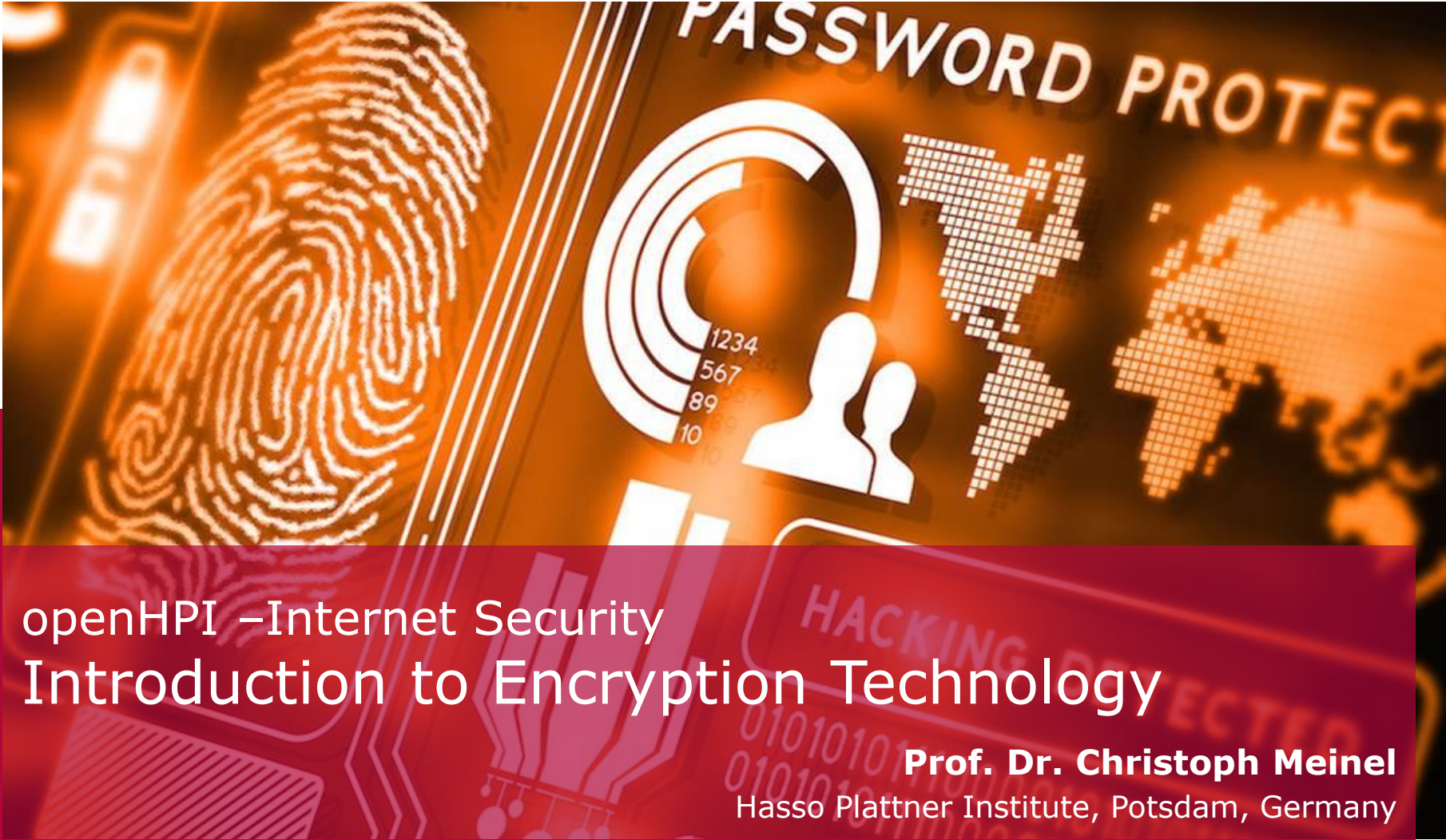




openHPI – Internet Security Introduction to Encryption Technology

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

Cryptography - the Science of Encryption (1/3)

- An effective method of protecting messages from unauthorized readers is by making them unreadable by "**encryption**"
- With encryption, a message is converted ("encrypted" or "encoded") into an illegible string by means of an encryption method, which only an authorized recipient can convert back to the original message ("decrypt" or "decode")
- Encryption and decryption methods are parameter-controlled; the parameter is called a "**key**"
- Recipients can only decrypt encrypted messages ("**ciphers**") if they have access to the decryption key that matches the encryption key ...

Cryptography - the Science of Encryption (2/3)

Cryptography is the science of **encryption**, today more commonly understood as the science of **information security**

- The quality of encryption methods depends on the extent to which it is possible to decrypt messages without authorization, i.e., without the matching decryption key
- According to the efforts that are needed to break an encryption we distinguish
 - weak cryptographic methods
 - strong cryptographic methods

Cryptanalysis is the area of cryptography that examines the quality of decryption techniques and possible attacks to break an encryption

Cryptography - the Science of Encryption (3/3)

In order to get unauthorized knowledge of an encrypted information, an attacker must

- intercept the encrypted message and then
- break the encryption, i.e. execute a (more or less) complex decryption

Always possible and not preventable are **brute force attacks**:

- an attacker tries to decrypt an encrypted information by systematically **testing all possible keys**...
- The difficulty of "cracking" an encryption is therefore dependent on the key length, as the number of possible keys is multiplied with the number of key symbols with each additional key character ...

Encryption Techniques Help to Achieve Various Security Objectives

Confidentiality:

- Only authorized persons can access information

Integrity:

- Protection from data tampering

Authenticity:

- Ensuring the origin of a message

Liability

- The originator of a message cannot deny its origin

...

Encryption Methods

Classical cryptography methods:

■ **Transposition:**

- Rearrange the letters in a word/ sentence/ text

■ **Substitution:**

- Replacing individual characters with other characters/ letters

Modern cryptography methods:

- Use of procedures at the bit level (which increases possible combinations)
- Symmetrical or 1-key methods ("secret key")
- Asymmetric or 2-key methods ("public key")