openHPI – Confidential Communication in the Internet

Introduction: Confidential Communication

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

Insecure Internet, Unsafe Communication

Exemplary case: Leaks from G0d – Criminal Advent calendar

- **December 2018**: Hackers publish **confidential data of celebrities** (politicians, actors, musicians, ...) via Twitter
- Published data includes lists of mobile phone numbers and home addresses, personal address directories and email lists, Facebook chats, copies of ID cards, photos, scans, ...
- Politicians are startled: **"How could this happen?"**
- **Problem**: **No awareness** of the need for **data security as a cornerstone of** a digital society
- Politics can create framework conditions, but **each individual must inform himself and take measures himself**

Our Course wants to offers an intro into **Confidential Communication**

Insecure Internet, Unsafe Communication

Other spectacular examples: CEO Fraud

- 2018, Karlsruhe regional court: Sparkasse is liable for the transfer of ~1.7 million Euros, which an accountant has executed after a fake message from the boss

August 2016, similar incidents:

- Chinese- Austrian aircraft component manufacturer FACC AG loses 50 million euros
- Bavarian automotive supplier Leoni AG loses 40 million euros

With the use of **cryptographic means** (such cases so-called digiale signatures) could have been avoided!

Digital Transformation Characterized by the Omnipresence of the Internet and the WWW

The Internet and WWW promise ...

- Almost cost free and **worldwide communication**
- Media without borders
- All **information available everywhere** and **anytime**
- Democratic access
- ...

Internet and WWW also Offer Entrance Gates for Multiple Threats

- Faulty software or hardware
- Inadequate protocols
- Computer viruses, worms, or trojans
- Incorrect operation
- Careless users
- Unauthorized users, hackers
- Reading information / espionage
- Falsification of messages
- Misdirection of mail
- ...

→ **Threats rise the more all parts of our world are interconnected by the Internet!**

Information Transmission on the Internet is Endangered in Many Ways ...

Confidentiality of messages not secured when communicated by the Internet

- Data packages with the messages can be **manipulated** during the transport through the Internet
- Sender name and/or address can be **forged**
- Messages can contain uploaded with hidden **malware**
- ... and **much more dangers** threaten the communication in the Internet

We Need Mechanisms to Ensure Information Security and Confidentially in the Internet ...

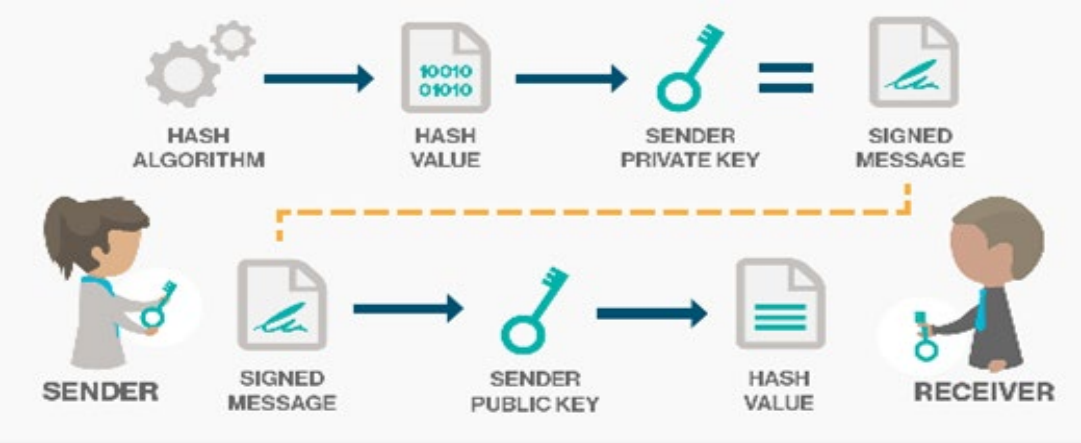
These are the **security goals** which have to achieved in the Internet:

- Ensure the **confidentiality** of messages
- **Prevent forgeries** of the sender
- **Uncover manipulation** of messages
- Prevent the denial of online orders
- ...

Cryptography is Science for Ensuring Information Security

With the help of **cryptographic methods**, one can:

- Ensure **confidentiality of messages**
- Detect forgery / manipulation of a message
- Detect forgery of the sender of a message
- Detect unfair behavior of an online purchaser
- ...



Derived from Ss_digitalsignature.png, Baskhuu1025, CC BY-SA 4.0, via Wikimedia Commons

Confidential Communication
In our openHPI course we will speak about:

Contents in course week 1 (Jan. 13th – Jan 19th 2021)**:**

- Introduction, threats, security goals …
- Symmetric and asymmetric **cryptography**
- Examples: DES, AES, hash functions, RSA, ...
- **Cryptographic** protocols & attacks

Contents in course week 2 (Jan. 20th – Jan 26th 2021)**:**

- Crypto Protocol: **Encryption**
- Crypto protocol: Digital **signatures**
- PKI and Trust Center
- Digital **certificates**
- PGP - secure Email

Confidential Communication
Some Literature

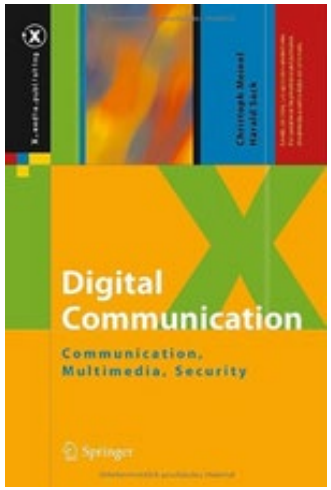
In our Springer book

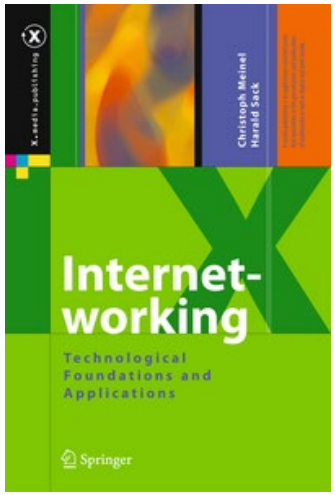
- **Meinel/Sack: "Digital Communication".**

there is plenty of material to read on and to deepen.

The volume is the first part of a trilogy

- **Meinel/Sack: "Internetworking"**
- **Meinel/Sack: "Web Technologies"**





Confidential Communication
Introduction of the Teaching Team

Prof. Dr. Christoph Meinel


- Institute Director and Dean of the Hasso Plattner Institute
- Head of the Chair "Internet Technologies and Systems"
- Research focus: Security Engineering, Learning and Knowledge Engineering, Digital Education, Innovation Research

Confidential Communication
Introduction of the Teaching Team

Daniel Köhler

- Security Engineering
- Netzwerksicherheit

Ali Alhosseini

- Social Media Analytics
- Attack Graphs