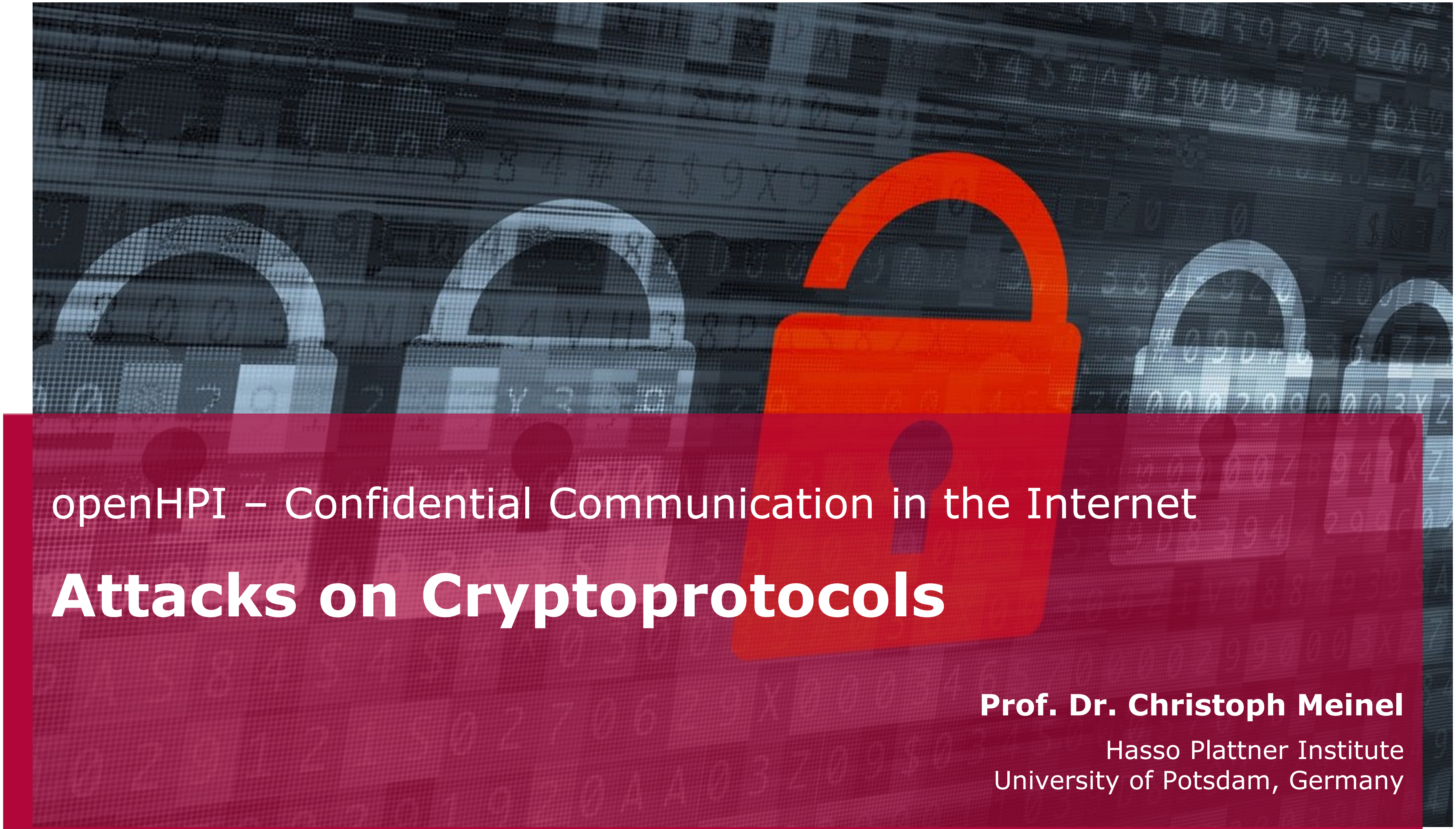


openHPI – Confidential Communication in the Internet

Attacks on Cryptoprotocols

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Attacks on Cryptoprotocols (1/4)

Attacks can focus on

- the cryptographic protocol itself
- the cryptosystem on which the crypto protocol is based
- the cryptographic algorithms used in the cryptosystem

Passive attacks:

- Participant or attacker from outside follows the protocol and tries to gain information about the participants and the communicated contents

Active attacks:

- Participant/attacker from outside tries to influence the workflow of the protocol to his/her advantage

Attacks on Cryptoprotocols (2/4)

Replay Attack

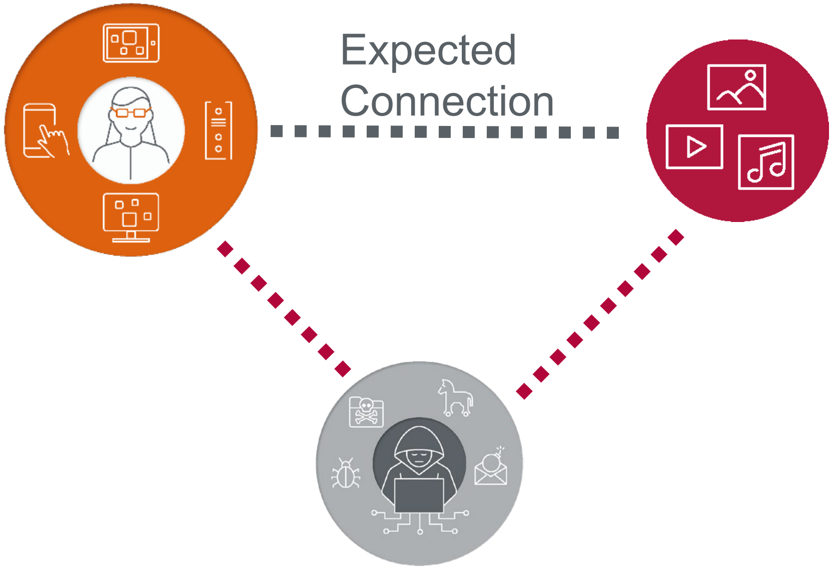
- Reuse a previously sent message, e.g. with user name and password

Spoofing attack

- Initiating a communication under a false name, e.g. use of incorrect IP address

Man-in-the-Middle Attack

- Mallory **intervenes unnoticed** by both communication partners actively in the communication and changes messages in a way that is advantageous for him



Attacks on Cryptoprotocols (3/4)

Hijacking attack

- From a certain point in time, blocking of messages from Alice to Bob
- Taking over and continuing communication with Bob
- Unnoticed to Bob that he is not longer communicating with Alice

Illegal change of state

- Mallory illegally changes state, e.g. changes state "*password not entered*" to state "*password entered and successfully checked*‟

Attacks on Cryptoprotocols (4/4)

Traffic Flow Analysis

- Collecting statistical data about all communications between Alice and Bob and analyzing these data, e.g. evaluating
  - □ which messages are encrypted and which are not,
  - □ when and to whom encrypted messages are sent
  - □ …

Denial of service attack

- Complete prevention of communication between Alice and Bob and causing a system crash by overloading their systems

Many more attacks …