openHPI – Confidential Communication in the Internet

Trust Problem

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

Trust Problem of Asymmetric Cryptosystems (1/2)

Asymmetric cryptosystems and asymmetric procedures, such as RSA, Diffie-Hellman and DSA have revolutionized cryptography and made it suitable for the Internet

What remains is to solved the **Trust Problem** of asymmetric cryptosystems, that consists in:

Authenticity of the public keys

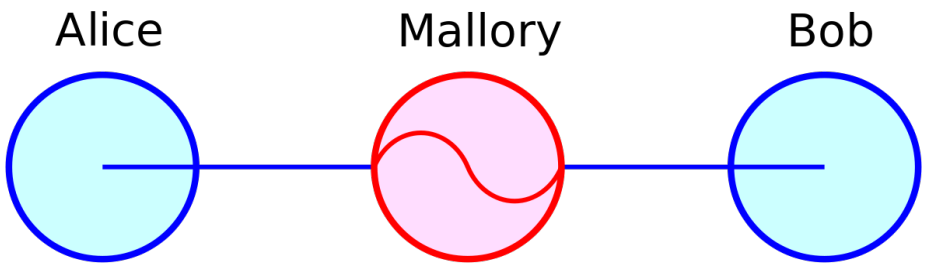
- To tamper-proofly liaise the public keys to their users, i.e. to create a trustworthy and legally secure allocation of **public keys** to **their owner**
- Otherwise Alice does not know that she is really using Bob's public key and not the public key of Mallory

Trust Problem of Asymmetric Cryptosystems (2/2)

Basic attack scenario:

Mallory tries to trick Alice into using his public key to encrypt a message for Bob instead of Bob's public key

- Mallory gives out his public key for the one from Bob
- Then Mallory can read Alice's (confidential) messages for Bob, but Bob cannot!
- Mallory can digitally sign documents in Bob's name!



Trust Problem – Other Problems that Need to be Solved (1/2)

Revocation of keys:

- If Bob's private key is compromised (Mallory has stolen it, Bob losts his SmartCard, ...), Bob needs a new pair of keys and has to replace his widely distributed old public key by the new one
- **But**: Who can help Bob to solve these problems?

Indisputable signature:

- Digital signatures are only binding if Bob cannot deny afterwards that the document was signed (encrypted) with his private key
- **But**: How one can check whether a private key belongs to certain user?

Trust Problem – Other Problems that Need to be Solved (2/2)

Enforcement of security policies:

- There must be fixed rules – **security policies –** for handling key pairs of asymmetric cryptosystems, e.g.
  - how are key pairs generated?
  - where are the public keys stored?
  - how long are the keys valid?
  - what happens if a key is compromised?
  - ...