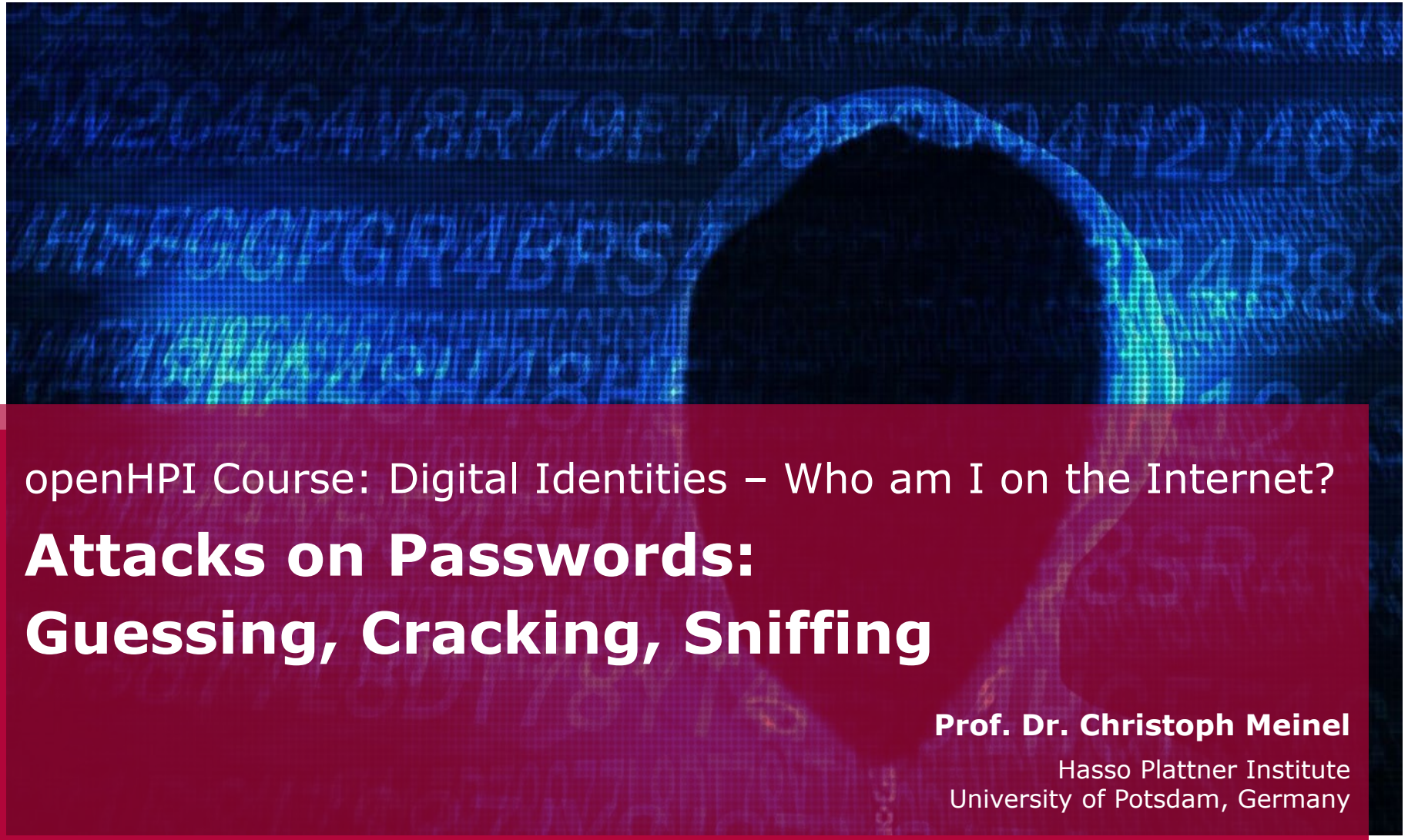

openHPI Course: Digital Identities – Who am I on the Internet?

Attacks on Passwords: Guessing, Cracking, Sniffing

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

Attacks on Passwords

Password-based authentication is often defeated by hackers with the following methods:

- **Guessing** passwords
- **Cracking** passwords
  - **systematic testing**, e.g. with word lists, password top 10 lists, ...
- **Interception** of passwords – **Password sniffing**
  - network packets are intercepted and searched for usernames and passwords
- Use of **keyloggers** and **trojans** (malware) to eavesdrop on password entry
- **Social engineering**

Password Guessing (1/3)

- Passwords are **guessed online** and used to try to get access to an Internet service
- Guessing username/password combinations is **surprisingly often successful**, because users use weak, i.e. too simple passwords

General Problem:

- Trade-off between security and usability:
  - simple passwords are easy to remember, but also easy to guess ...

Password Guessing (2/3)

Discovering a valid username

A guessed password can only be abused if the associated username is also discovered

A Username can be found by…

- Trying default usernames, e.g. admin, guest, service, ...
- Using usernames from other services, e.g. from leaked databases
- Generating usernames according to familiar patterns
  - frirst and/or last name as username
  - first and/or last name with attached numbers, e.g.
    - John64, Robert17, …
  - email addresses, ...

Password Guessing (3/3)

Discovering valid passwords

To make passwords easier to remember, many users choose simply structured passwords:

- Studies show that about 10% of all users choose their first name as a password
- Users also use unchanged default settings for username/password combinations by which systems are delivered or which are used in manuals (example: private WLAN routers), e.g.
  - *test / test, guest / guest, admin / admin*
  - hackers can easily check through lists of common combinations ...

Password Cracking (1/4)

So-called **password cracking** is executed offline on a list of hashed passwords

Aim:

- Deriving passwords in plaintext from the disguised table of hash values
- Often much faster than password guessing

Requirement:

- A disguised user file with password hashes, e.g. from
  - leaked database
  - cracked computer
  - …

Password Cracking (2/4)

Cracking is performed either with the help of
→ dictionaries or with **→ brute-force attacks**

Dictionary attack

- Lists of dictionary entries are hashed one after the other
- Hashes are compared with the hashes from the disguised password table

Brute-force attack

- One after the other password is formed from all (!) possible character combinations and then tested ...
- Brute force attacks are **definitely successful** and find the password – but if the password is long enough, it will take far too long (decades, centuries, ...)

Password Cracking (3/4)

- **Passwords cracking programs** are today very fast because they can use both the processors (CPUs) and graphics processors (GPUs) of a computer
- **Historical development:**
  - 40 years ago three passwords could be tested per second (DEC-PDP-11)
  - **today**: per second
    - almost 1 billion SHA-1 passwords can be tested on a current PC
    - almost 200 billion MD5 passwords can be tested using a GPU cluster

Password Cracking (4/4)

Recommendation:

Test your own passwords against freely available wordlists, e.g.

- https://www.openwall.com/john/
- https://www.openwall.com/wordlists/
- https://www.oxfordwordlist.com/
- https://haveibeenpwned.com/Passwords

Spying for Passwords

Small malicious programs – **keyloggers** – are secretly installed on the victim system

- Keyloggers **intercept keyboard inputs** and save them in a special file as soon as they are executed
  - recorded text is later filtered for "login ..." or "passw ..."
- Attackers can download these files from the system at a later date or automatically send them via email to the attackers server

Attacks on passwords
Summary

Attackers have developed **numerous attack methods to obtain passwords:**

- **Guessing** passwords
- **Cracking** stolen password (hashes)
- **Sniffing** - interception of network packets
- Use of **malicious software** (keyloggers, Trojans)
- **Social engineering attacks**