

Information Security Security & Cryptography

Elisabeth Oswald

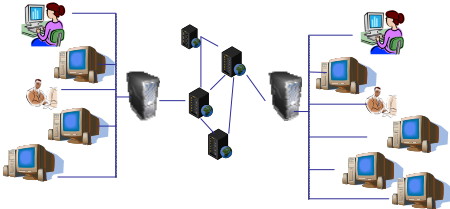
Outline

- Security concerns in a networked world
- Overview of basic cryptographic techniques
- Overview of basic vocabulary/concepts

Handouts

- Team up with your neighbours and have a look at the handout you got
 - There are different handouts each group works with one handout
- Jot down what you believe the most important security concerns are for the scenario depicted in your handout
- We'll discuss your thoughts thereafter

Handout 1: wired WAN



Handout 2: Bluetooth



Handout 3: Wireless LAN



Handout 4: Mobile Communication



Security concerns

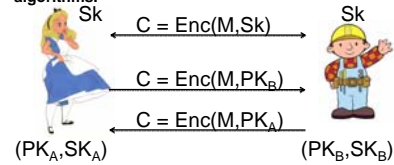
- Security of data flow
 - Confidentiality
 - Integrity
 - Authenticity
 - Of Data, but also entities
 - Non repudiation
- Security of devices/entities
 - Accessibility
 - Availability
 - Authenticity
 - Access control
 - Malware
 - Viruses
 - Trojans
 - Worms

CIA

- Confidentiality
 - Encryption
 - Public-key vs. Private-key or asymmetric vs. symmetric
- Integrity
 - Hash functions
 - Keyed vs. Unkeyed
- Authenticity
 - Data: cryptography
 - Entities: protocols
- CIA w.r.t. data connections
 - Connection conf.
 - E.g. Online banking, SSL
 - Connectionless conf.
 - E.g. . Encrypting UDP packets
 - Selective field conf.
 - E.g. Encryption of credit card number only in packet
 - TCP/IP level conf.
 - IPSEC

Confidentiality

Confidentiality of data is achieved by using encryption algorithms.



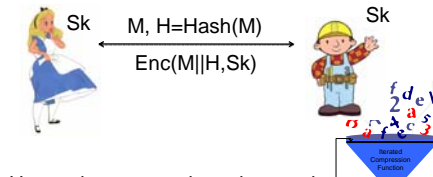
- Symmetric enc.: Alice and Bob share the same key
- Asymmetric enc.: Alice and Bob have key pairs and only share public parts of them

Confidentiality: algorithms, properties

- Symmetric encryption
 - Fast, key distribution can be a problem
 - Used to encrypt bulk messages
 - DES, AES
- Asymmetric encryption
 - Slow, key distribution can be elegant
 - Used to encrypt (symmetric) keys
 - RSA

Integrity

Integrity of data is achieved by using hash functions.



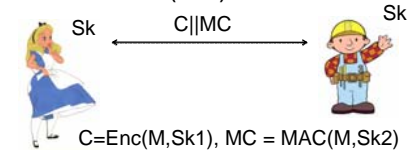
- H must be communicated securely
- H compresses message and 'mixes' bits

Integrity: algorithms, properties

- First: encryption does not provide integrity checking hence hash functions are crucial!
- Unkeyed hash functions
 - Compression + integrity check
 - MD family (broken), SHA family
- Keyed hash functions
 - Compression, integrity, authenticity
 - HMAC

Authenticity

Authenticity of data is achieved by using message authentication codes (MACs).



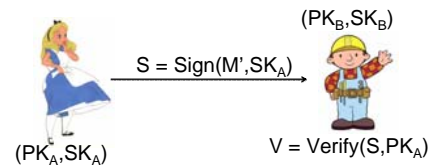
- Alice and Bob need different keys for encryption and MAC computations
- MACs can be appended to the (encrypted) message

Authenticity: algorithms, properties

- MAC
 - Keyed hash function: can only be verified by legitimate party
 - HMAC, UMAC
 - Key distribution problem
 - fast

Non repudiation

Non repudiation is achieved by using digital signatures.



- Only Alice can produce a valid signature for herself because only she has access to the secret key
- Bob can verify any signature Alice has created using her public key

Non repudiation: algorithms, properties

- Can only be achieved using asymmetric key cryptography!
 - Symmetric key cryptography is used to hash message first
- Digital signatures
 - With appendix: means S is appended to message, and verification requires S and M
 - With message recovery: means S is transmitted and allows to recover M
- RSA-PSS, DSA, ECDSA

How cryptography is often used

Cryptography is used as means to secure information AND as means to authenticate users.

- To show that we know/possess something secret:
 - Knowledge of a secret can be demonstrated by encrypting something with a symmetric key cipher or decrypting something with an asymmetric key cipher.
- Then we tie knowledge of this secret to having some access rights or being someone.

🏰 Where is security implemented

- Real world systems consist of several layers
 - Application layer
 - Service layer
 - Operating system
 - Operating system kernel
 - Hardware
- Good security comes from making use/taking into account all layers!
 - The further down the more generic and 'clear' security mechanisms are, the higher up the more user/application specific and 'fuzzy' they get

🏰 How security is defined

- If security is focused on security of data, then CIA is a good definition
- But for any more general system, one typically writes a **security policy which specifies**
 - **Threats**
 - E.g. loss of confidentiality
 - **Attacks (realisation of threat)**
 - E.g. attacker gains access to computer storing data
 - **Security mechanism**
 - E.g. encryption scheme
- How to choose mechanisms? -> Risk analysis

🏰 Summary

- Information security has cryptography as sub-field
 - Cryptography is used to secure information and authenticate users
- Terminology distinguishes between threats, attacks and mechanisms, and often elaborate security policies are written that specify how a system is protected