Energy Informatics
04 Security

Christian Schindelhauer
Technical Faculty
Computer-Networks and Telematics
University of 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

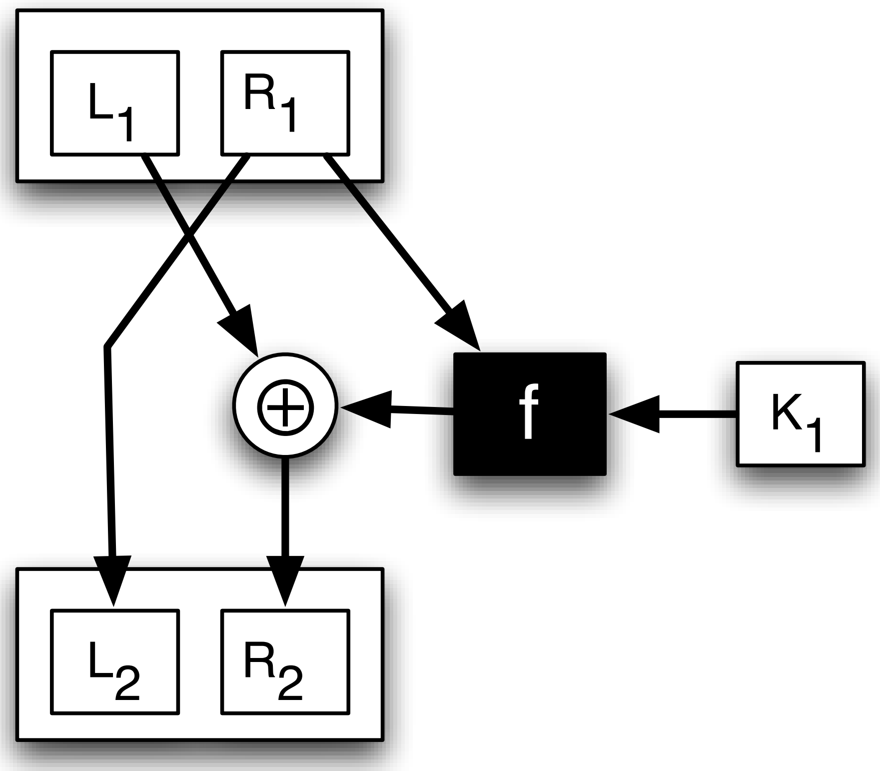
- Symmetric encryption algorithms, e.g.
  - Feistel cipher
  - DES (Digital Encryption Standard)
  - AES (Advanced Encryption Standard)
- Cryptographic hash function
  - SHA-1, SHA-2
  - MD5
- Asymmetric encryption
  - RSA (Rivest, Shamir, Adleman)
  - El-Gamal
- Digital signatures (electronic signatures)
  - 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
  - $R_{i-1} = L_i$
  - $L_{i-1} = R_i \oplus f(L_i, K_i)$
- 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

Asymmetric Encryption

- E.g. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977
  - Diffie-Hellman, PGP
- Secret key: sk
  - Only the receivers of the message know the secret key
- Public key: pk
  - All participants know this key
- Generated by
  - keygen(sk) = pk
- Encryption function f and decryption function g
  - Known to everybody
- Encryption
  - f(pk,text) = code
  - everybody can generate code
- Decryption
  - g(sk,code) = code
  - only possibly by receiver

Example: RSA

- R. Rivest, A. Shamir, L. Adleman
  - On Digital Signatures and Public Key Cryptosystems, Communication of the ACM
- Algorithm is based on the computational complexity of integer factorization
- 1st example
  - 15 =   ? * ?
  - 15 = 3 * 5
- 2nd example
  - 386581864584112731912956727734835955744479041028993358648355 2047443 =
    1234567890123456789012345678900209 * 3131313131313131313131313131300227
- To this day no efficient integer factorization algorithm is known
  - Yet, multiplication can be done efficiently
  - Prime numbers can be found efficiently
    - Since prime numbers occur frequently
    - Efficient randomized prime number tests are available

RSA

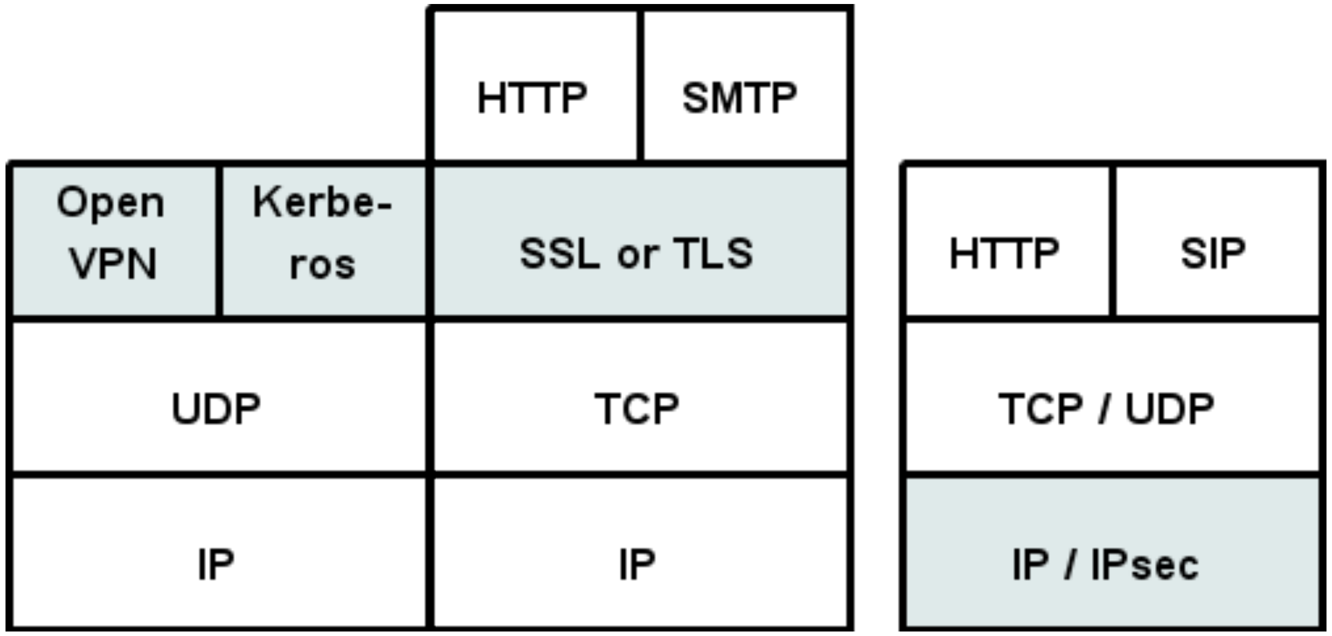
- Generation of keys
  - Choose two random prime numbers p, q with k bits ($k \geq 500$).
  - $n = p \cdot q$
  - e is a number relatively prime to $(p - 1)\cdot(q - 1)$.
  - $d = e^{-1} \bmod (p - 1)(q - 1)$
    - i.e. $d \cdot e \equiv 1 \bmod (p - 1)(q - 1)$
- Public key pk = (e, n)
- Secret key sk = (d, n)
- Encoding
  - Partition message in block sizes of 2^k bits
  - Interprete block M as number $0 \leq M < 2^{2k}$
  - Code: $P(M) = M^e \bmod n$
- Decoding
  - $S(C) = C^d \bmod n$

Digital Signatures

- Digital Signatures
  - signer has a secret key **sk**
  - document will be signed with the secret key
  - and can be verified with a public key **pk**
  - public key is known to all
- Example of a signature scheme
  - m: message
  - Signer
    - computes **h(text)** with cryptographic hash function **h**
    - and publishes m and
signature = g (sk, h (text)),
g is the decryption function
  - Checker
    - computes h(text)
    - and verifies
f (pk, signature) = h (text)
for the asymmetric encryption function **f**

Network Security on Different Layers

- Security measures could be hooked to different layers of the stack
  - Link layer: one `hop` (e.g. wireless link)
  - IP Layer (IP-Sec): transparent to application
  - Transport Layer (SSL/TLS): easy, widely used
  - Application Layer (PGP, S/MIME)



SSL (Secure Socket Layer)

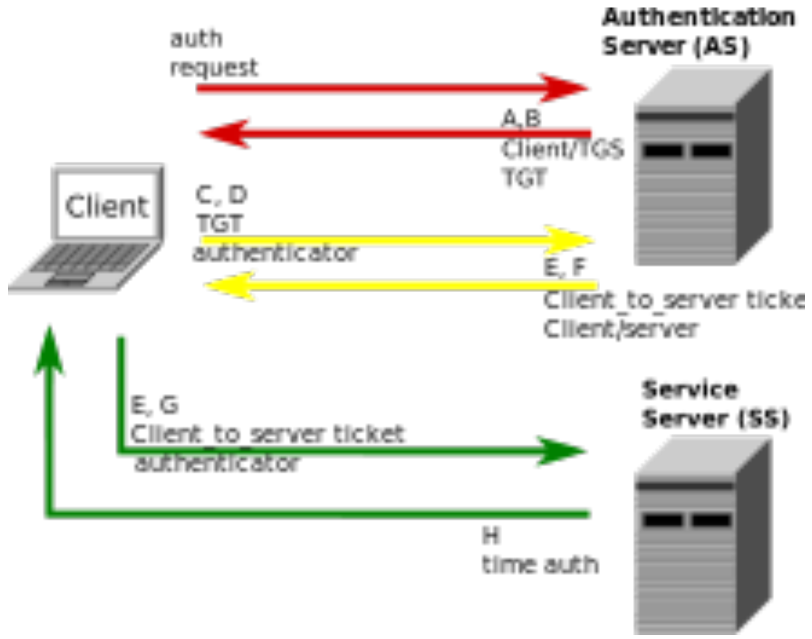
- Transport layer security service, yields secure channel
  - Secure byte stream
  - Optional public-key server authentication
  - Optional client authentication
- Development started by Netscape to offer secure Internet business
  - Used/Implemented with HTTP first (HTTPS, port 443)
  - Hash: combined MD5 & SHA
  - Encryption: Diffie Helman, RSA & DES, RC4
- Version 3 designed with public input; subsequently became Internet standard TLS (Transport Layer Security)
- Uses TCP to provide a reliable end-to-end service
  - Not restricted for secure web (HTTP) transactions
  - Useful for any TCP based service to be secured: HTTP, IMAP, POP, NNTP, telnet, telephony signaling

OpenVPN

- Networking
  - uses UDP
  - creates SSL tunnel
  - Point to point
- Encryption
  - OpenSSL library with RSA, AES, RC5, MD4, SHA-2, …
- Authentication by
  - pre-shared keys
  - certificates
  - user/password

Kerberos

- Authenticates
  - servers and client
  - protects against eavesdropping and replay attacks
- Networking
  - uses authentication server (AS)
  - client authenticates to the AS
    - via UDP
  - receives a ticket to connect to the service
- Encryption methods
  - DES, AES for communication
  - Public key during authentication (optionally)



Wikipedia

IP sec

- IP level security -> IPsec
- IPSEC is Internet Protocol SECurity
  - above the network layer
  - no alteration to the IP was needed
  - simply the transportation protocol was interchanged (or and additional security header introduced)
- Strong cryptography
  - Authentication ensures that packets are from the right sender and have not been altered in transit
  - Encryption prevents unauthorized reading of packet contents

IPsec

- IPSEC: framework for encrypting the whole IP traffic that might occur
- In reality: mainly secure tunnels through untrusted networks
  - Every packet passing through the untrusted net
  - encrypted by the IPSEC gateway machine
  - decrypted by the gateway at the other end
- Another implementation of a Virtual Private Network (VPN)
  - Seen OpenVPN in practical as another example

Energy Informatics
04 Security

Christian Schindelhauer
Technical Faculty
Computer-Networks and Telematics
University of Freiburg