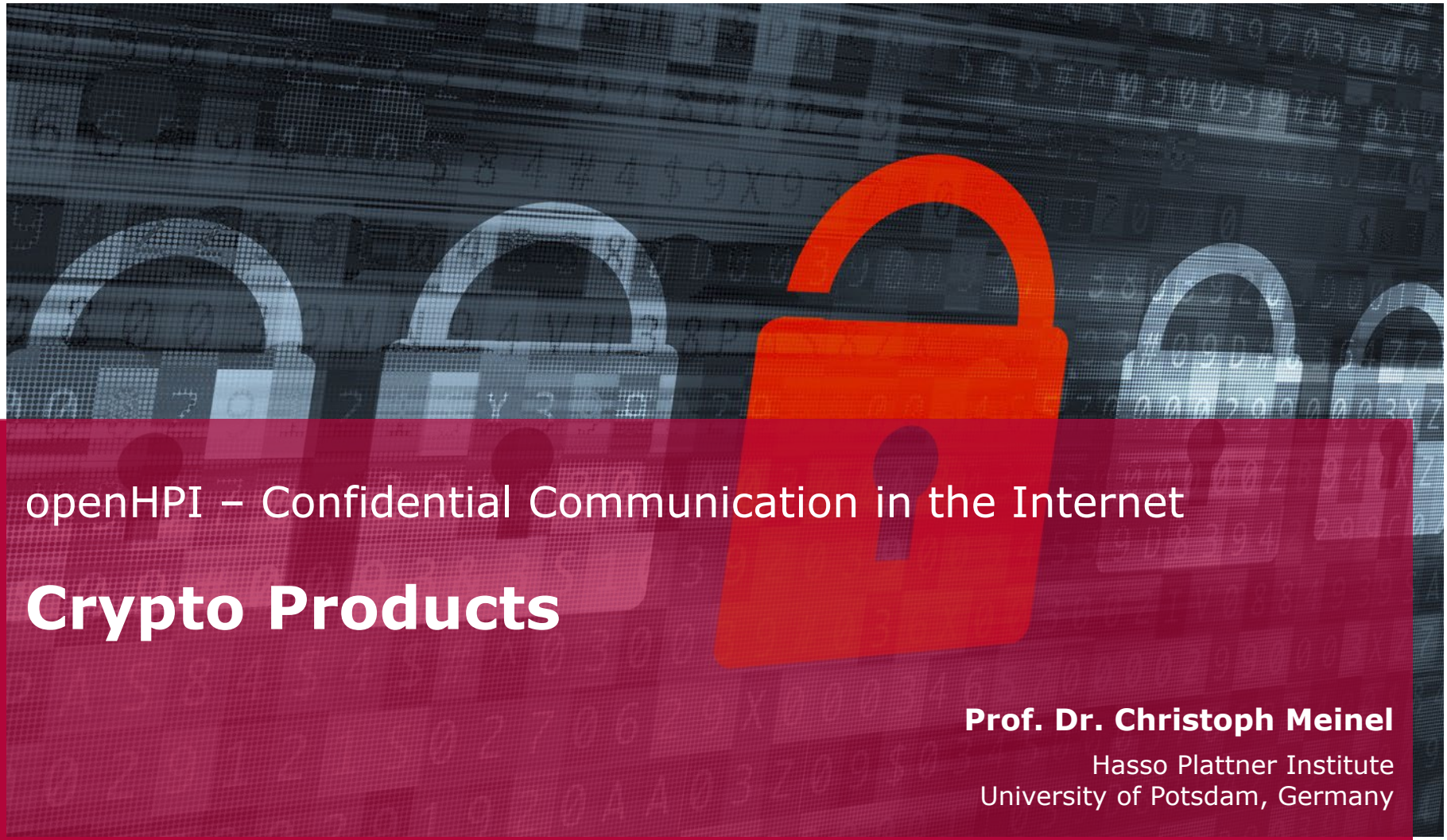

openHPI – Confidential Communication in the Internet

Crypto Products

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

Crypto Products (1/2)

We have already mentioned various **crypto products** in previous videos:

- **ENIGMA**
  - Encryption machine of the German Wehrmacht in World War II
- **Smart Token** and **SecureID**
  - Response generation hardware for Challenge-Response Protocols
- **Kerberos**
  - Key distribution system
- …

Crypto Products (2/2)

- …
- **Implementations of DES, Triple-DES, AES**
  - symmetric cryptosystems
- **Implementations of RSA**
  - asymmetric cryptosystem
- **Implementations of SHA, SHA-1, SHA-2, SHA-3, MD4, MD5**
  - cryptographic hash functions

Crypto Hardware

Crypto products are available as

- **Crypto hardware**
- **Crypto software**

Crypto hardware

- Faster than software
- **DES** and **AES** are optimized for hardware realization
- Manipulation of hardware is more difficult than software
- More difficult to analyze than software
- Secure storage of secret keys so that they cannot leave the **personal security environment**
- In personal care and disposal
- …

Crypto Software

Crypto software

- Less complex and much more flexible than hardware
- Less safe
- Slower
- Secure key storage difficult to impossible
- Availability of secret keys is much more difficult to organize than with hardware
- ...

Some Crypto Products: **SmartCards with Crypto Processors** (1/3)

SmartCard - plastic card in credit card size with embedded computer chip and crypto processors

- First patents at the end of the 60s
- In mass use since the mid 80s
  (Banks, telephone, identity card, ...)
- Input and output by means of a card reader via contact areas on the chip surface
- Excellent for cryptographic applications, e.g. for storing secret private keys, signature execution, ...

Problematic:

- Still rather slow and limited storage capacity

Some Crypto Products: **SmartCards with Crypto Processors** (2/3)

Protection of SmartCards:

- Based on the principle of “property and knowledge”
  - one owns the card
  - one knows a **secret**, e.g. **PIN**
- Based on the principle of "property and biometric"
  - one owns the card
  - one has a biometric characteristic, e.g. fingerprint to unlock / use the card

Authentication with SmartCards:

- By so-called **challenge-response procedures**, SmartCards are perfectly suited for authentication in order to gain access to PCs, computer systems, laboratories, buildings, ... **secure**

Some Crypto Products: **SmartCards with Crypto Processors** (3/3)

Usage scenarios for symmetric cryptosystems:

- Storage of a secret key on the card
- Encryption and decryption of data on the card using AES or other symmetrical method

Usage scenarios for asymmetric cryptosystems:

- Generation of the key pair on the card
- Storage of the private key on the card, so that it cannot be extracted
- Extraction of the public key from the card to publish it for communication partners
- Decryption of received ciphertext encrypted with the private key from the card
- Signing documents / messages with private key

Some Crypto Products:
HSM - Hardware Security Modules

Modern computers usually have a **Hardware security module** with integrated crypto processor

- Similar functionality to smartcards / crypto hardware:
  - Secure **storage of secret keys**, encryption of data, calculation of hash values, etc.
- Implemented as a separate chip (in addition to the main processor): **Trusted Platform Module**
- Also available in mobile devices:
  - Apple Secure Enclave
  - Titan M in Google Pixel
  - ARM TrustZone in other Android devices

Note: Proprietary implementation of crypto functions may contain **vulnerabilities**!

Some Crypto Products:
VPN - Virtual Private Networks

Company networks often consist of different local networks at different locations, connected by (expensive) rented physical communication lines

Idea of VPNs – **virtual private networks**:

- Replacement of expensive private dedicated lines by cryptographically generated **virtual data channels** on the Internet
  - Users are authenticated and all data packets are encrypted before they are send
- Securing data traffic at the Internet level, e.g. with **IPSec**
- Use of the IPSec tunnel mode, in which IP packets including IP headers are encrypted before sent

Some Crypto Products:
IBE - Identity Based Encryption

Idea:

- Asymmetric encryption with a key pair
- The public key does not have to be distributed separately, because it is the "identity" of the recipient, e.g. email address, server DNS entry, etc.

Origin:

- Proposed by Adi Shamir in 1984
- However, there has been no concrete implementation of identity-based signatures for a long time
- In 2001, first proposals were published…

But:

- With IBE there is no possibility to make keys invalid as long as the "identity" is used