ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithms for Radio Networks

Security in Computer Networks

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Prof.Christian Schindelhauer

CoNe
Freiburg

IIF
INSTITUT FÜR
INFORMATIK
FREIBURG

What is a Threat

- **Definition**
  - A threat of a computer network is any possible event or series of actions that can lead to a breach of security objectives
  - The realization of a threat is an attack
- **Examples**
  - A hacker gains access to a closed network
  - Publication of passing e-mails
  - Unauthorized access to an online bank account
  - A hacker brings a system to crash
  - Identity theft

Security Objective

- **Confidentiality**
  - transmitted or stored data can only be read or written from the target audience
  - anomity: confidentiality of the identity of the participants
- **Data integrity**
  - changes of data should be explored
  - author of data should be visible
- **Accountability**
  - for each communication event the responsible person should be detectable
- **Availability**
  - services should be available and operating
- **Access control**
  - Services and information should be accessible only to authorized users

Threats

- **Masquerade**
  - someone pretends to be someone from another
- **Eavesdropping**
  - someone reads information that is not for him
- **Authorization Violation**
  - someone uses a service or a resource that is not allowed for him
- **Loss or alteration of information**
  - data is altered or destroyed
- **Denial of communication**
  - Someone claims not to be in responsible for the ongoing communication
- **Falsifying information**
  - Someone created or changed messages on behalf of other
- **Sabotage**
  - Every action restricting the availability or proper functioning of the services or the system

Threats and Security Goals

Security Objective	Threat						
	Masquerade	Eavesdropping	Authorization Violation	Loss or Alteration of Information	Denial of Communication	Falsifying Information	Sabotage
Confidentiality	X	X	X				
Anonymity	X		X	X		X	
Accountability	X		X		X	X	
Availability	X		X				X
Access Control	X		X			X	

Terminology of Communication Security

- **Security service**
  - An abstract service that tries to achieve a security feature
  - can be realized with (or without) the help of cryptographic algorithms and protocols, e.g.
    - encryption of data on a hard disk
    - CD in a safe
- **A cryptographic algorithm**
  - mathematical transformations
  - used in cryptographic protocols
- **A cryptographic protocol**
  - Series of steps and messages to achieve a security goal

Security Service

- **Authentication**
  - Digital Signature: data is provable received from the author
- **Integrity**
  - secures that a date is not modified without detection
- **Confidentiality**
  - data can only be understood by the recipient
- **Access control**
  - check that only authorized persons have access to services and information
- **Repudiation**
  - proves that the message is undeniably from the originator

Encryption Methods

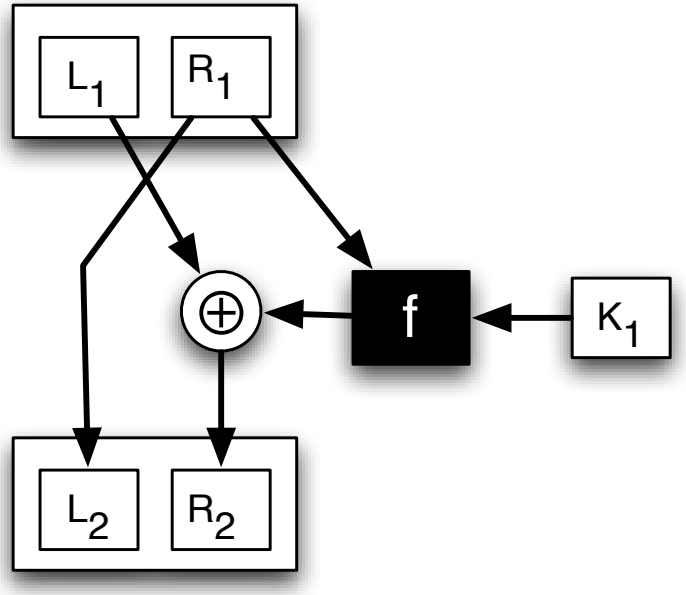
- **Symmetric encryption algorithms, e.g.**
  - Feistel cipher
  - DES (Digital Encryption Standard)
  - AES (Advanced Encryption Standard)
- **Cryptographic hash function**
  - SHA-1, SHA-2
  - MD5
- **Asymmetric encryption**
  - RSA (Rivest, Shamir, Adleman)
  - El-Gamal
- **Digital signatures (electronic signatures)**
  - PGP (Phil Zimmermann), RSA

Symmetric Encryption

- **E.g. Caesar's code, DES, AES**
- **Functions f and g, where**
  - Encryption f
    - f (key, text) = code
  - Decoding g:
    - g (key, code) = text
- **The key**
  - must remain secret
  - must be available to the sender and receiver

Feistel Chiffre

- **Splitting the message into two halves L_1, R_1**
  - Keys K_1, K_2, ...
  - Several rounds: Resulting code: L_n, R_n
- **encoding**
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
- **Decryption**
  - $R_{i-1} = Li$
  - $L_{i-1} = R_i \oplus f(L_i, K_i)$
- **f may be any complex function**



Other Symmetric Codes

- **Skipjack**
  - 80-bit symmetric code
  - is based on Feistel Cipher
  - low security
- **RC5**
  - 1-2048 bits key length
  - Rivest code 5 (1994)
  - Several rounds of the Feistel cipher

Digital Encryption Standard

- **Carefully selected combination of**
  - Xor operations
  - Feistel cipher
  - permutations
  - table lookups
  - used 56-bit key
- **1975 developed at IBM**
  - Now no longer secure
  - more powerful computers
  - New knowledge in cryptology
- **Succeeded by: AES (2001)**

Advanced Encryption Standard

- **Carefully selected combination of**
  - Xor operations
  - Feistel cipher
  - permutations
  - table lookups
  - multiplication in GF [2^8]
  - 128, 192 or 256-bit symmetric key
- **Joan Daemen and Vincent Rijmen**
  - 2001 were selected as AES, among many
  - still considered secure

Cryptographic Hash Function

- **E.g. SHA-1, SHA-2, MD5**
- **A cryptographic hash function h maps a text to a fixed-length code, so that**
  - h(text) = code
  - it is impossible to find another text:
    - h(text‘) = h(text) and text ≠ text'
- **Possible solution:**
  - Using a symmetric cipher

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithms for Radio Networks

Security in Computer Networks

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Prof.Christian Schindelhauer

CoNe
Freiburg

IIF
INSTITUT FÜR
INFORMATIK
FREIBURG