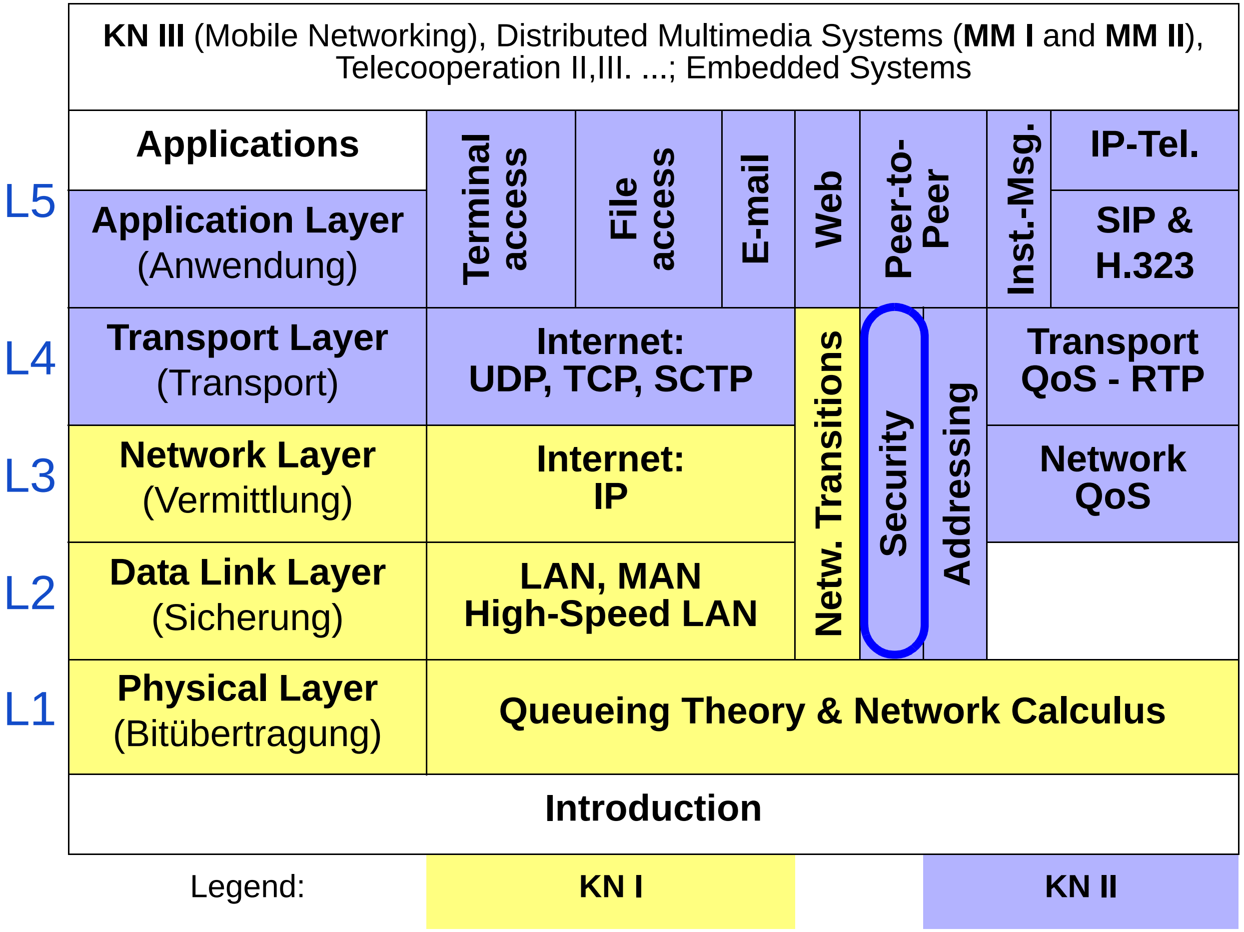
Communication Networks II
Security

Prof. Dr.-Ing. **Ralf Steinmetz**

TU Darmstadt - Darmstadt University of Technology,
Dept. of Electrical Engineering and Information Technology, Dept. of Computer Science
KOM - Multimedia Communications Lab
Merckstr. 25, D-64283 Darmstadt, Germany, Ralf.Steinmetz@KOM.tu-darmstadt.de
Tel.+49 6151 166151, Fax. +49 6151 166152

httc - Hessian Telemedia Technology Competence-Center e.V
Merckstr. 25, D-64283 Darmstadt, Ralf.Steinmetz@httc.de

Scope


KN III (Mobile Networking), Distributed Multimedia Systems (MM I and MM II), Telecooperation II,III. ...; Embedded Systems
L5
Applications
Application Layer (Anwendung)
Terminal access
File access
E-mail
Web
Peer-to-Peer
Inst.-Msg.
IP-Tel.
SIP & H.323
L4
Transport Layer (Transport)
Internet: UDP, TCP, SCTP
Transport QoS - RTP
L3
Network Layer (Vermittlung)
Internet: IP
Network QoS
L2
Data Link Layer (Sicherung)
LAN, MAN High-Speed LAN
Netw. Transitions
Security
Addressing
L1
Physical Layer (Bitübertragung)
Queueing Theory & Network Calculus
Introduction
Legend:
KN I
KN II

Overview

1. Introduction
2. Cryptographical Methods/Implementations
3. Secure Communication
4. Network Access Control - Firewalls
5. Conclusion

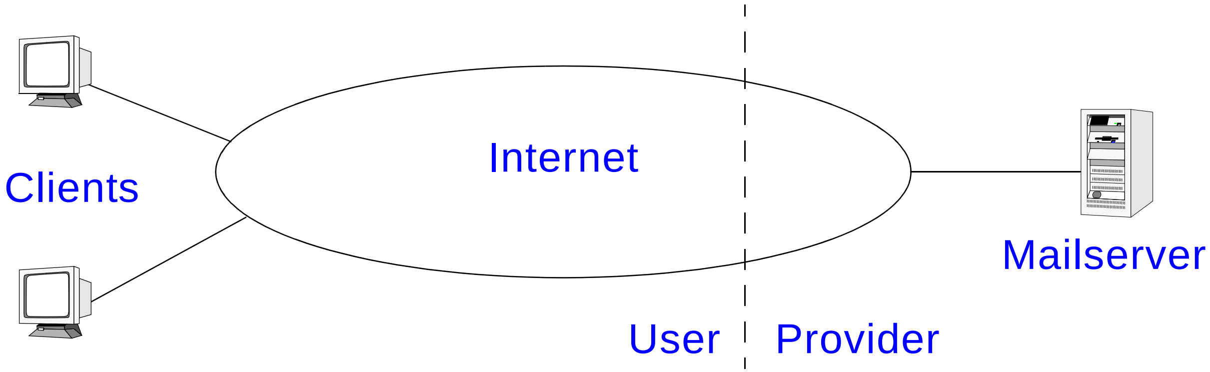
1. Introduction

Service requirements for success

- **Functionality, economic efficiency, ...**
- **Trust in**
  - Availability, reliability, predictability, **SECURITY**, ...

⇒ **Security is one necessary feature for a service to become successful**

Example: security requirements for a mail service



- **User view:** **who is reading my mail?**
  solution: ENCRYPTION of mails (e.g. PGP)
- **Provider view:** **who is using the mail service (billing)?**
  solution: ACCESS CONTROL to the mail server

⇒ **Users need privacy, provider needs billing**

⇒ **Different (maybe contradicting) SECURITY GOALS**

1.1 Security Goals

Focus of the lecture is on communication networks

⇒ **Security goals defined in the context of communication networks**

Goals:

- **CONFIDENTIALITY** — **Only sender and receiver should be able to read a message.**

  ⇒ **prevent unauthorized data access**

- **AUTHENTICATION** — **It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.**

  ⇒ **proof of the identity of the originator**

- **INTEGRITY** — **It should be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one.**

  ⇒ **proof that data is unchanged**

- **NON-REPUDIATION** — **A sender should not be able to falsely deny later that he sent a message.**

  ⇒ **guarantee communication liability**

1.2 Attacker

Some possible attackers

- **(Defective) software**
  - A software or system influences the behavior of an other system
  - Examples: mail server with a mail loop (**DoS** attack),
    P2P software consuming all available bandwidth
- **(Stupid) user**
  - User might attack a system without knowing it (accident)
  - User might be angry because he was fired 5 minutes ago
  - Examples: deleting files on the file server,
    P2P software scanning for network nodes
- **Hacker**
  - A hacker tries to get control over a system or to destroy a system
  - Examples: get control over a file server to distribute hacked software
    kill the www server of an unloved company
- **Spies**
  - People from an competing company/country
  - Examples: get a copy of the new marketing campaign,
    have a look at the new patent applications,
    read the mail of the president

⇒ **Most attackers affect the systems, not the information (spies are rare)**

1.3 Attacks

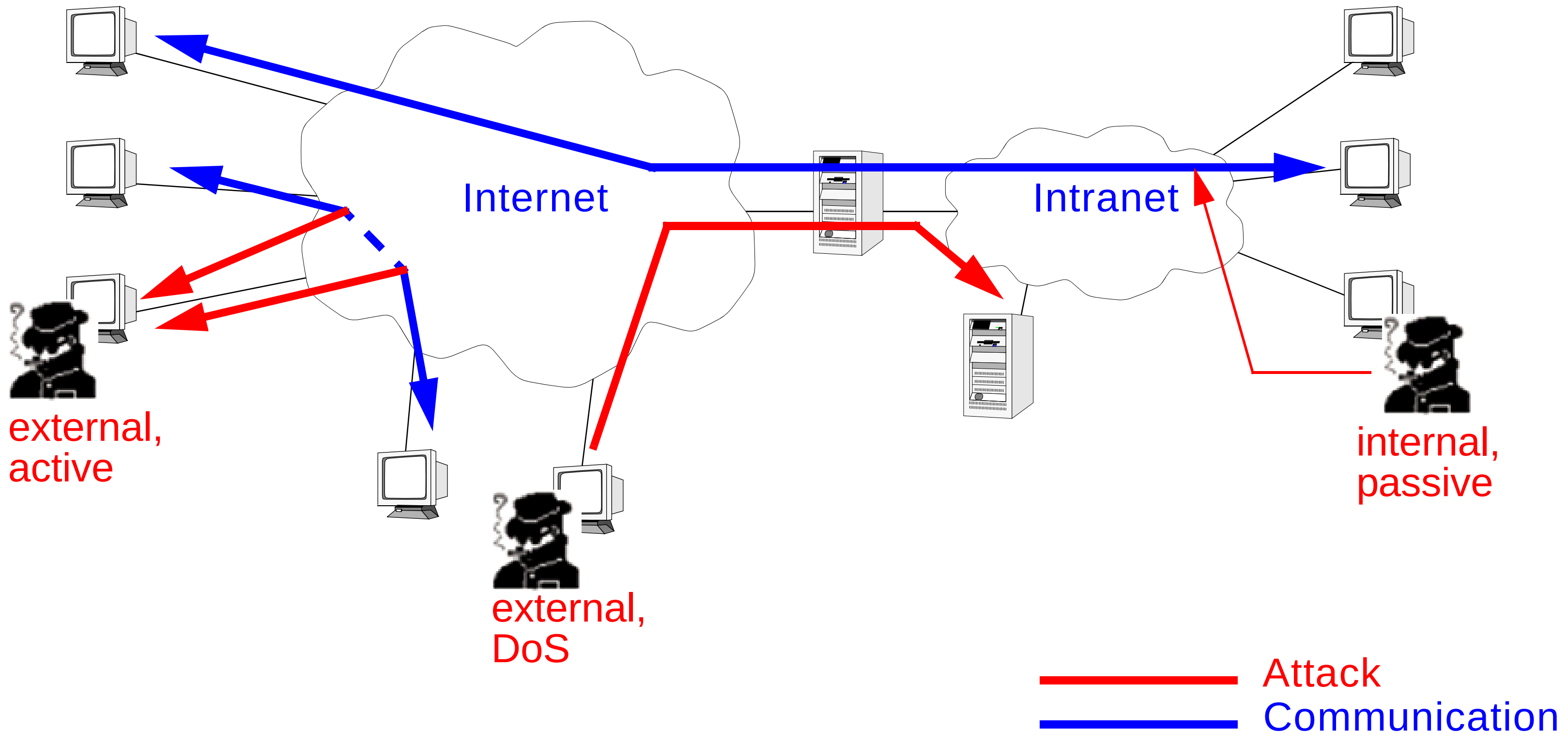
Attacker

- **External, internal**

Attacks

- **Passive attacks, active attacks, Denial of Service (DoS) attacks**

Different points of attack in distributed systems

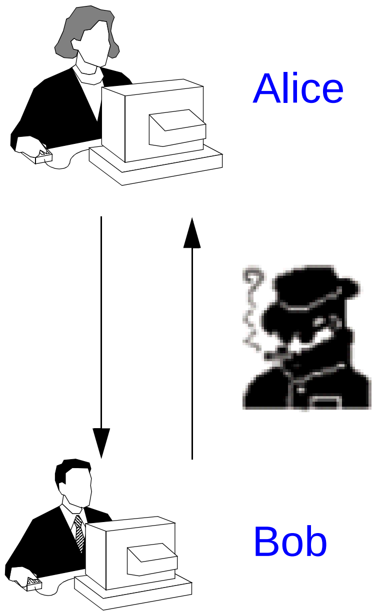


www.kom.tu-darmstadt.de
www.httc.de

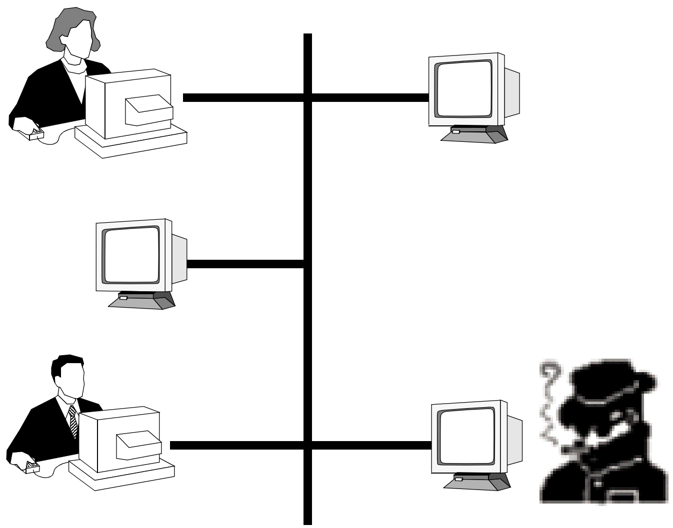
Passive Attacks

Passive attacks (examples)

- **Sniffing**
    1. Read all packets
    2. Select interesting packets using protocol information (IP address, Ports, ...)
    3. Checking data part
- **Message traffic analysis**
    1. Who communicates with whom
    2. What are the traffic parameters (time, amount, size and frequency of messages, ...)
    3. Conclusions regarding message contents



Example: Ethernet



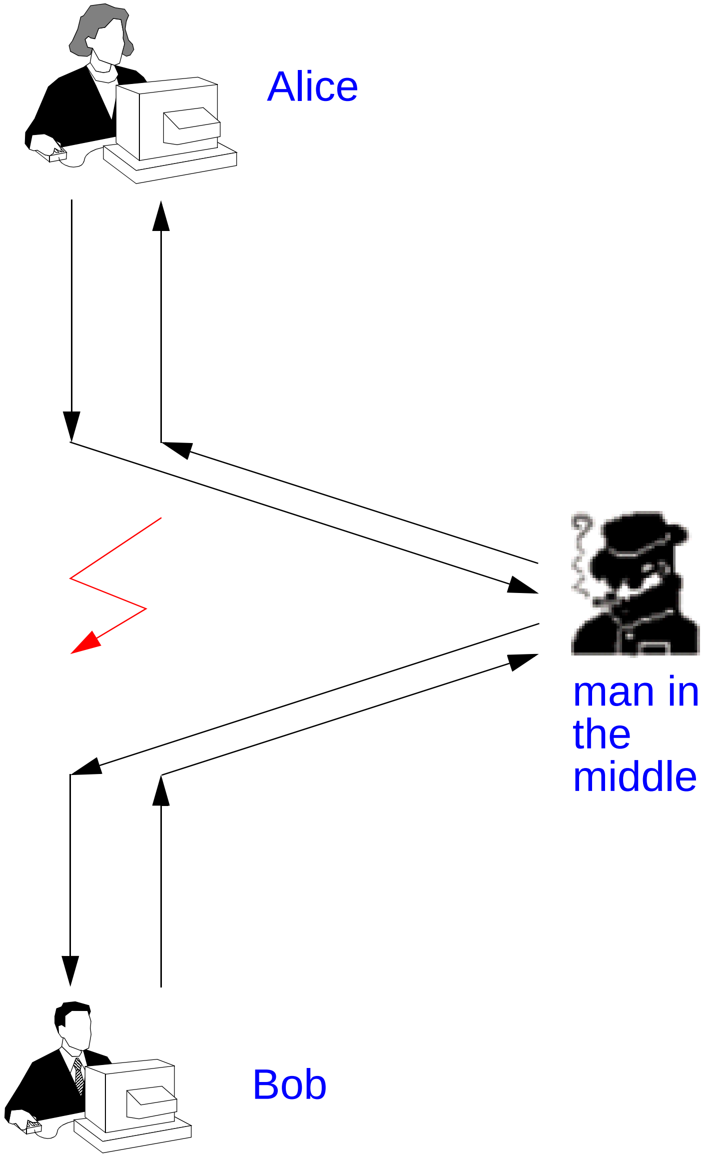
Tools

- **Sniffer Pro**
- **Sniffit**
- **Tcpdump**
- **dsniff**

Active Attacks

Active attacks (examples)

- **Interruption**
  - E.g. deleting messages
- **Modification of messages**
  - E.g. man in the middle
- **Fabrication of messages**
  - E.g. replay of old messages or generation of new messages (spoofing)
  - E.g. sending login requests to a server
  - .....



Tools

- **ipspoof**
- **mandax**
- **dsniff**

Denial of Service Attacks

Denial of service attacks (examples)

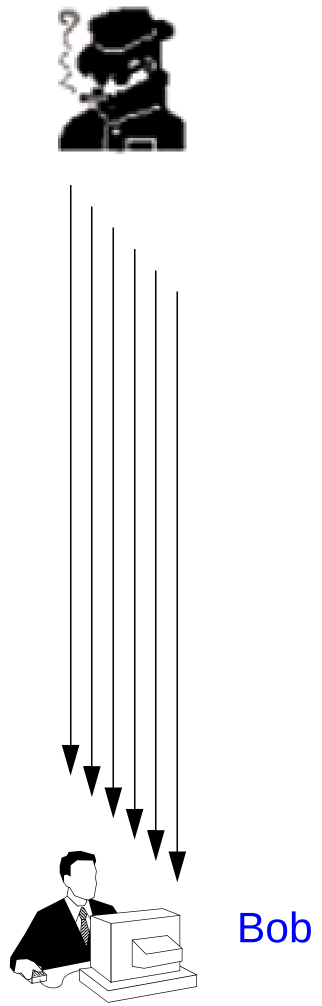
- TCP SYNC Flooding
- UDP Packet Storm
- Ping Flooding
- E-Mail Bombing
- IP Fragmentation

Distributed Denial of service attacks

- Controlled combination of many attackers
- Well known DDoS attacks
  - DNS
  - HTTP

Tools

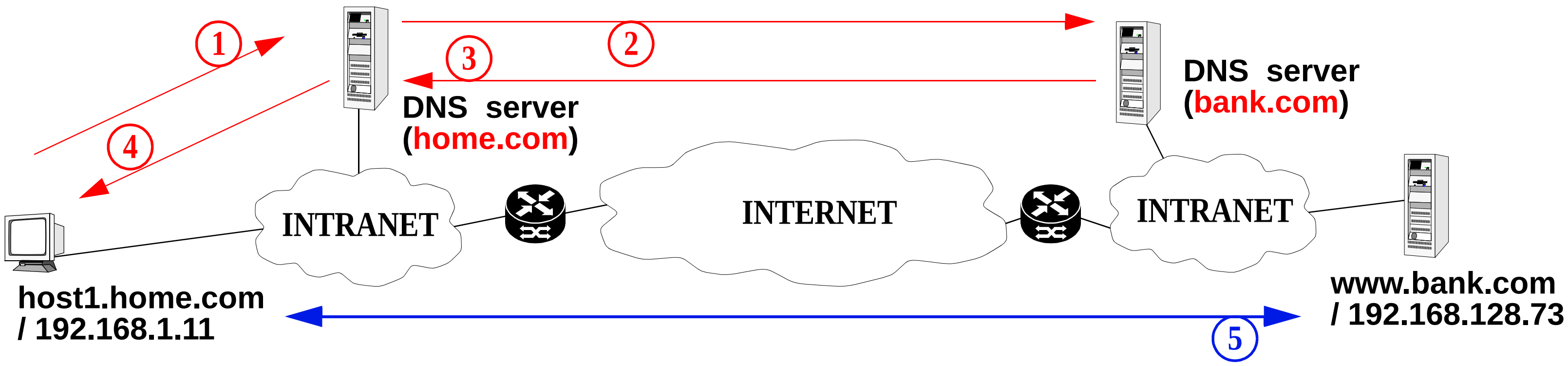
- "Stacheldraht"
- Tribe Flood Network
- Shaft
- M Stream



1.4 Attack Example

Example: DNS spoofing

"good case"

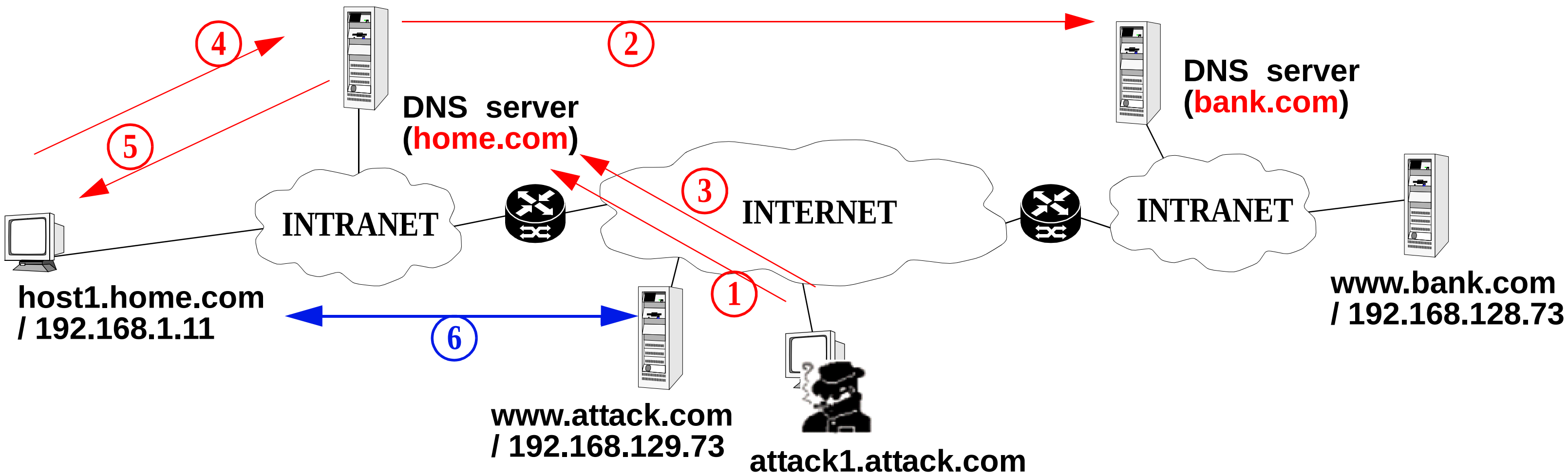


1. **Host1 sends a DNS request to its local DNS server and asks for the IP address of www.bank.com.**
2. **The DNS server can not resolve the request and forwards the request to the DNS server of bank.com.**
3. **The DNS server is capable to resolve the request and sends the IP address (192.168.128.73) back to the requesting DNS server.**
4. **The home.com DNS server sends the answer to host1.**
5. **Host1 is now able to communicate with www.bank.com.**

Attack Example

Example: DNS spoofing

"bad case"



1. Attack1 sends a DNS request to the home.com DNS server and asks for the IP address of www.bank.com.
2. The DNS server can not resolve the request and forwards the request to the DNS server of bank.com.
3. Attack1 creates a fake DNS packet. The UDP packet uses the source address of the DNS server of bank.com. The information contained in the packet is www.bank.com = 192.168.129.73 (www.attack.com). This information is accepted by the home.com DNS server. The information is cached!
4. Host1 sends a DNS request to its local DNS server and asks for the IP address of www.bank.com.
5. The home.com DNS server sends the answer to host1 (192.168.129.73!!).
6. Host1 now connects to www.attack.com and thinks it is www.bank.com. The user types in his password/pin/tan which can now be used by the attacker.

1.5 Summary

Security problem

- It is not possible to proof that a system is secure
- It is only possible to proof that a system is insecure

Building secure systems

- Usage of well known methods/components
- Monitor the security of a system
- Adapt the system to new threats (attackers learn!)

$\Rightarrow$ **Security is an ongoing process**

Basic building blocks

- Cryptographical methods/implementations
- All other methods/implementations of KN I and KN II (protocols, devices, ...)

Methods/Implementations

- Secure communication: PPTP, IPSec, SSL, ...
- Network access control: Firewalls, NAT
- ...

2. Cryptographical Methods/Implementations

Cryptography

- **Science dealing with the encryption and decryption of messages**

Encryption

- **Transformation of plain text into coded / cipher text**

Decryption

- **Re-transformation of cipher text into plain text**

Basic elements

- **Hash functions**
- **Cryptographical procedures (encryption/decryption)**
  - Symmetric cryptographical procedures
  - Asymmetric cryptographical procedures
- **Digital signatures**
- **Digital certificates**

2.1 One-way Hash Functions

Purpose

- **To produce a “fingerprint” h of a message M**
- **A hash function operates on an arbitrary-length message M and returns a fixed length value h.**

Hash — Message — Procedure

$$h = H(M)$$

fixed length (h) — varying length (M)

One-way characteristics

- **Given M, it is easy to compute h.**
- **Given h, it is hard to compute M such that H(M)=h.**
- **Given M, it is hard to find another message, M’, such that H(M)=H(M’).**

Collision resistance

- **It is hard to find two random messages, M and M’, such that H(M)=H(M’).**

Usage example: storage of passwords

- The value h’ of the user password M is stored in a password file
- At login the user types M, h is computed and compared to h’
- If h=h’, access is granted to the user
- An attacker, stealing the password file will not be able to compute M from h’

One-way Hash Functions

Examples

Message Digest 5 (MD-5)

- Defined in RFC 1321 (Ron Rivest, MIT)
- Length: 128 bit
- Operation "find message matching hash" needs at least 2^{64} operations
- Vulnerable to collision search (Hans Dobbertin, 1996)

Secure Hash Algorithm (SHA)

- Defined by the National Institute of Standards and Technology (NIST)
- Based on MD-4, a predecessor of MD-5
- Length: 160 bit

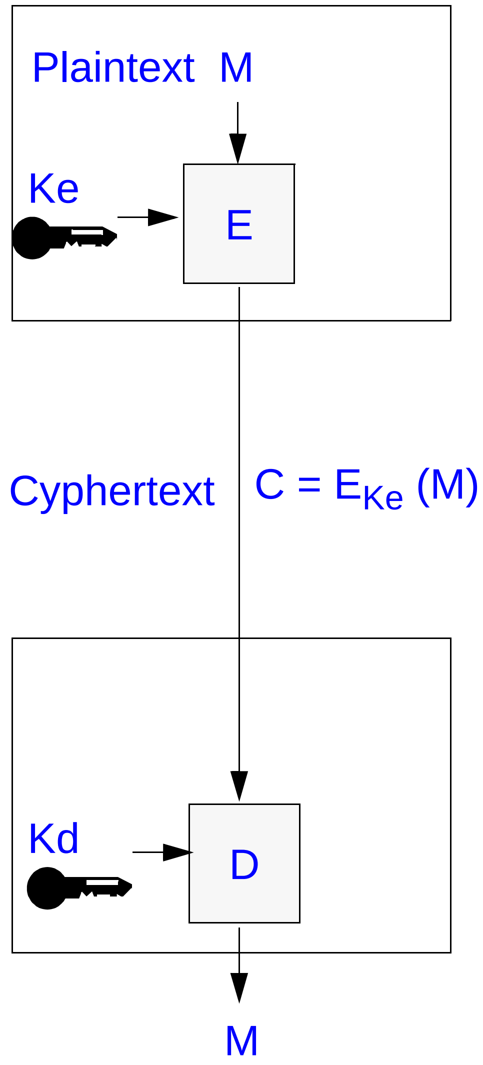
RIPEMD-160

- Developed by a European research project team
- Based on RIPEMD, MD-4 respectively
- Length: 160 bit

2.2 Encryption

Principle

- **M = Message**
- **Ke = Key for encryption**
- **Kd = Key for decryption**
- **E = Encryption algorithm**
- **D = Decryption algorithm**
- **C = Coded message - cypher text**



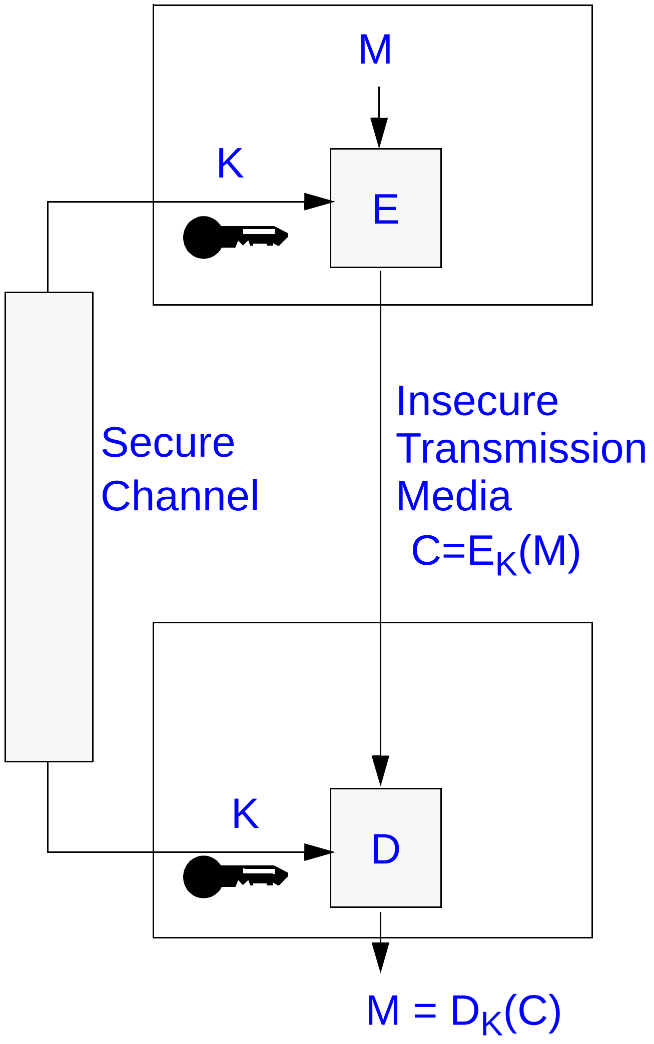
- $C = E_{Ke}(M)$ **and** $M = D_{Kd}(C)$
- $D_{Kd}(C) = D_{Kd}(E_{Ke}(M)) = M$

$\Rightarrow$ **D is the inverse to E**

Symmetric Encryption

Principle

- **Encryption and decryption with secret key K**
- **K = Ke = Kd**
- **Key K has to be exchanged over a secure channel. Sender and recipient have identical keys.**



Examples

- **Data Encryption Standard (DES)**
- **Triple DES (3DES)**
- **IDEA (International Data Encryption Algorithm)**
- **....**

$\Rightarrow$ **Problem: existence of a secure channel for key distribution**

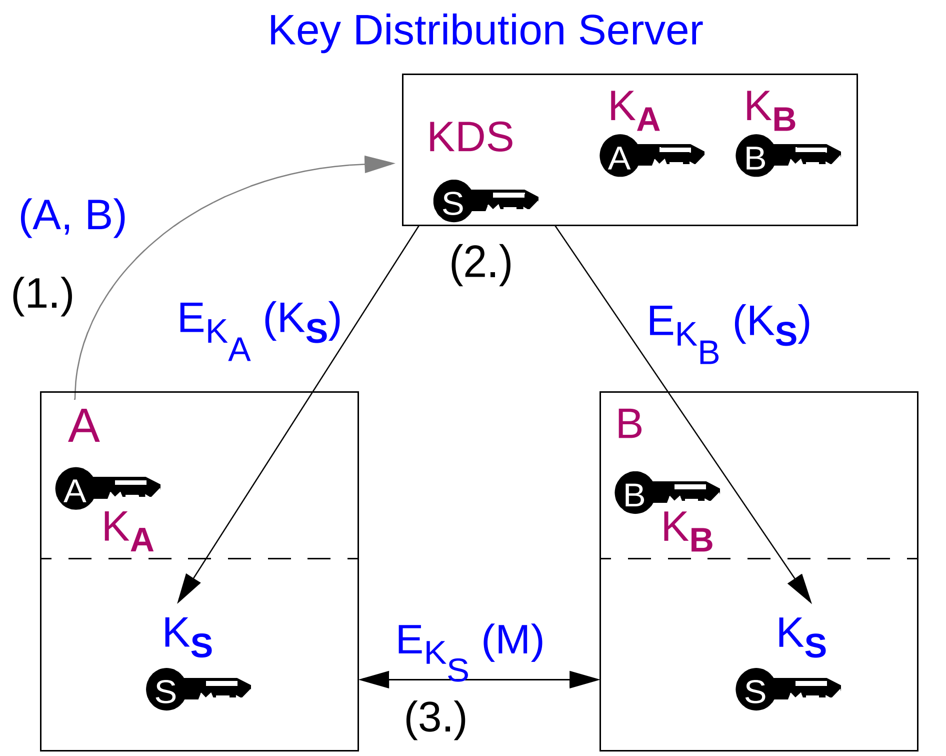
Key Distribution for Symmetric Encryption

Problem

- **Secure distribution of keys K for each participant**

Solution

- Key distribution server (KDS)



Functionality

- **Users A and B and KDS have a common secret key (K_A and K_B for A and B respectively)**
  1. **Upon request from A the KDS generates a key K_S valid for one session between A and B**
  2. **KDS distributes session key K_S encoded with K_A or K_B to both partners A and B.**
  3. **A and B exchange messages symmetric encrypted using session key K_S**

Remaining problem

- **Key distribution server not always and effectively available**

⇒ **Simplify key distribution with asymmetric encryption**

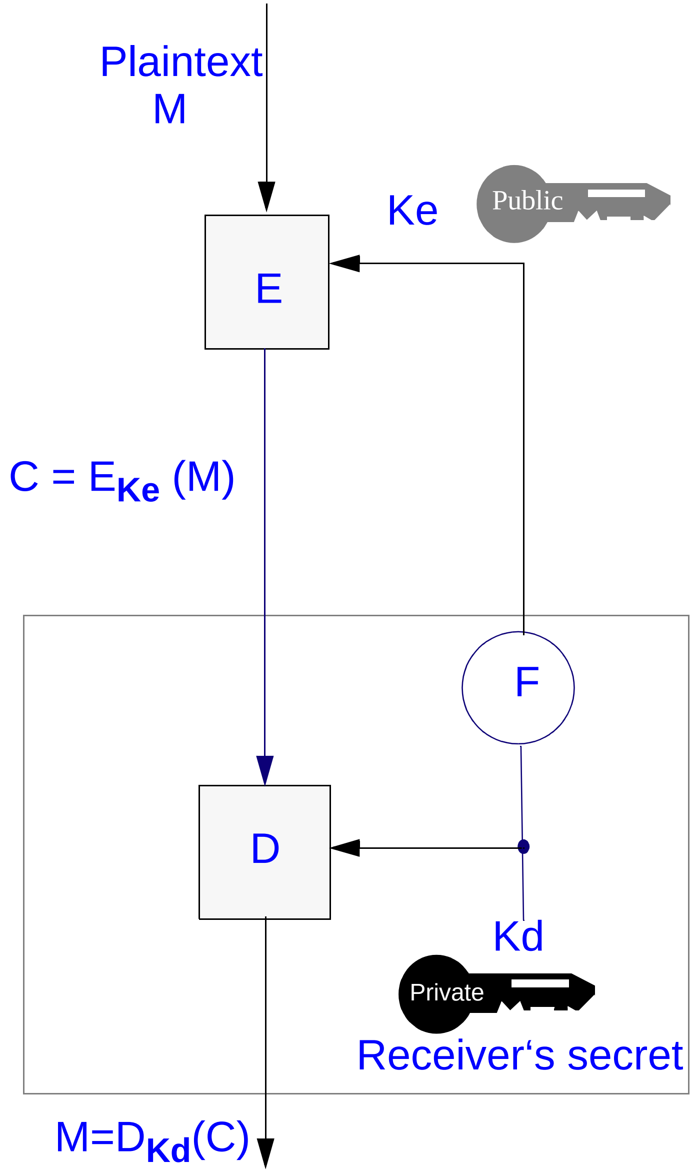
Asymmetric Encryption

Principle

- **Simplify key distribution**
- **Algorithms E and D are public**
- **Ke ≠ Kd and Ke is public**
- **Kd is secret and $M = D_{Kd}(E_{Ke}(M))$**

⇒ **rule 1**
a message encrypted with the public key can only be deciphered with the appropriate private key

⇒ **rule 2**
a message which has been encrypted with a private key can only be decrypted with the matching public key.



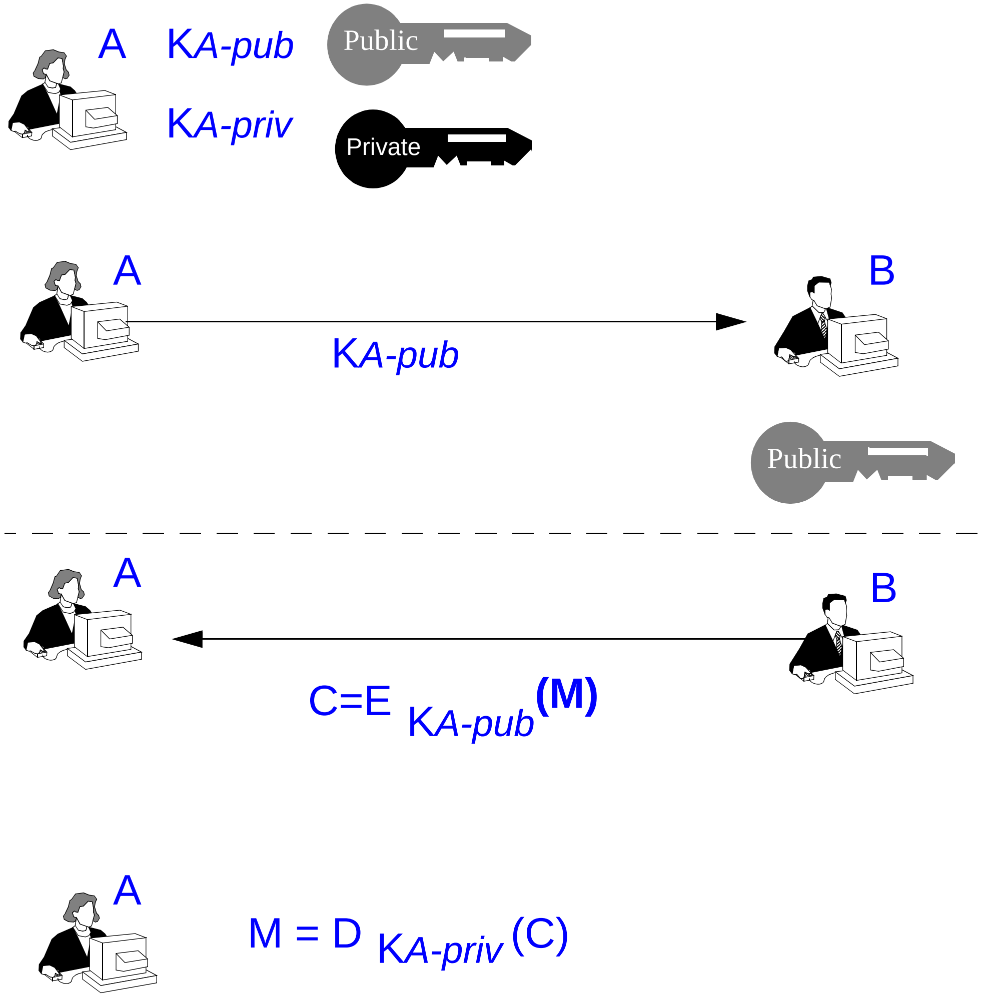
Examples

- **RSA, EL Gamal**

Application of Asymmetric Encryption "Rule 1"

Principle (confidentiality)

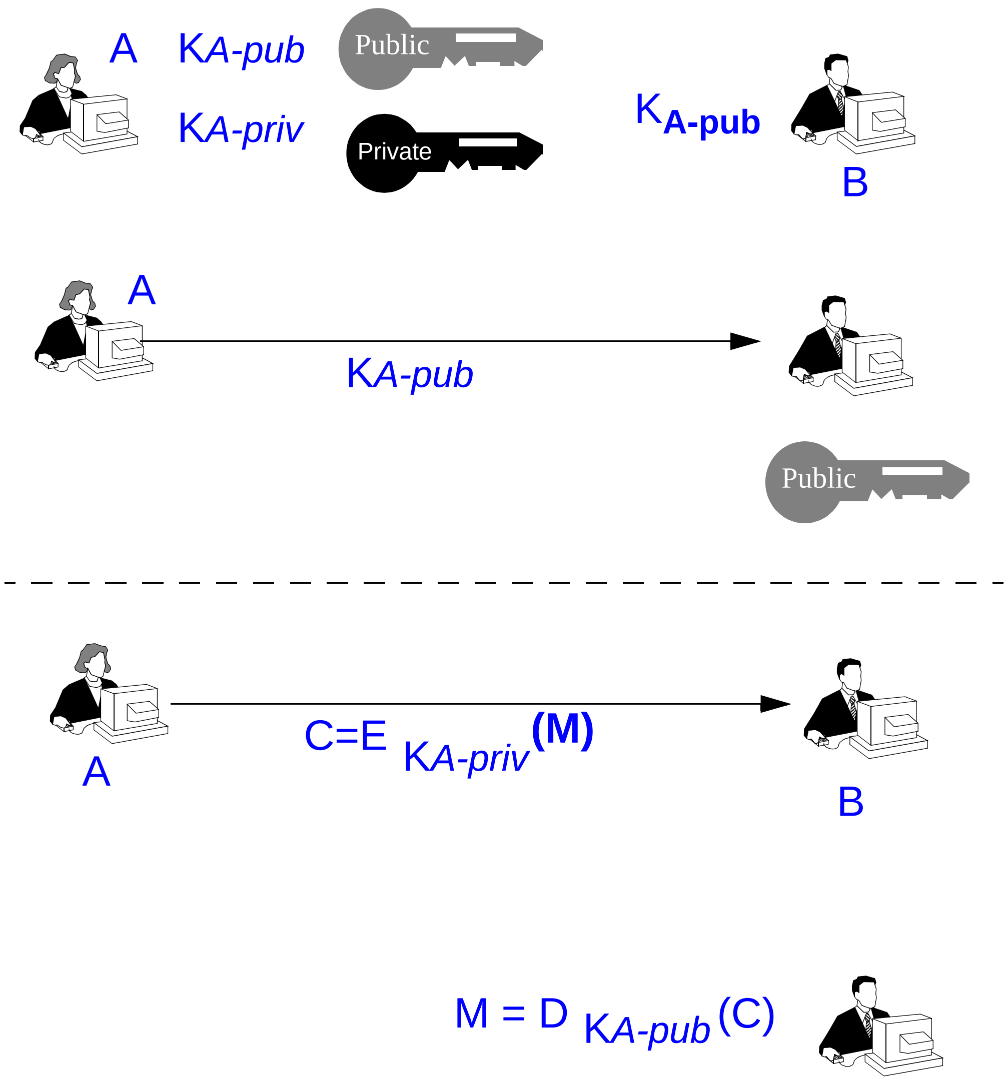
- ***A*** **generates and owns both a public and a private key.**
  1. ***A*** **sends his public key K*A-pub* one times to *B*.**
  2. ***B*** **uses A's public key to encrypt the message and sends the encrypted message to *A*.**
  3. **A can decipher the message with his private key K*a-priv***



Application of Asymmetric Encryption "Rule 2"

Principle (integrity and authenticity)

- A generates and owns both a public and a private key.
  1. A sends his public key K*A-pub* one times to *B*
  2. A encrypts message M with his private key K*a-priv* and sends it to B
  3. B decrypts the encyrted message with the public key of A K*A-pub* .
  4. If this works, only A can have encryted the message and the message has not be changed during transfer.



Note: this does not guarantee confidentiality

$\Rightarrow$ **Combination of both procedures**

A Comparison of Cryptographical Procedures

Symmetric procedures : DES

+ not very complex, higher efficiency
- extensive key distribution
- extensive realization of digital signatures

Asymmetric procedures: RSA

+ simple key distribution
+ digital signatures can easily be realized
- more complex, lower efficiency

Combinations are recommended

starting an interaction with asymmetric procedures

then change to symmetric procedures

2.3 Digital Signature

Required characteristics

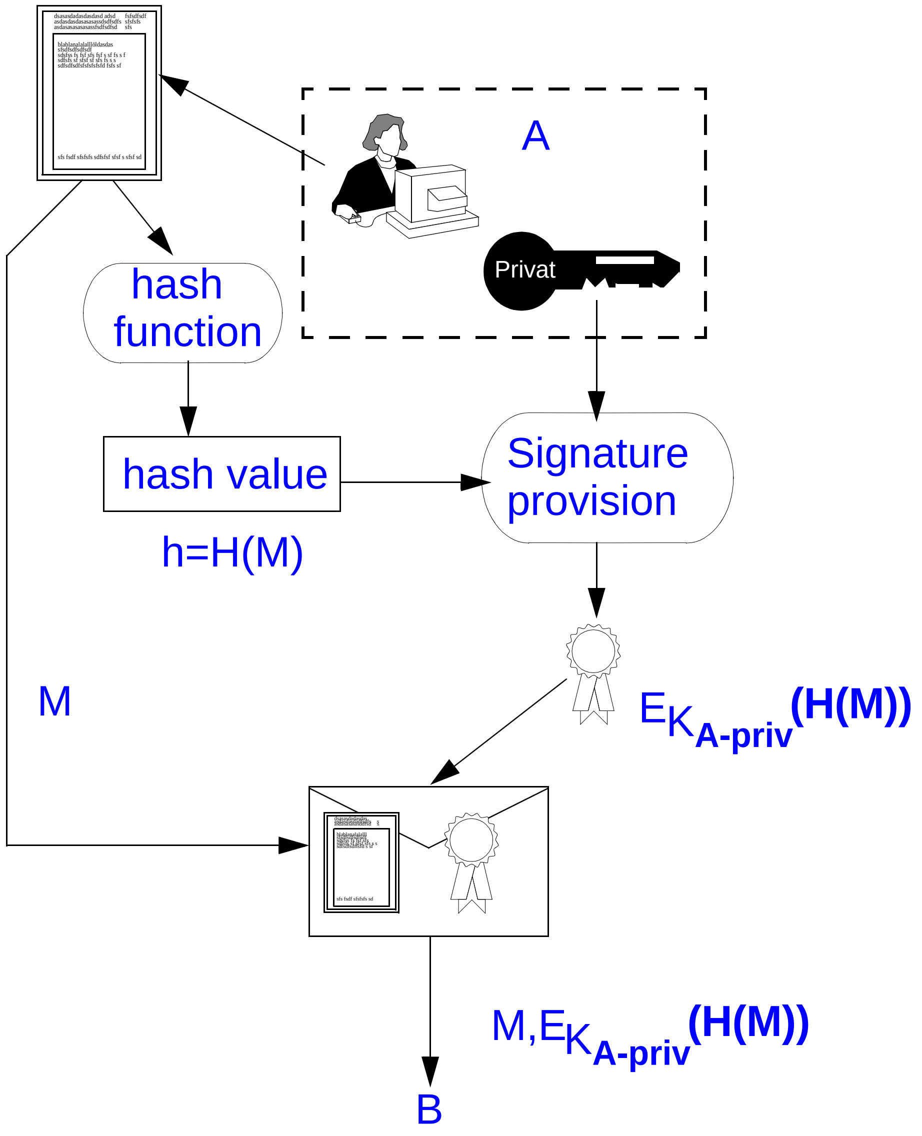
- **Recipient can verify the message's authenticity**
- **Later message repudiation by the sender is prohibited**

To be applied:

- **(Mostly) asymmetric procedures**
- **Secure hash function h=H(M)**

Signature generation:

1. **Hash is generated by the message.**
2. **Hash is encoded with A's private key and is sent together with the message.**



Digital Signature

Signature check

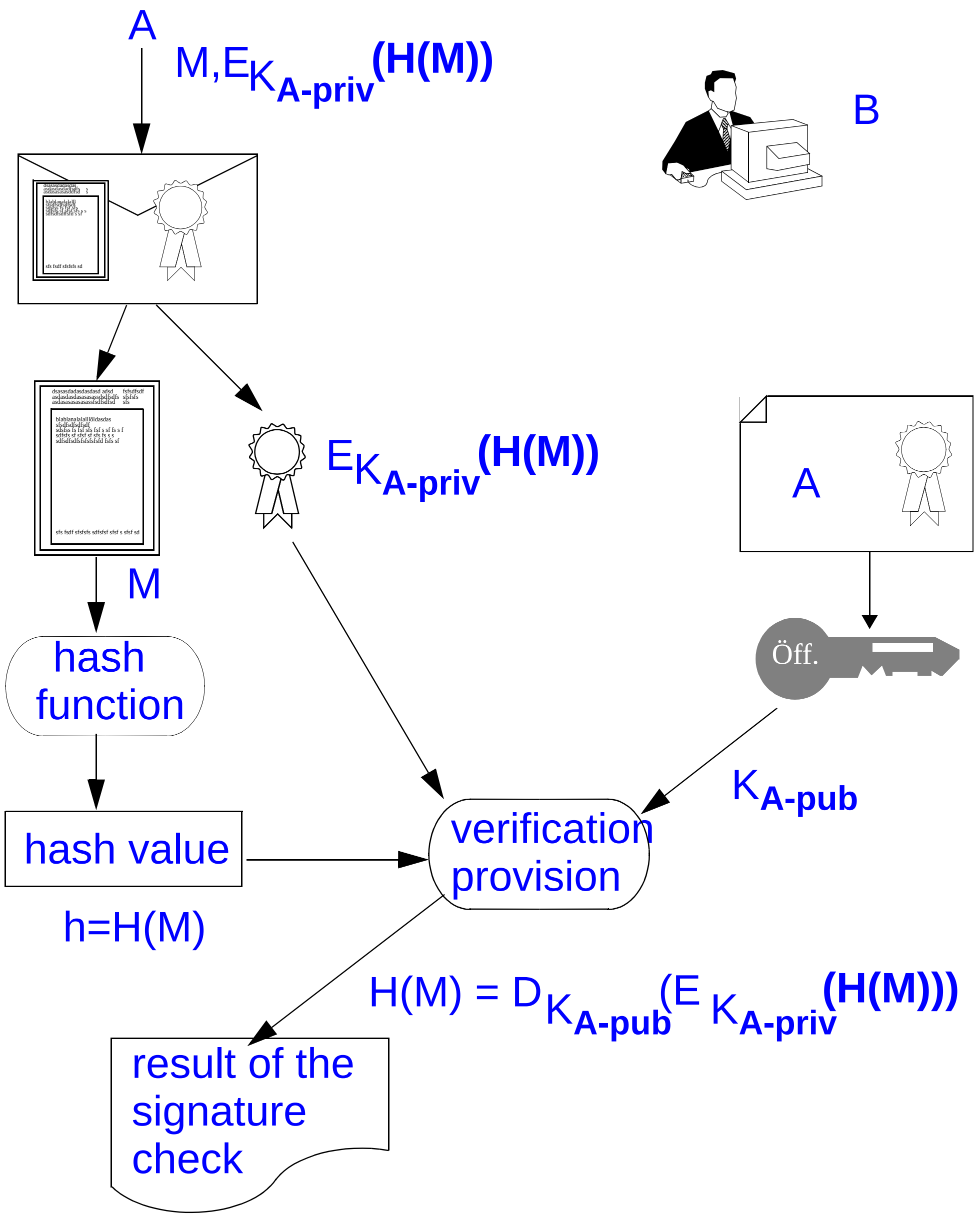
1. **Recipient calculates the hash value of message M.**
2. **The message's digital signature is deciphered with the sender's public key.**
3. **Hash value is compared to deciphered digital signature.**

Result

- **The hash value guarantees the integrity**
- **Only the owner of the private key A can have sent the message (authenticity)**

Problem

- **Who is the owner of the key pair 'A'?**



2.4 Certificates

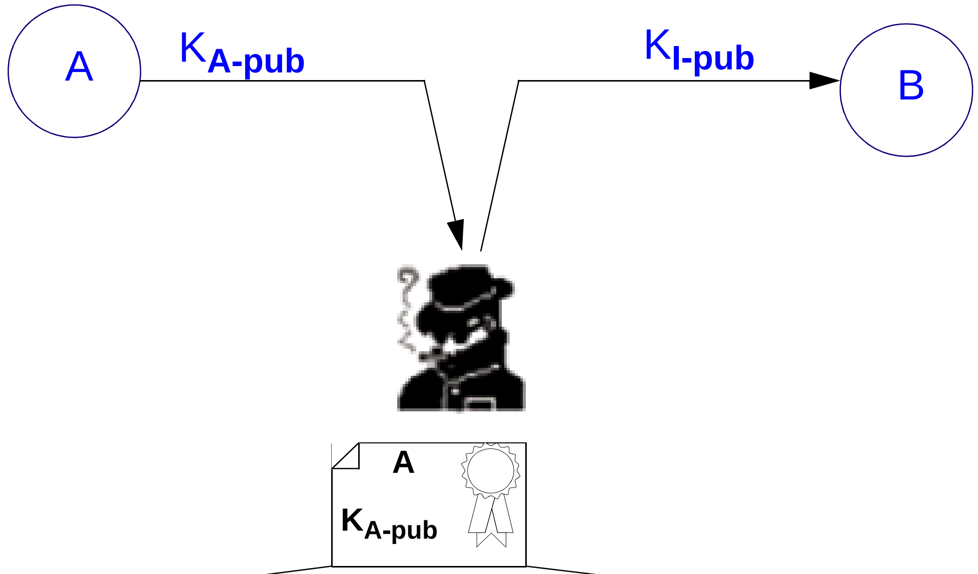
Problem

- **Key distribution in asymmetric procedures "man in the middle attack"**

$\Rightarrow$ **Certificates**

Principle

- **Trustworthy institution signs and allocates a public key to a participant**
- **Public key $K_{Trust\text{-}pub}$ known to the certification issuer**

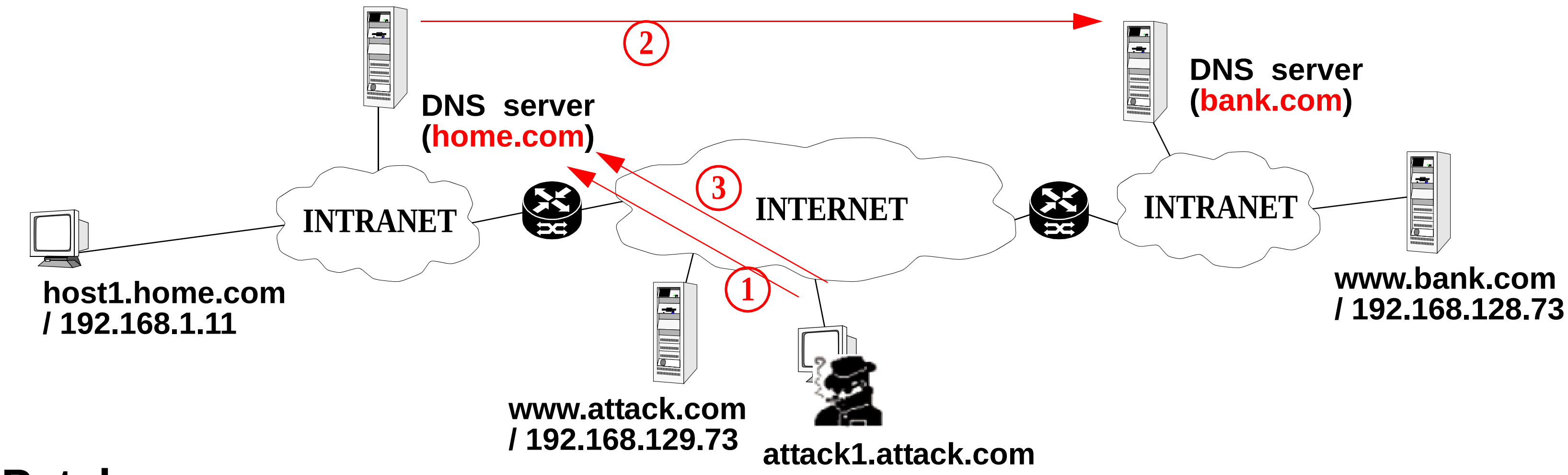


Identity informtion certificate owner	Public key owner of certificate	Identity information cert. issuing entity	Digitale signature
A	$K_{A\text{-}pub}$	Trust	27B25432

2.5 Attack Example

Example: DNS spoofing

"bad case", patched



Patch:

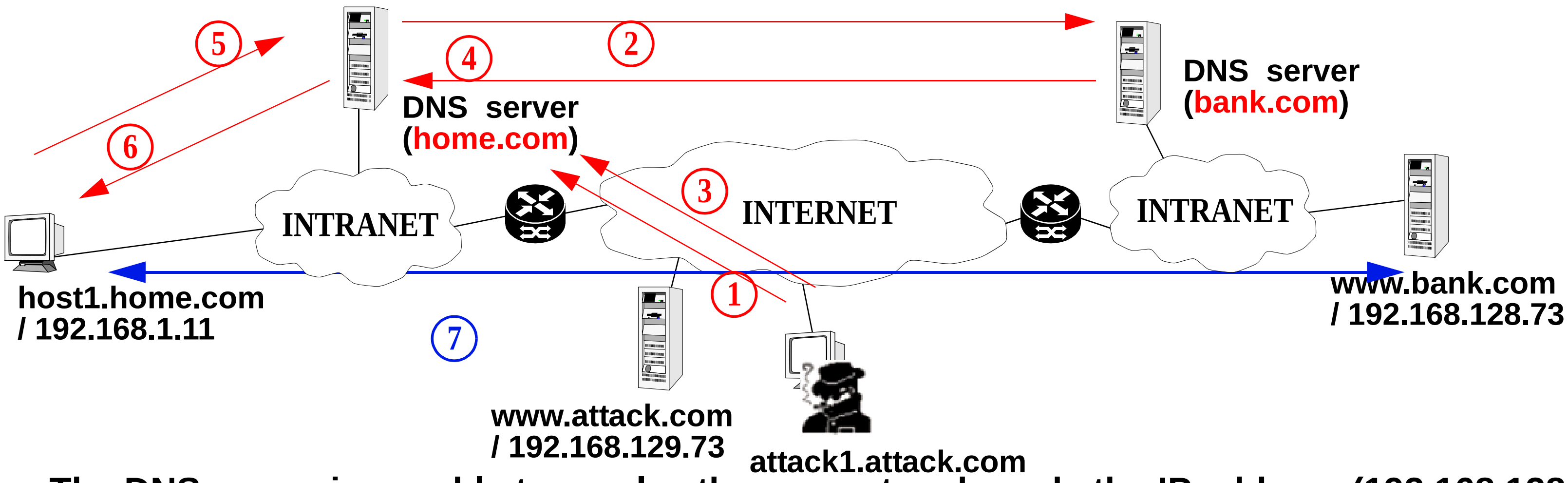
- The DNS servers use digital signatures to sign the messages

1. Attack1 sends a DNS request to the home.com DNS server and asks for the IP address of www.bank.com.
2. The DNS server can not resolve the request and forwards the request to the DNS server of bank.com. Before sending the message it is signed.
3. Attack1 creates a fake DNS packet. The UDP packet uses the source address of the DNS server of bank.com. The information contained in the packet is www.bank.com = 192.168.129.73 (www.attack.com). This information is NOT accepted by the home.com DNS server. The verification of the signature fails because the attacker does not posses the private key of the bank.com DNS server.

Attack Example

Example: DNS spoofing

"bad case", patched



4. The DNS server is capable to resolve the request and sends the IP address (192.168.128.73) back to the requesting DNS server. Before sending the message it is signed. The home.com DNS server checks the signature and stores the answer in the cache.
5. Host1 sends a DNS request to its local DNS server and asks for the IP address of www.bank.com.
6. The home.com DNS server sends the answer to host1.
7. Host1 is now able to communicate with www.bank.com.

Other possible solution:

- The DNS servers use TCP instead of UDP for communication

3. Secure Communication

Communication security can be implemented on different layers

Application Layer	Example: • Secure HTTP (SHTTP) • Secure Shell (SSH)
Transport Layer	Example: • Secure Socket Layer (SSL), • Transport Layer Security (TLS)
Network Layer	Example: • IP Security Protocol (IPSec)
Data Link Layer	Example: • PPTP - Point-to-Point Tunneling Protocol • L2TP - Layer 2 Tunneling Protocol
Physical Layer	Example: • WLAN 802.11 Wired Equivalent Privacy (WEP)

⇒ **Security services of lower layers are transparent to upper layers.**

⇒ **Security services of lower layers need the modification of more network devices**

⇒ **Fulfil all security goals:**
confidentiality, authentication, integrity and non-repudiation

3.1 Security at the Data Link Layer

Principle

- **Data Link Layer is enhanced by encryption/decryption functionality**

Advantages

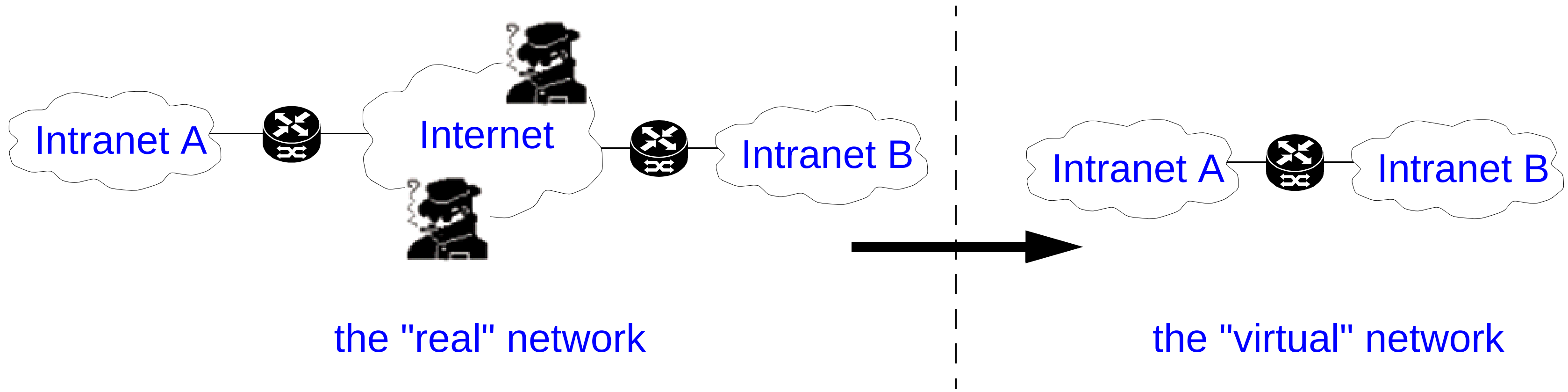
- **The modifications are not**
  - protocol specific
  - application specific

Drawbacks

- **Every host needs the same modification in the Data Link Layer.**
- **In practice: modification of the used operating system**

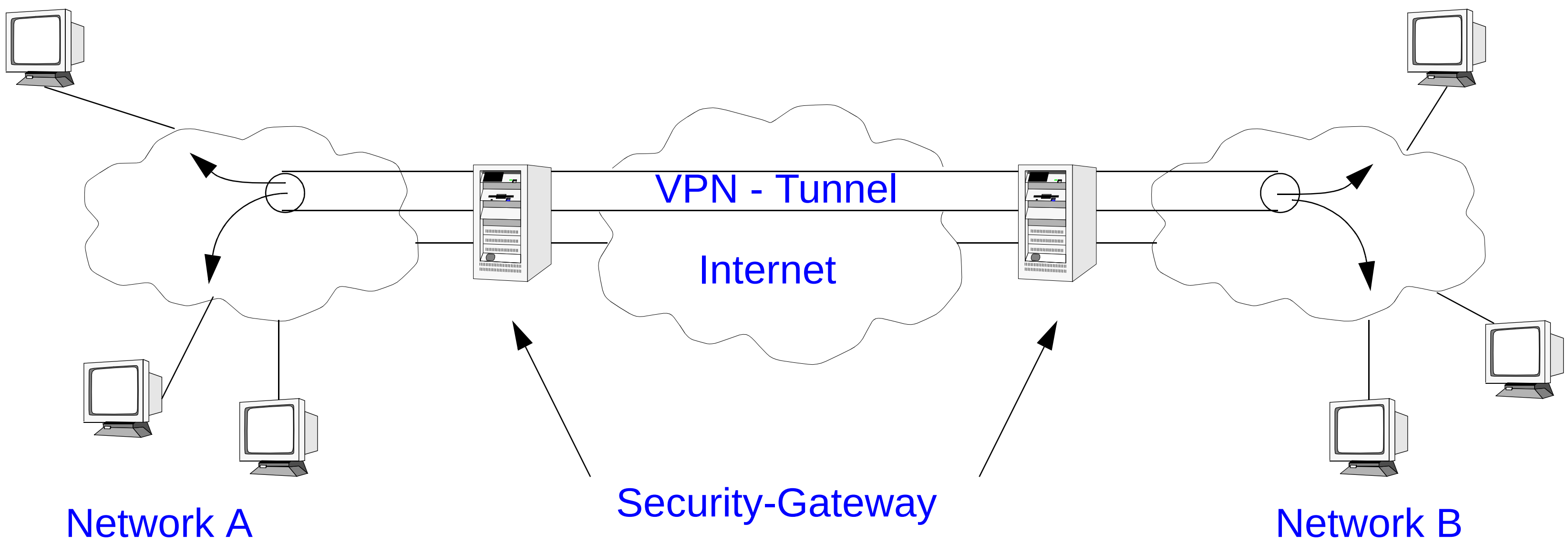
Today used for

- Virtual Private Networks (VPNs), secure dial-in, WLAN



Virtual Private Networks (VPN)

Application of the tunneling principle



Security gateway

- Specialized host (modified operating system)

Clients

- Standard, unmodified hosts

Internet

- Only used as transportation medium

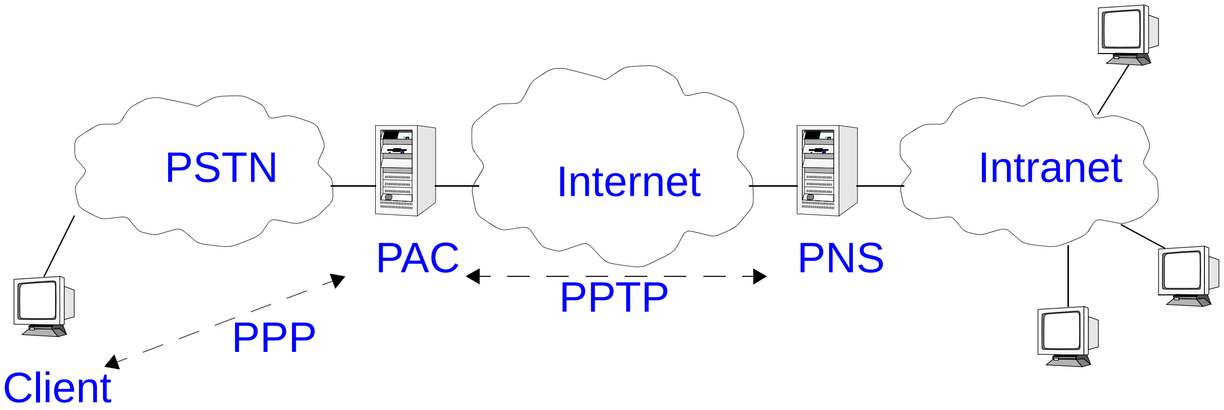
Examples

- PPTP, L2TP

PPTP - Point to Point Tunneling Protocol

History

- Started by Microsoft
- PPTP-Forum



Principle

- Split of a Network Access Server in a client-server architecture.
  PPTP Access Concentrator (PAC) and PPTP Network Server (PNS)
- Transport of the PPP packets over the intermediate IP-Network
- Usage of a TCP control channel and a GRE data channel

IP-Header	TCP	PPTP-Packet	

IP-Header	GRE	PPP	IP-Tunnel-Packet	

Security services

- PPP authentification at session setup
- PPP compression algorithm replaced by an encryption algorithm
- Key distribution not defined in the standard!

3.2 Security at the Network Layer

Principle

- **Network Layer is enhanced by encryption/decryption functionality**
- **Modification of the IP-standard**

Advantages

- **The modifications are not**
  - application specific

Drawbacks

- **Every host needs the same modification in the Network Layer.**
- **In practice: modification of the used operating system (IP-stack)**

Today used for

  - Virtual Private Networks (VPNs)
  - Secure host-to-host communication

Examples

  - IPSec

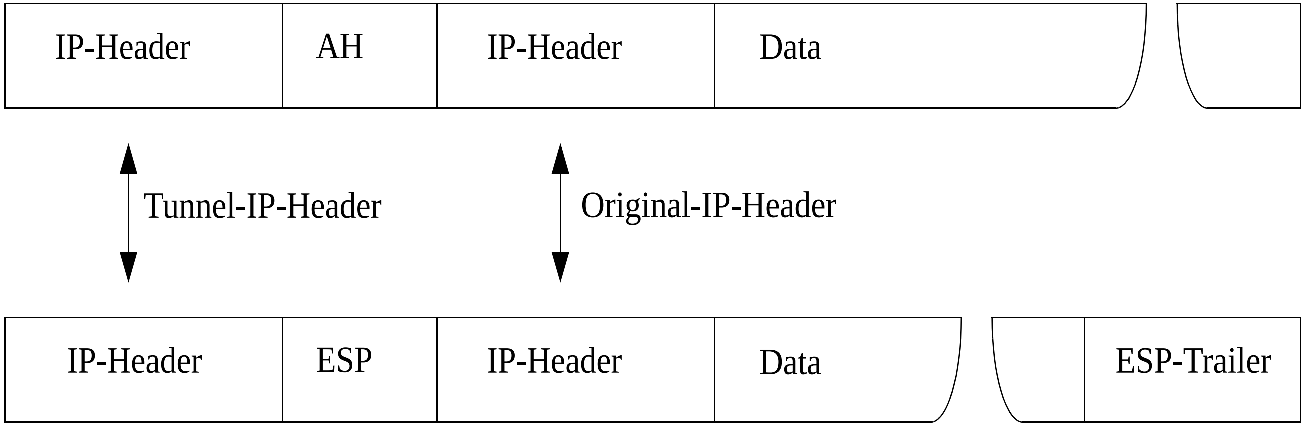
IPSec - IP Security Protocol

History

- **IETF - Working Group**

Principle

- **Separation of security mechanisms and key management**
  - IP Security Protocol: AH and ESP in tunnel or transport mode
  - Internet Key Management Protocol (IKMP): ISAKMP, OAKLEY, ...



Security services

- **Authentication Header (AH): integrity, authentication**
- **Encapsulating Security Payload (ESP): integrity, authentication, confidentiality**
- **AH and ESP can be combined**

3.3 Security at Transport Layer

Principle

- **Transport Layer is enhanced by encryption/decryption functionality**
- **Modification of the socket API**

Advantages

- **The modifications are not**
  - application specific .... but in practice they are
    (modification is between application and transport layer; modification is part of the application code, not part of the operating system)

Drawbacks

- **Modification has to be performed for each application**

Today used for

- Various applications: e.g. mail clients/server, www browser/server
- Secure application-to-application communication

Examples

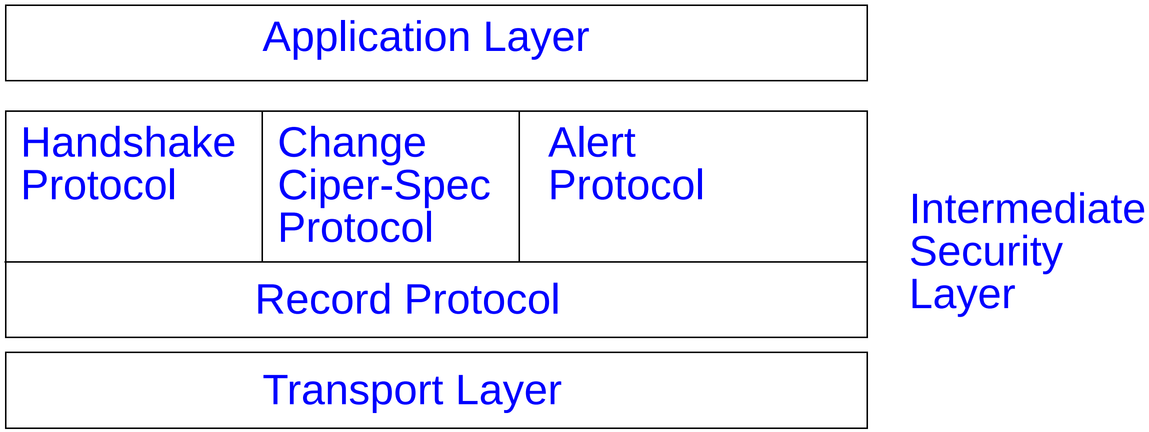
- SSL, TLS

SSL - Secure Socket Layer

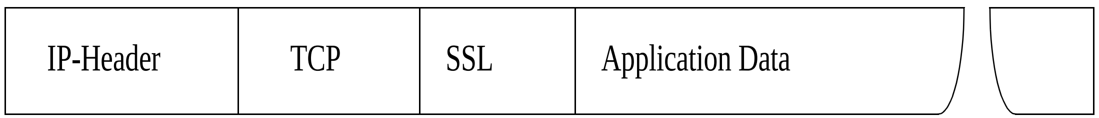
History

- **Netscape, IETF**

Principle



- **Handshake Protocol: session setup**
- **Change Ciper-Spec Protocol: key negotiation**
- **Alert Protocol: error handling**
- **Record Protocol: encryption/decryption**



Security services

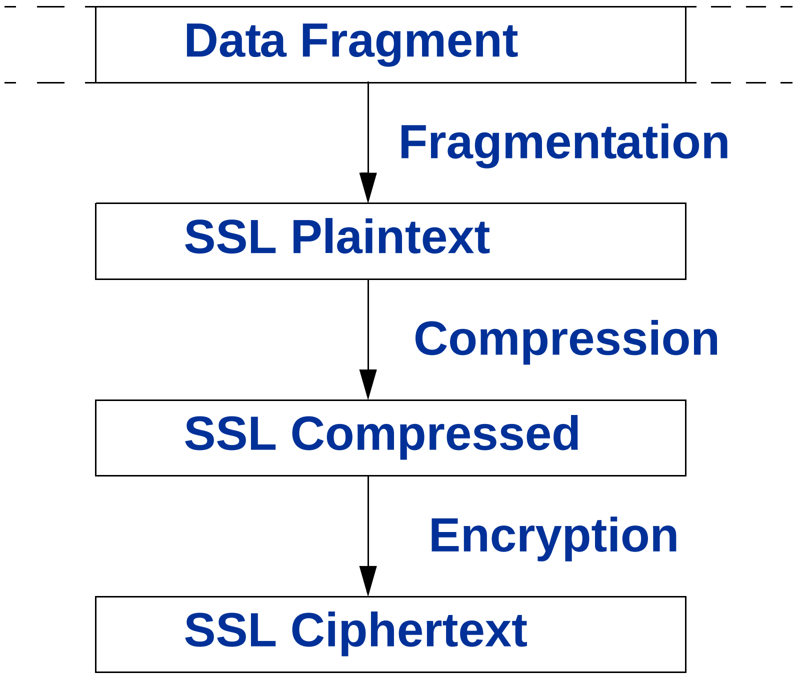
- **Integrity, authentication, confidentiality**

www.kom.tu-darmstadt.de
www.httc.de

SSL Record Protocol

Principle

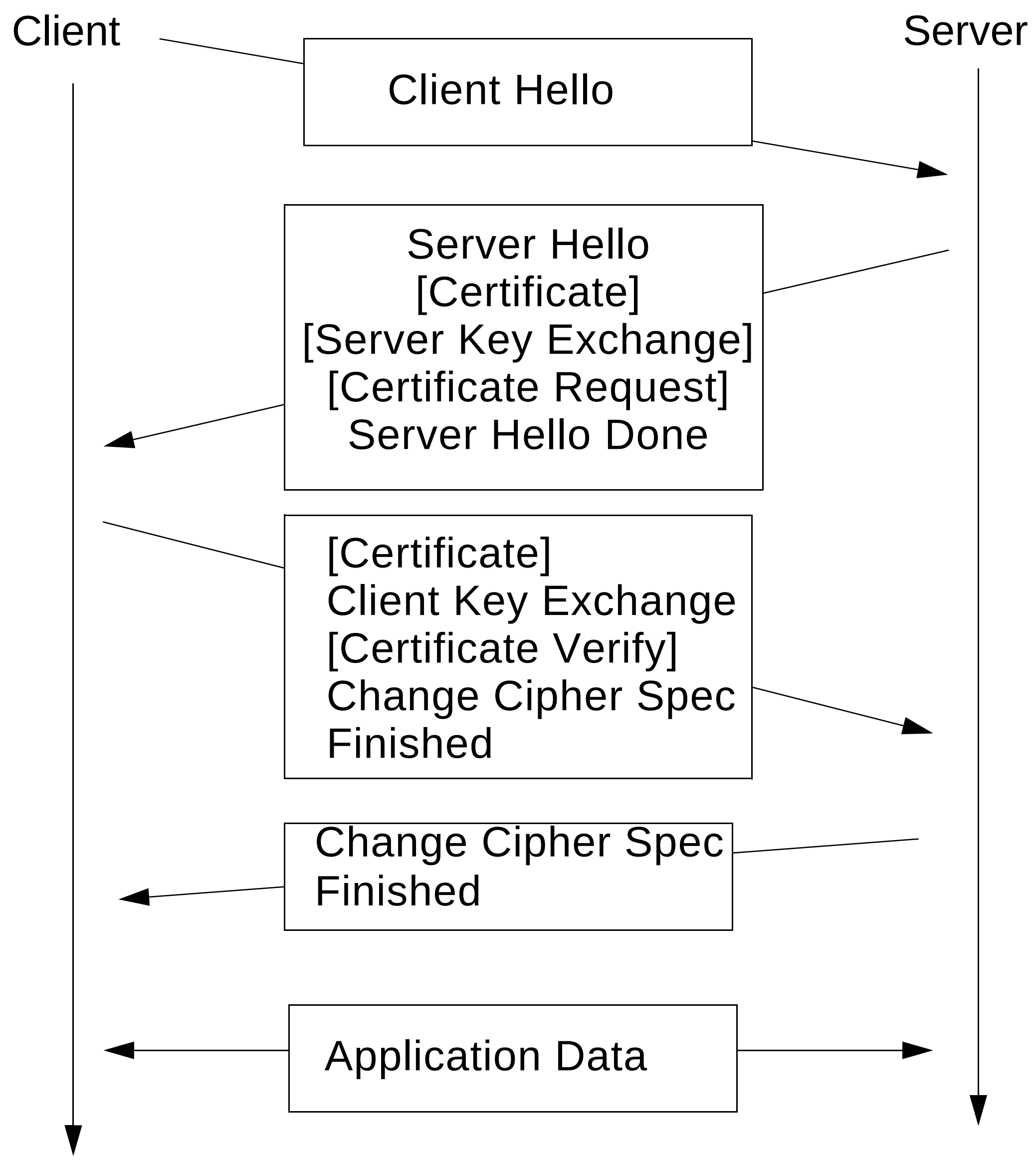
1. **Fragmenting**
   - A message can be split in many packets
2. **Compression**
   - To reduce traffic, a compression algorithm is used.
3. **Encryption**
   - Usage of algorithm/keys negotiated by the Ciper-Spec Protocol



SSL Handshake Protocol

Principle

- **Used during session setup**
- **Negotiation of protocol version**
- **Negotiation of cryptographic algorithms**
- **Bilateral authentication**
- **Negotiation of session keys**



3.4 Security at Application Layer

Principle

- **Application Layer is enhanced by encryption/decryption functionality**
- **Modification of a specific application**

Advantages

- **The modifications can be implemented very easy**

Drawbacks

- **Modification has to be performed for each application**

Today used for

- Various applications: e.g. mail, www browser/server
- Secure application-to-application communication

Examples

- Pretty Good Privacy (PGP), Secure HTTP (S-HTTP), ...

Pretty Good Privacy (PGP)

History

- Developed by Philip Zimmermann to be used within: Electronic Mail

Principle

- Freely available international version for various platforms
- Combination of:
  - Internationally recognized cryptographical algorithms (RSA, IDEA, MD-5)
  - Key management procedures (key signing, Web of Trust)
  - Compression processes (PKZIP)
  - Transfer encoding for electronic mail and capability for self description

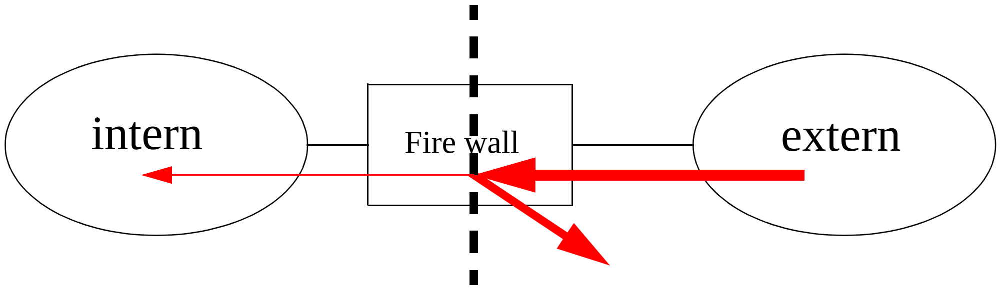
Security services

- Confidentiality is ensured through symmetric encoding of the complete message by session key, and its protection by the recipient's public key
- Signing messages (authentication and impossibility to deny the place of origin) by using one's own private key for message digest
- Combining several / all procedures
- Key for conventional encryption can be chosen freely

4. Network Access Control - Firewalls

Firewall charateristics

- System located between different (Internet - Intranet) networks
- Complete data traffic between the networks has to pass the firewall
- Only authenticated traffic can pass the firewall
- Firewall has to be secured



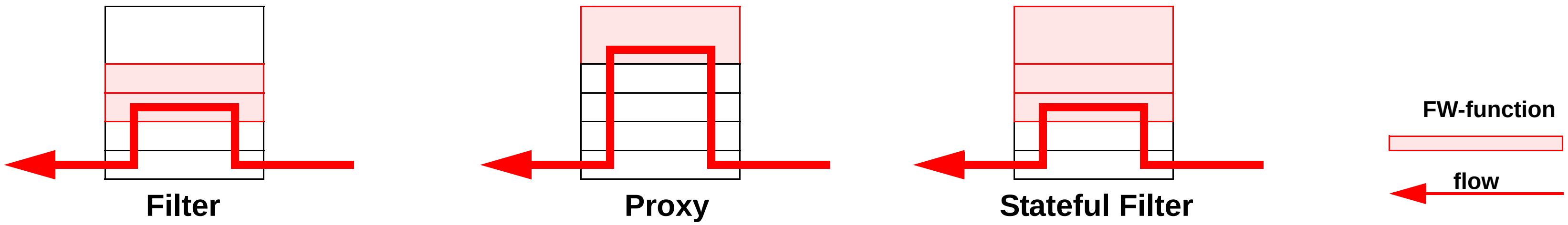
Firewall Functions

- Permit/deny dedicated data flows
- Assignment of dedicated data flows to users/systems
- Hiding internal structures (e.g. NAT)
- Monitoring, logging and alerting

Firewalls

Firewall components

- Filters
- Proxies
- Stateful Filters



Firewall architectures

- DMZ
- Inbound Filters
- Dual homed Gateway

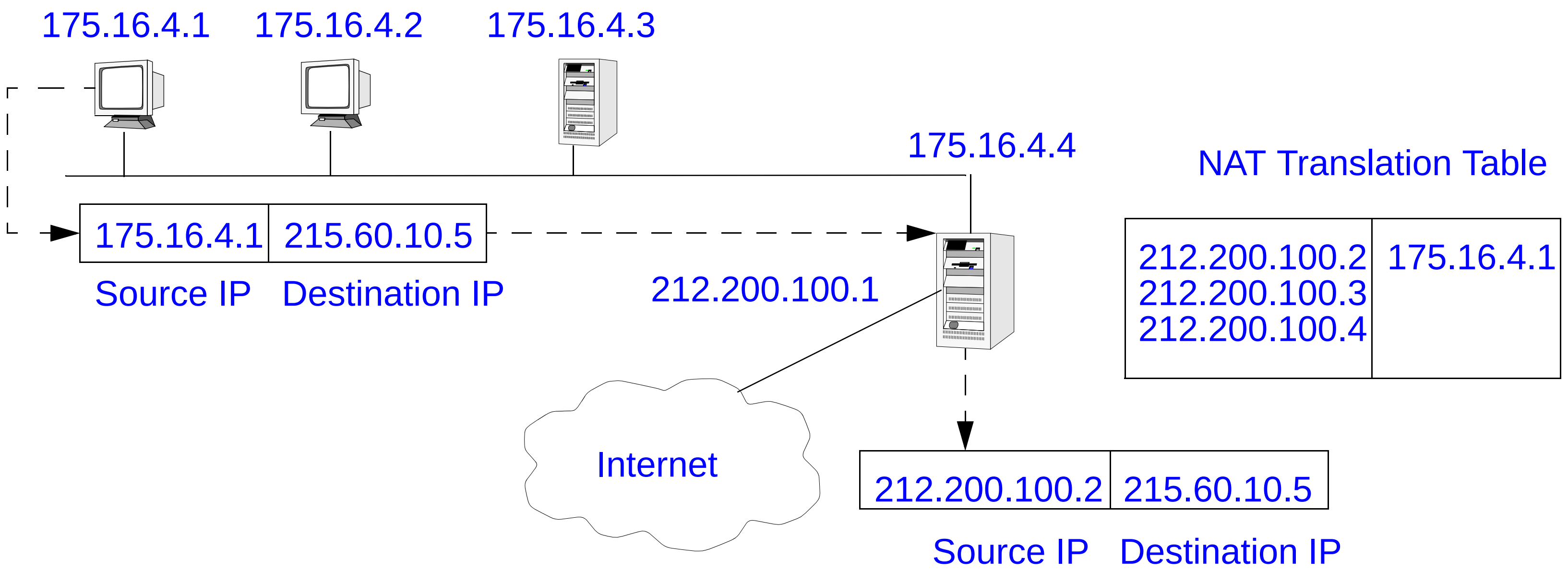
Problems

- Insider attacks
- Tunneling of IP packets
- Using alternative insecure network connections (modems...)
- Firewall configuration (esp. for multimedia applications)

Network Address Translation

Goals

- **Conceal the existence of different hosts in the Intranet**
- **Conceal the IP addresses of hosts in the Intranet**
- **Using private IP addresses that can not be routed on the Internet**
- **Load balancing**



Network Address Translation (2)

Router functions

- Changing IP addresses
- Recalculating IP header checksum
- Recalculating TCP header checksum
- Updating TTL

Network Address Port Translation

- Changing TCP Ports also
- Allows the usage of only one IP address

NAT Problems

- Encryption of header fields (e.g. IPsecurity)
- Applications with end-to-end significance of IP addresses
  - IP Telefonie (H.323 / SIP)
  - Multiplayer games

5. Conclusion

Summary

- Security goals, attackers and attacks
- Cryptographical methods
- Selected security mechanisms and there implementation

⇒ Only a small subset of security mechanisms and implementations has been shown!

To remember

- For distributed services security is an extremely important factor (necessary for the (financial) success of a service)
- Good protection mechanisms already exist
  (use existing building blocks; do not re-invent parts)
- The security of a system has to be monitored

Additional Readings

Additional information:

e.g.,

- **Stephan Fischer, Achim Steinacker, Reinhard Bertram, Ralf Steinmetz, Open Security: Von den Grundlagen zu den Anwendungen, Springer Verlag, Berlin Heidelberg 1998**
- **Schumacher, M., Roedig, U., Moschgath, M.-L., Hacker Contest: Sicherheitsprobleme, Lösungen, Beispiele´, Springer-Verlag 2003**