Distributed Systems
Security

Prof. Dr. Oliver Hahm
Frankfurt University of Applied Sciences
Faculty 2: Computer Science and Engineering
oliver.hahm@fb2.fra-uas.de
https://teaching.dahahm.de

Introduction

Information Security[1]

"Information security [. . .] is the practice of protecting information by mitigating information risks. [...] It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.".

- Separation between policy and methods
  - Security policies (Set of rules)
  - Security methods (Mechanisms for enforcement)

[1] https://en.wikipedia.org/wiki/Information_security

Introduction

Information Security[1]

"Information security [. . .] is the practice of protecting information by mitigating information risks. [...] It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.".

- Separation between policy and methods
  - Security policies (Set of rules)
  - Security methods (Mechanisms for enforcement)

[1] https://en.wikipedia.org/wiki/Information_security

Secure Systems

- . . . do not exist.
- The completely secure firewall:

http://www.brauwesen-historisch.de/seitenschneider.jpeg

Secure Systems

- . . . do not exist.
- The completely secure firewall:

http://www.brauwesen-historisch.de/seitenschneider.jpeg

- An application can be considered secure, if the cost for an attacker are higher than the value of the protected value

Protection goals

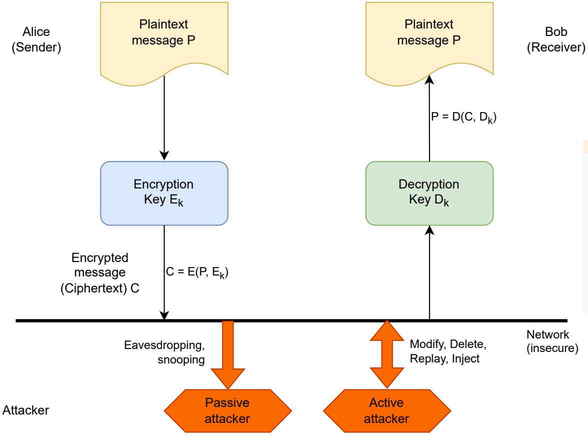
- Common protection goals (CIA triad):
  - Confidentiality:
    Information can only be accessed by authorized users
  - Integrity:
    Data must not be modified unnoticed
  - Availability:
    Data access is ensured with an agreed quality
- Further protection goals:
  - Authenticity:
    Authenticity of a person or a service is verifiable
  - Non-Repudiation:
    The author of any data must be identifiable and cannot repudiate this
  - Accountability:
    Any action can be accounted to a user
  - Privacy:
    Personal attributes must be kept confidential and the anonymity should be preserved if possible

Terms

- Authentication:
  - Verification of an identity
  - Mutual authentication of communication peers is required, e.g., user $\leftrightarrow$ computer
- Authorisation:
  - Have and exercise permissions
  - Security models
    - Discretionary Access Control
      Access matrix as abstract model
      Method: Capabilities, Access Control Lists (ACLs)
    - Mandatory Access Control

Cryptography

- Practise of techniques for secure communication
- Base model:



Cryptographic methods are based on mathematical theory, but can be applied without in-depth understanding of the mathematical foundations.

Threats

- STRIDE Model
  - **S** poofing ⇝ Authenticity
  - **T** ampering ⇝ Integrity
  - **R** epudiation ⇝ Non-repudiability
  - **I** nformation disclosure ⇝ Confidentiality
  - **D** enial of Service ⇝ Availability
  - **E** levation of Privilege ⇝ Authorization

Threat Examples

- Faulty specification of security policies
- Fault design or specification of components
- Faulty configuration
- Faulty code
- Weak cryptographic methods
- Exploiting insider information
- "‘Social Engineering"’
- Eavesdropping
- Denial-of-Service attacks
  - e.g., by generating a very high load
  - Prevention of exercising a certain right
- Theft of keys or masquerading (faking an identity)
- Active modification, deletion, or replay of messages
- Injection or infiltration of messages, emails, viruses, worms, Trojan horses ...

Risk Assessment

https://iso25000.com/images/figures/en/iso25010.png

- May conflict with other characteristics of software quality
- Effort-benefit must be weighed
- Per threat:
  - Potential damage (life and limb, property damage, reputation)
  - Probability of occurrence
  - Probability of detection of occurrence
- The higher the risk, the more important the consideration as part of the security policy

Agenda

1. Cryptographic Concepts
   - Encryption Methods
   - Cryptographic Hash Functions

2. Cryptographic Methods
   - Authentication
   - Digital Signatures
   - Key Management

Agenda

1 Cryptographic Concepts
- Encryption Methods
- Cryptographic Hash Functions

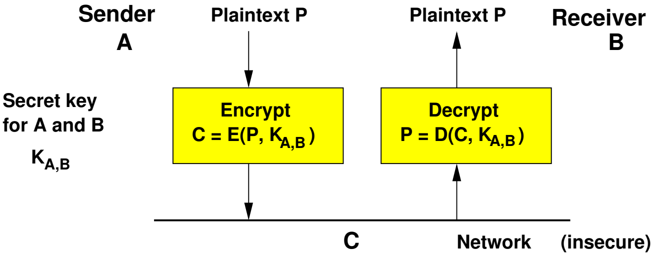
2 Cryptographic Methods
- Authentication
- Digital Signatures
- Key Management

Agenda

1. Cryptographic Concepts
   - Encryption Methods
   - Cryptographic Hash Functions
2. Cryptographic Methods
   - Authentication
   - Digital Signatures
   - Key Management

Symmetrical Encryption

- a secret key for encryption and decryption
- requires a secure channel for key distribution
- Advantages:
  - short key sizes (symmetrical keys of at least 128 bit length are considered today)
  - low computational cost (fast)
- Problems:
  - Key Management
  - Repudiable



Symmetrical Encryption

- Block algorithms
  - Encryption of data of fixed length, e.g., 64 bit
  - Alternatives:
    - Electronic Code Book
      - all blocks are encrypted independently from each other
    - Cipher Block Chaining
      - Encryption is chained with the previous encrypted block via an **XOR** operation
- Stream Algorithms
  - Bit or byte stream oriented
  - typically very fast, but missing standardization
- Examples:
  - DES Data Encryption Standard (US) historically most widespread representative
  - Triple-DES, IDEA, AES
  - RC4 (Stream Algorithm)

Asymmetric Encryption (public key encryption)

- A pair of keys is required (private and public key)
  - different keys for encryption and decryption → Hence the name "‘asymmetric"’
  - Assumption: the secret can not be derived from the public key or the method with realistic computational costs
- Advantages:
  - No secrete channel for key distribution required → the secret key gets never transmitted
  - Public keys can easily be distributed using directory services
  - Non-repudiation is possible
- Drawbacks:
  - rather long keys are required (→ currently at least 2048 bit are recommended)
  - high computational cost
  - Reliable key management is required

Examples Asymmetric Encryption

Representatives

- RSA Algorithm
  - Rivest, Shamir, Adelman: 1978
  - based on prime factorization of big numbers $\rightarrow$ computational hard one-way problem
- Diffie-Hellman
  - Establishing secure connections from an unsecure state (without authentication)
- Elliptic Curve Cryptography (ECC)
  - based on rather modern mathematical methods
  - allows smaller keys with equivalent security
  - especially suited for resource constrained devices

Typical Use Cases

- Asymmetric Encryption
  - Authentication
  - Digital signatures
  - Key management
- Symmetrical Encryption
  - fast encryption of a bigger amount of data

$\Rightarrow$ Asymmetric methods are used to negotiate keys for subsequent symmetrical encryption (Session Key)

Agenda

1. Cryptographic Concepts
   - Encryption Methods
   - Cryptographic Hash Functions
2. Cryptographic Methods
   - Authentication
   - Digital Signatures
   - Key Management

Cryptographic Hash Functions

- Calculating a digital fingerprint for documents or messages $\rightarrow$ message digest
- Basis for digital signatures
- Hash function H
  - $h = H(P)$
  - Message P of arbitrary length
  - h Sequence of bits of fixed length (e.g., 128 bit)
  - cf. CRC
- Assumptions
  - Calculation of H is easy
  - The reverse operation, i.e., determining the original message for a given hash value is computational hard ($\rightarrow$ one-way function)
  - Any change to the message P results in a different hash value (h)
- Examples:
  - MD5 (not considered secure anymore)
  - SHA-0, SHA-1, SHA-2, SHA-3

Agenda

1 Cryptographic Concepts
- Encryption Methods
- Cryptographic Hash Functions

2 Cryptographic Methods
- Authentication
- Digital Signatures
- Key Management

Agenda

Authentication

Authenticity and Integrity

Authentication and message integrity are not separable from each other

- What use is authenticity if the message can be changed?
- What use is message integrity if its sent by anyone else?

Authentication

Authenticity and Integrity

Authentication and message integrity are not separable from each other

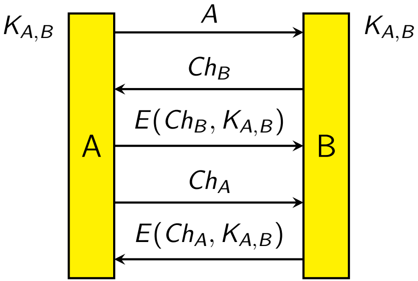
- What use is authenticity if the message can be changed?
- What use is message integrity if its sent by anyone else?

Procedure

1. First, setup of a secure channel with mutual authentication
2. Next, use a secret session key to ensure integrity (and confidentiality)

Authentication with Secret Keys

- Principle of a Challenge-Response-Protocol



$K_{A,B}$: common secret key

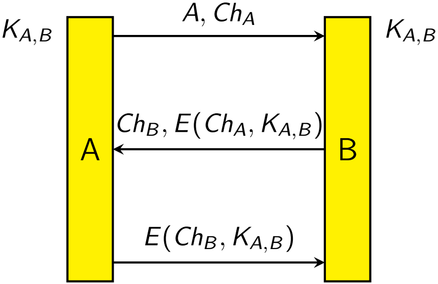
- Communication request A, contains the identity of A
- Challenge Ch_B (e.g., random number) posed by B
- B can check if the response contains Ch_B ($\rightarrow$ only A can be the communication partner)
  - analog in the reverse direction ($\rightarrow$ only B can be the communication partner)

- Problem: Management of many secret keys

$\rightarrow$ Key Distribution Center (KDC) may be used

On the Design of Secure Protocols (1/2)

- The design of a secure protocol is error-prone!
- Example: Seemingly simplified challenge-response-protocol

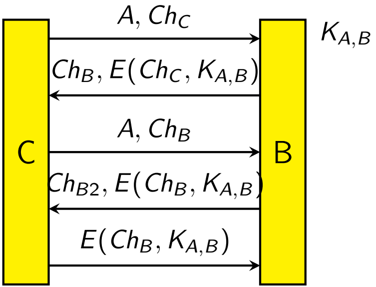


- Idea: Merging messages
  1. Communication request A **and** Ch_A
  2. Response to Ch_A **and** Ch_B
  3. Response to Ch_B
- Only three steps $\rightarrow$ more efficient?

- Claim: This protocol is **not** secure any more!

On the Design of Secure Protocols (2/2)

- Reflection attack: Attacker C, **not** knowing the secret $K_{A,B}$

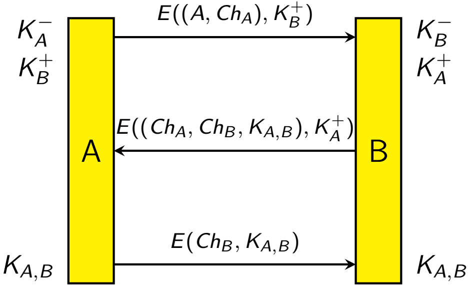


- C starts a first session and retrieves Ch_B
- C starts a second session using Ch_B as alleged own challenge
- C retrieves Ch_B encrypted with $K_{A,B}$: $E(Ch_B, K_{A,B})$
- C uses this to continue the first session

Result: B trusts C, even though C does not know the common secret $K_{A,B}$

Authentication with Public Keys

- Principle
  - No KDC required
  - Attribution of the public keys to the real persons must be ensured



- K_A^- secret key of A
- K_A^+ public key of A
- $K_{A,B}$ session key, generated by B, short-lived

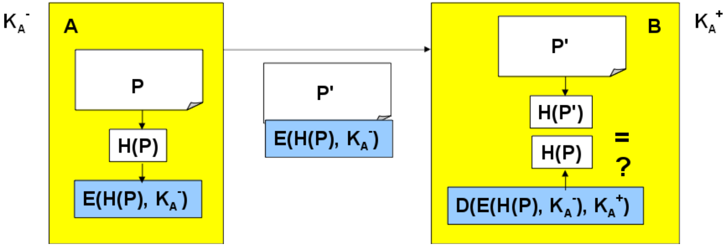
Agenda

Digital Signatures

- Comparable to a physical signature
  - Must not be detachable from the signed document
  - Not (easily) forgeable
- Signature provides reliable determination of ...
  - Authorship
  - Non repudiation
  - Integrity
  - Authenticity
- ... but does not protect the confidentiality of the message
  - → Requires encryption
- Combination of ...
  - Hash Algorithm
  - Public Key Infrastructure

Procedure

- Sign the message by encrypting the hash value of a message with the private key
- The public key can be used by the receiver to verify the validity of the signature



Procedure

1. Alice (A) is the sender and Bob (B) the receiver of a message
2. Alice uses the hash algorithm H on the plaintext message P to create a hash value $V_A = H(P)$
3. Alice encrypts the hash value V_A with her private key K_A^-

   $$VC_A = E(V_A, K_A^-) \text{ (=Signature)}$$

4. The encrypted hash value is appended on the (unencrypted) message and transmitted along with the message
5. Bob decrypts VC_A using Alice's public key K_A^+

   $$V = D(VC_A, K_A^+)$$

6. Determination of the hash value of message P:

   $$V_B = H(P)$$

7. $V = V_B$?
   if yes: Signature is authentic and the message has not been modified

Agenda

1 Cryptographic Concepts
- Encryption Methods
- Cryptographic Hash Functions

2 Cryptographic Methods
- Authentication
- Digital Signatures
- Key Management

Key Management

- Goal
  - Secure and efficient life cycle management for keys
    - Generation/setup
    - Distribution
    - Revocation
  - Trust in key management is mandatory!
- Different approaches
  - When working with secret keys:
    Key Distribution Center (KDC)
  - When working with public keys:
    Public Key Infrastructure (PKI)

  → Anything but trivial!

PKI Systems

- Main problem:
  - Secure distribution of public keys
  - Man-in-the-Middle (MitM) attack during key exchange is possible
- Basis
  - Certificates
    - Authenticity of public keys
  - Directory services
    - Lookup for public keys
    - e.g., LDAP (Lightweight Directory Access Protocol)

Certificates

- Certificates
  - Are used to confirm the authenticity of a public key
  - ⇒ Confirm the affiliation to a certain entity (person, service, organization ...)
- Certification Authority (CA)
  - Issuing authority
  - Ensures the ownership of an key
  - Trustworthiness is required or the public of the CA must be certified itself by a higher CA
  - Controlled by central entity (root CA) which certifies the public keys of CA (→ chain of trust)
- Certification Revocation List (CRL)
  - Contains serial numbers of certificates which became invalid (have been revoked)

X.509 Standard for Certificates

- Versions: v1-v3
- Essential information of a certificate:
  - Version
  - Public key of the certificate owner
  - Distinguished Name (of the owner)
    - Common Name, CN
    - Organization, O
    - Organizational Unit, OU
    - Locality, L
    - State, ST
    - Country, C
  - Name and country of the issuing CA (Distinguished Name)
  - Validity period
  - Used algorithms
  - Extensions

Important takeaway messages of this chapter

- An 100% secure system does not exist $\rightarrow$ security is always a tradeoff
- Security measures are often implemented via cryptographic methods
- Encryption and authentication are the foundation for every security concept