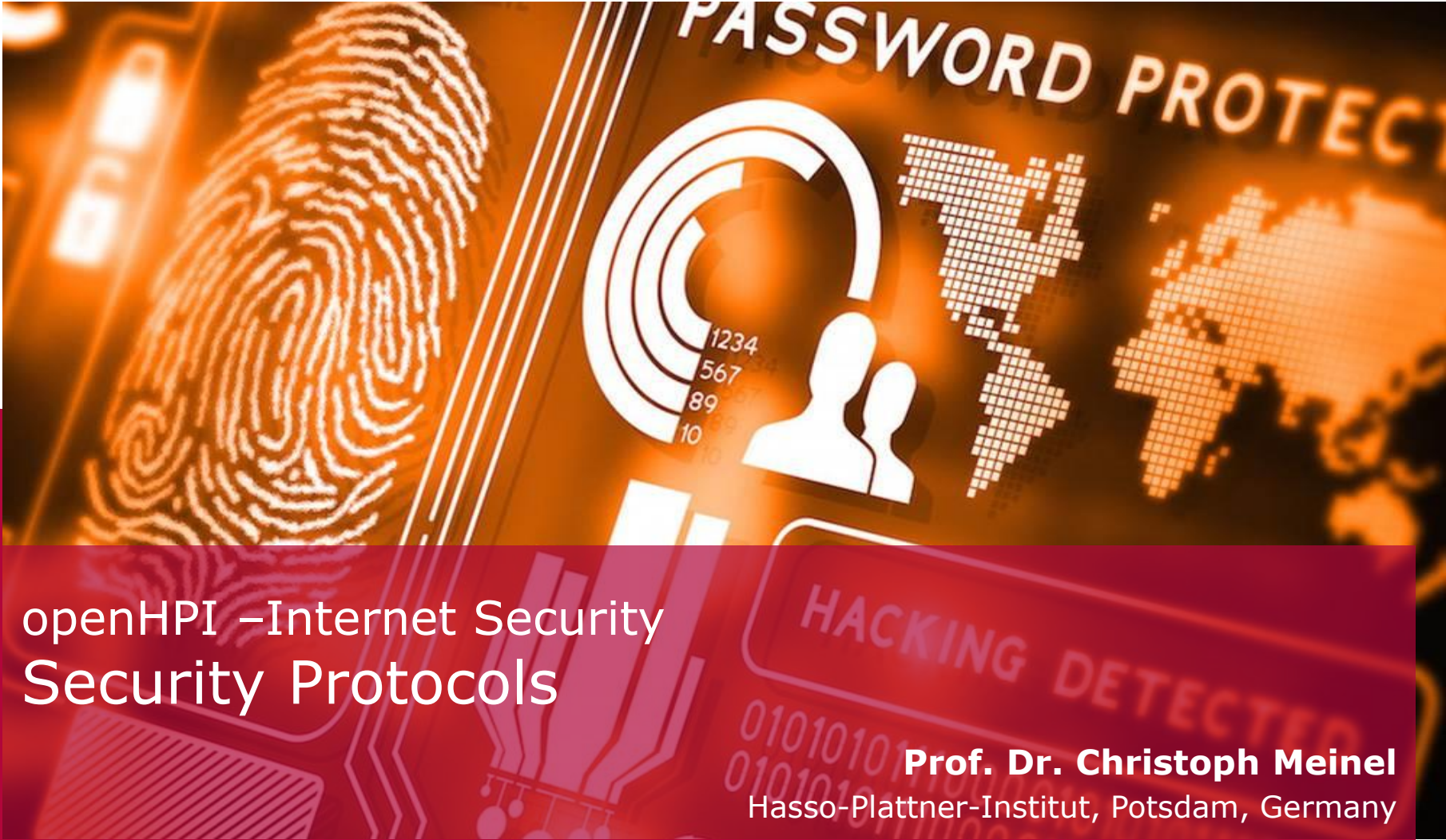




openHPI – Internet Security Security Protocols

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam, Germany

Security Protocols (1/2)

Security protocols:

- Serve the achievement/ guarantee of **security objectives**
- Provide steps that participants in a distributed information processing process must follow, **to ensure the specified security requirements**

Examples:

- Authentication methods
- Encryption, hybrid encryption
- Digital signature
- ...

Security Protocols (2/2)

Notes on the definition

- The aim of a security protocol is not to secure the process, but to ensure the prescribed safety requirements
- Unlike in the case of communication protocols, one cannot assume that security protocols are used in the correct way by all parties
 - attacks on security protocols are aimed at leveraging the security protocol, or the encryption method used by it, in order to achieve a one-sided advantage
- Therefore, one must ensure that a security protocol cannot be misused without notice ...

Security Protocols: Some Requirements

■ **Error Tolerance**

- Even with faulty usage/ user inputs, the protocol does not stop, but offers solutions

■ **Negotiating Capacity**

- Allows participants to agree on shared procedures and parameters

■ **Minimum Disclosure**

- Only the most necessary information is disclosed

■ **Perfect Forward Secrecy**

- Even if an encryption key is cracked, the entire data traffic must not be endangered. There must be no possibility of drawing conclusions from previously used session keys

Attacks on Security Protocols

Aimed mostly at

- the security protocol itself,
- on the involved encryption methods, and
- On the key(s) used
- **Passive attacks**
 - attacker follows the flow of communication and tries to gain information about its content and participants, e.g.,
 - eavesdropping, traffic flow analysis, ...
- **Active attacks**
 - attacker intervenes in the protocol and tries to change it in his favor, e.g.,
 - spoofing, injections, ...

- **Replay attack**

- recording a message and resending it

- **Spoofing attacks**

- communication activities under a false identity

- **Man-in-the-Middle attacks**

- unnoticed interposition in a communication

- **Hijacking attack**

- hijacking an already established communication link

- **Denial of Service attack – DoS**

- interfering with or preventing communication with a service

- ...

Security Protocols: Encryption

Security objective to be ensured:

Users want to ensure the confidentiality of their messages when they are transported through an open communication channel

- Users initially agree on a common encryption system
 - users must be technically capable of executing the algorithms used in the encryption system
 - users generally agree on the strongest algorithms of the encryption system that each of them can master
- Users agree on a session key

Start of the encrypted communication ...

Security Protocols: Digital Signature

Security objective to be ensured:

Ensuring the authenticity of the sender and the integrity of the messages he/she sends via an open network

- Users agree on a 2-key encryption system, procure key pairs, and ensure secure release of their public keys
- Sender "signs" messages before sending them
 - sender hashes message and created a so-called "**digital signature**" that consists of message hash encrypted with sender's private key
- Receiver can verify authenticity of the sender and the message
 - received message is hashed and digital signature is decrypted with sender's public key
 - coincidence of the generated hash and the decrypted signature proves that the message comes from the sender