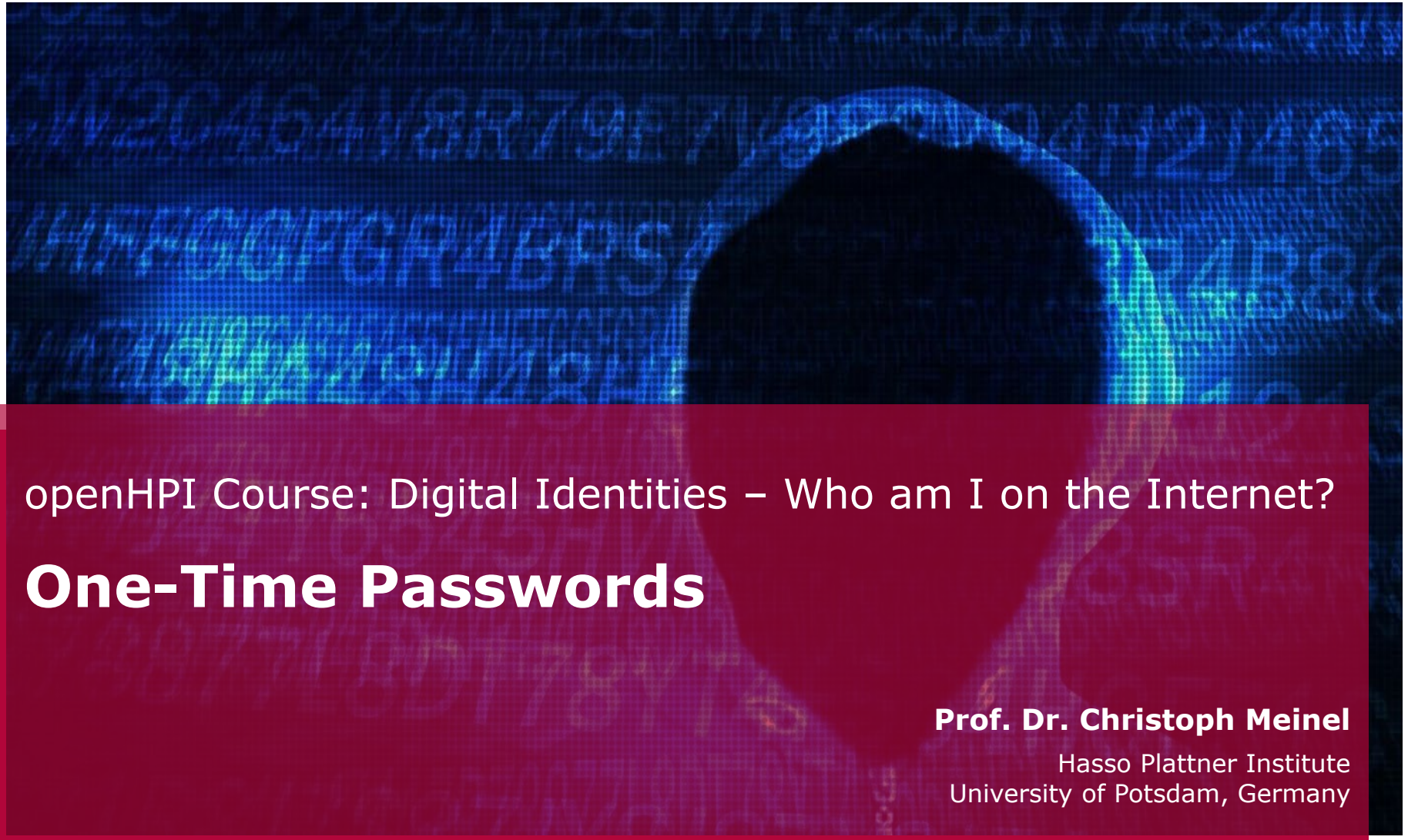

openHPI Course: Digital Identities – Who am I on the Internet?

One-Time Passwords

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

Secure Authentication With One-Time Passwords

The idea of a **one-time passwords**:

- Each password can only be used once for authentification. It loses its validity immediately after the first use
  - interception and spying is useless
- Typically, one-time passwords are **automatically** and **randomly generated character strings** that are sent to the user over a second, independent transmission channel

Provision of One-Time Passwords

Challenge

- Both user and authentication authority must know which one-time passwords are valid and which are already used

Two possible solutions

- Password lists
  - list of valid one-time passwords is generated by the authentication authority and transmitted to the user over a second secure transport route, e.g.
    - TAN lists, mTAN, ...
- Password generators
  - dynamically generate one-time passwords that are only valid for a certain time span

Password Generators ...

... are small devices – **tokens** – or applications

- Password generators produce one-time passwords by means of special algorithms
- Can distinguish three generation methods:
  - **time-controlled** generation
  - **event-driven** generation
  - **challenge-response-controlled** generation

Time-Controlled One-Time Password Generation

Token and authentication authority work synchronously

- Both sides calculate one-time passwords at the same time interval, which are valid until use or the next calculation iteration
- Authentication authority allows a time tolerance range, as the clock in the token is not always 100% accurate
- **Examples**:
  - Google Authenticator
  - SecurID

SecurID

Google Authenticator

Event-Controlled One-Time Password Generation

Generation of a one-time password is triggered by the user, e.g. by pressing a key on a token

- Token and authentication authority remember the number previously generated passwords
- Calculation of the one-time password is carried out using previously generated passwords
- Authentication authority allows tolerance range, just in case, that the user has not used a generated password

Challenge-Response-Controlled One-Time Password Generation

User wants to authenticate himself and asks the authentication authority

Procedure:

(1) Authentication authority sends a random value to the token

(2) By the calculation algorithm the token computes from the received value an outputs, the one-time password

(3) User sends the generated one-time password to authentication authority

(4) Authentication authority knows the calculation algorithm and checks the value calculated by the token

→ If correct, the user is authenticated

Authentication with One-Time Passwords
Summary

One-time passwords

- One-time passwords can only be used once
- Provision by means of password lists or password generators
- Password generators can be divided into three categories:
  - time-controlled generation
  - event-driven generation
  - Challenge-response-controlled generation