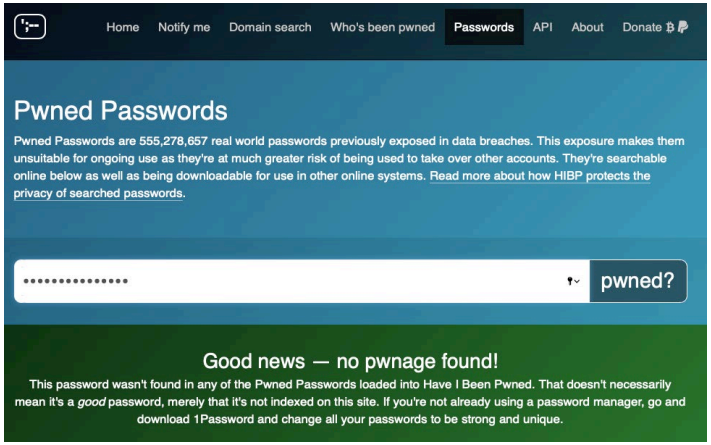
Strong Passwords (3/3)

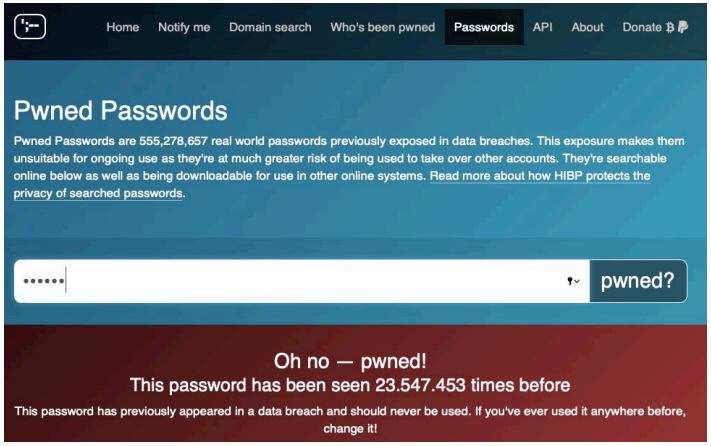
In the Internet you can find **helpful tools** to check whether a password has already been stolen

- Already stolen passwords should never be used

Example: „**Pwned Passwords**“ (= „discovered“ passwords)

- Link: https://haveibeenpwned.com/Passwords





Secure Storage of Passwords

In addition to choosing secure passwords, it is important to **store them securely**

- Never pass on passwords to third parties
- Should be unreachable for data thieves, e.g.
  - encrypted memory ➡ **password manager**

Strong Passwords
Summary

Secure passwords…

- …contain upper and lower case letters, numbers and special characters
- …are at least 12 characters long
- …cannot be found in the dictionary
- …cannot be derived from the user context
- …are not reused

Password managers help with generation and storage of passwords.