Information & Communication Security (SS 2020)

Network Security I
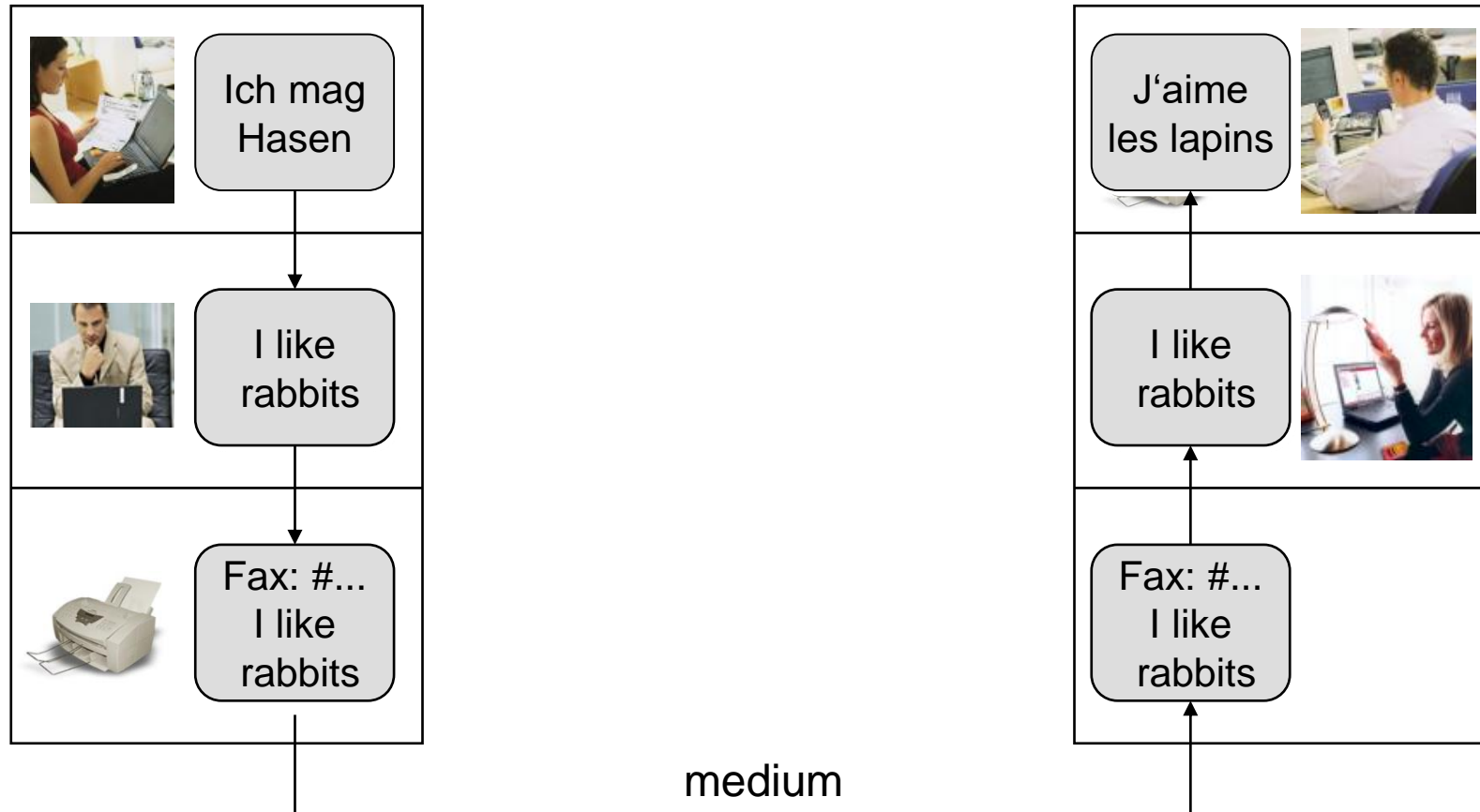
Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Agenda

- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
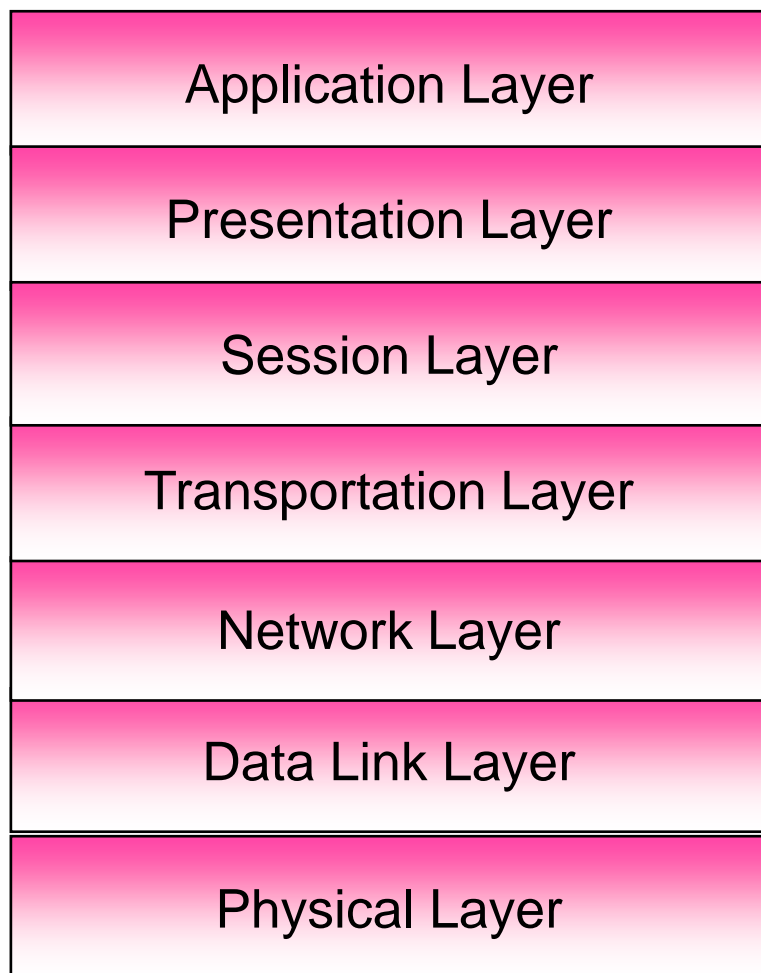- Wireless / Mobile Security

Agenda

- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security

- **Network security** is the **control of** unwanted intrusion, misuse, modification, damage or denial of a computer network and network-accessible resources. [Ba10]

- Network security is the process of taking physical and software preventative measures to protect the networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. [SANS]
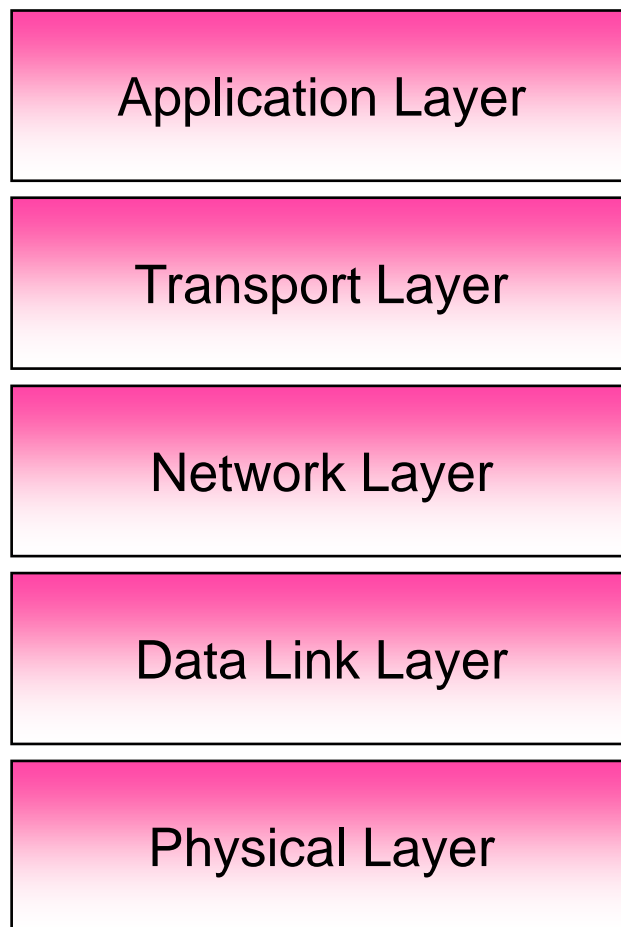
Layered Communication

[Based on Tan96]

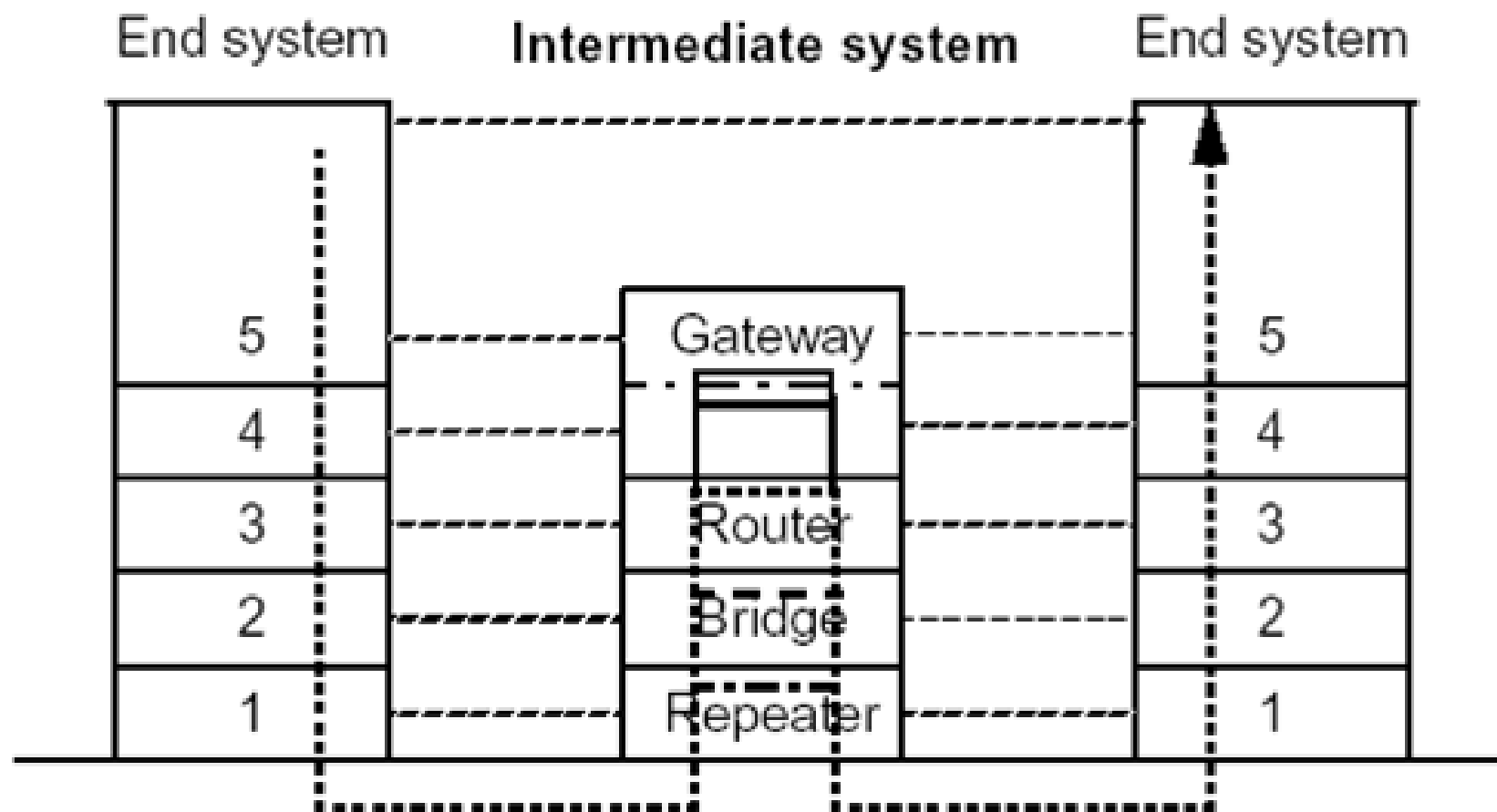| Application Layer |
|---|
| Presentation Layer |
| Session Layer |
| Transportation Layer |
| Network Layer |
| Data Link Layer |
| Physical Layer |

- Information technology — Open Systems Interconnection — Basic Reference Model
- 7-Layer-Model
  - First version ISO/IEC 7498-1:1984
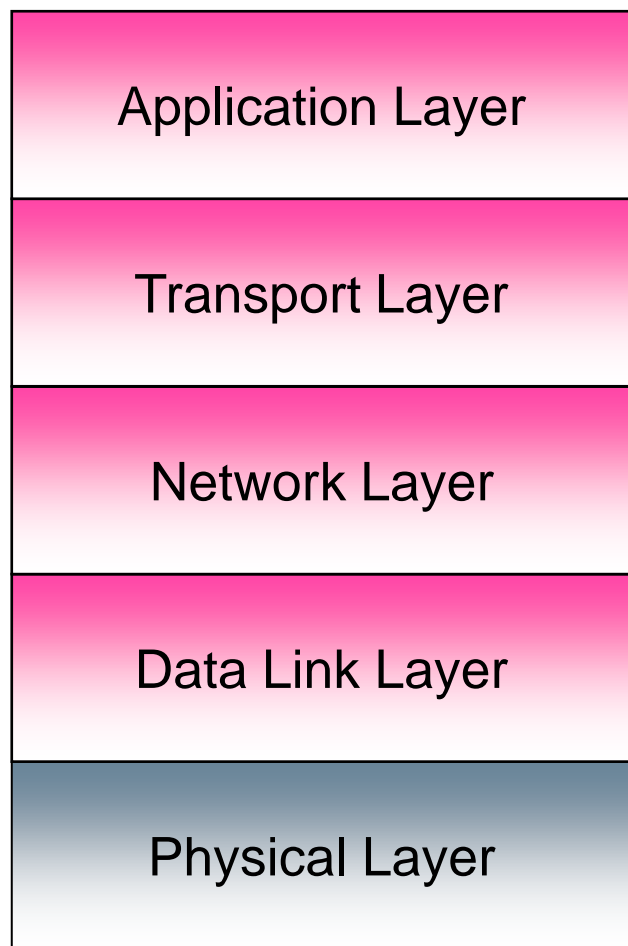 - Current version ISO/IEC 7498-1:1994

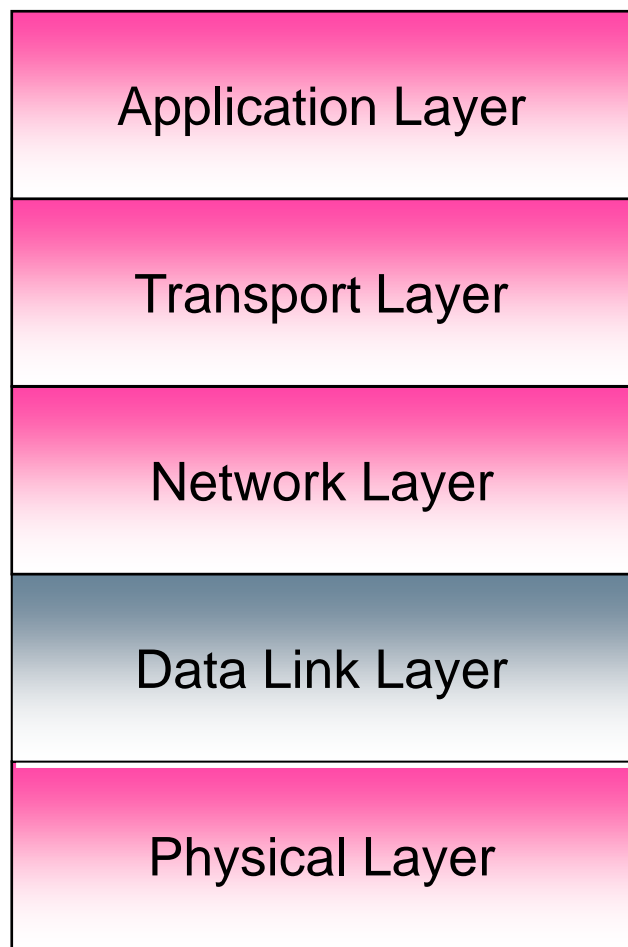   Corrected: 1996

Internet Reference Model

Application Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

[Based on Tan96]

Communication Example

[Based on Tan96]

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Tasks:
- Bit transfer
- Mechanic (connector, medium)
- Electronic (signal durability of a bit, voltage)

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Tasks:
- data transmission between stations in the direct neighbourhood
- error detection and elimination
- flow control
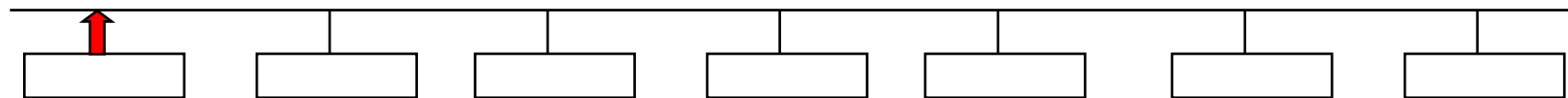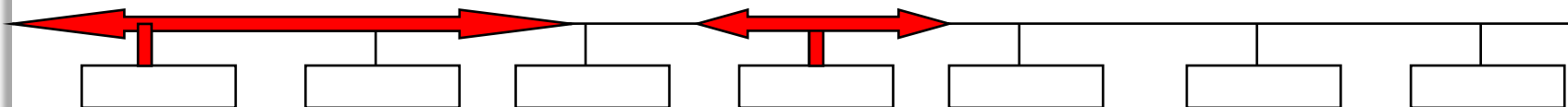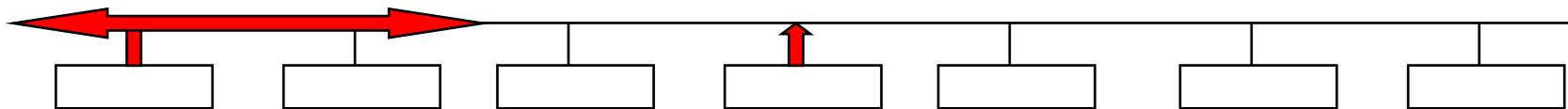- Medium access control (MAC)

Bus-Network
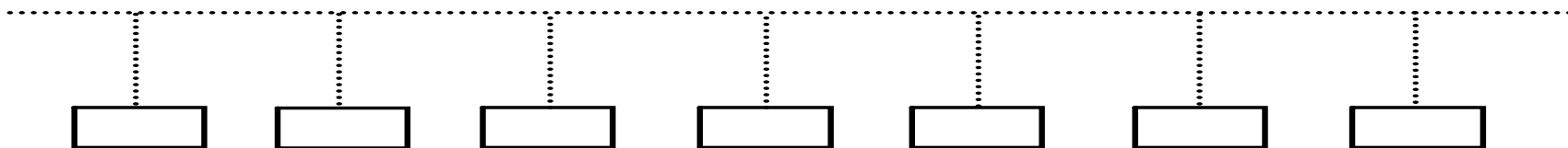
- Developed by XEROX
- Additional nodes can easily be added.
- Protocol: Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

CSMA/CD:

Carrier Sense:

Multiple Access:

Collision Detection:

Frame Sniffing
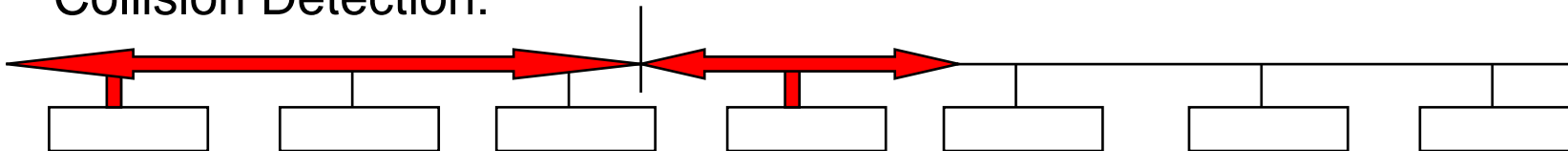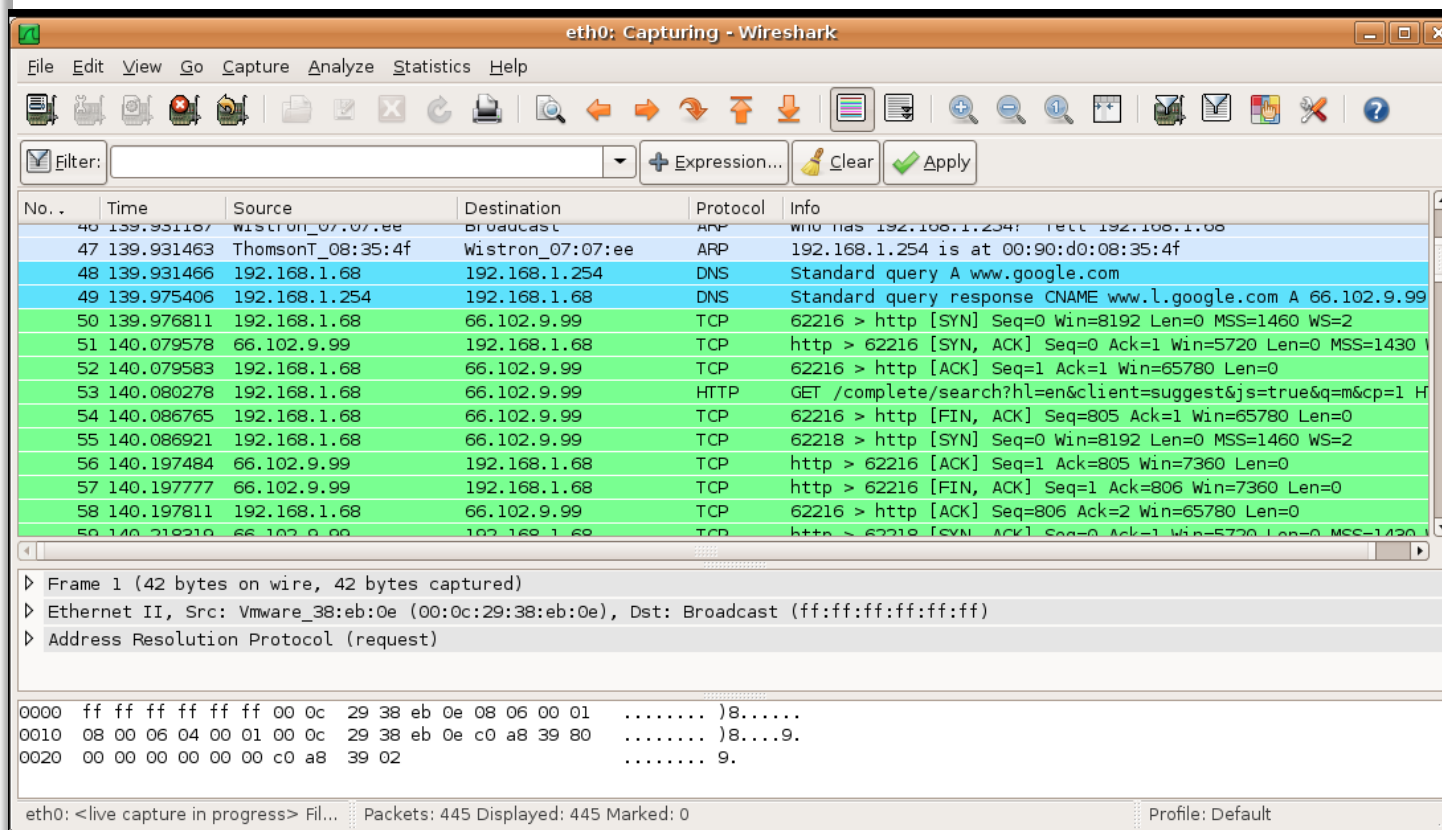
Eavesdropping of frames
i.e. Wireshark:

Meta-data of packets of higher protocol layers

[Based on Wireshark]

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
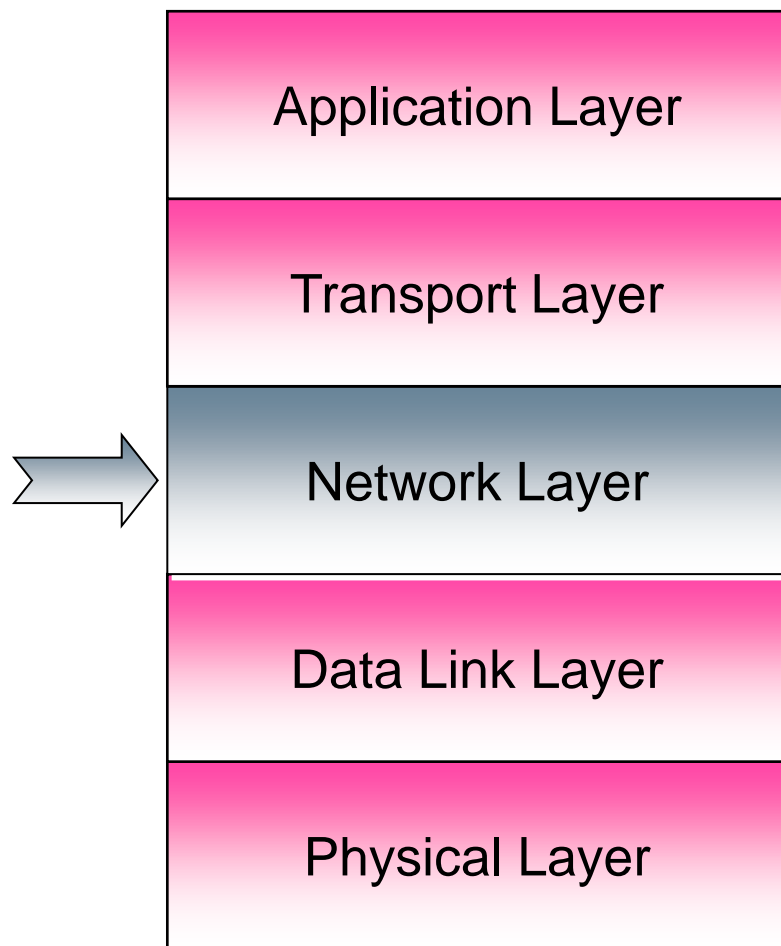
Tasks:
- End-to-end connections between systems
- Routing
- Addressing
- Typically connectionless

For example: IP

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
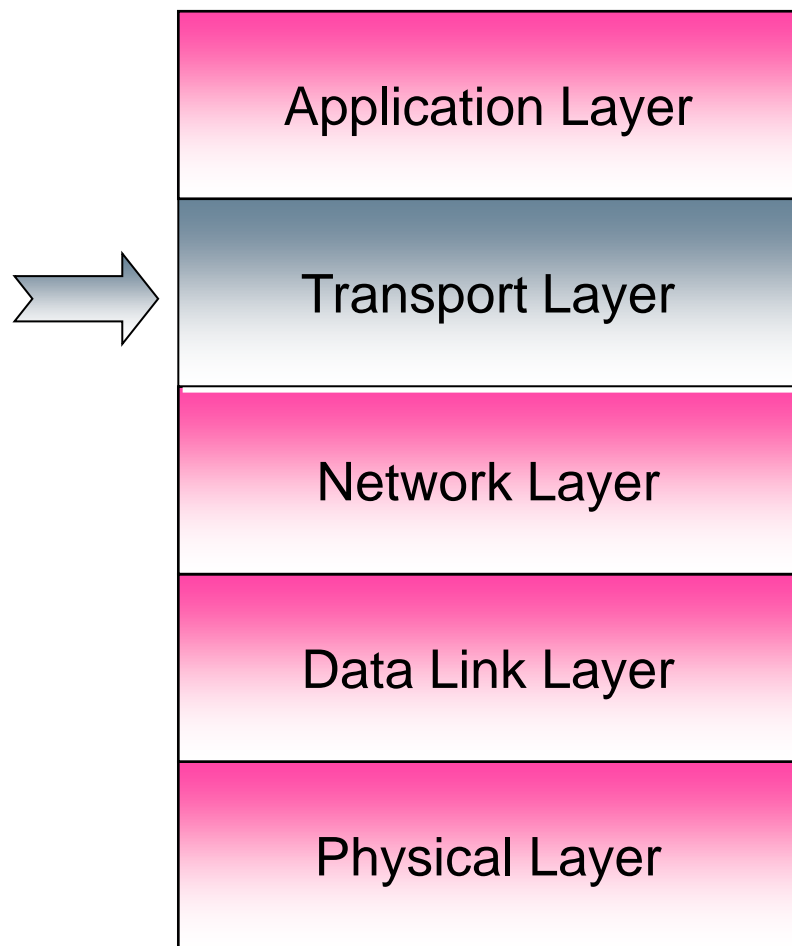
Tasks:
- Connection between source and target
- Optimisation of quality of service and service costs
- Flow control
- Connection management

For example: TCP, UDP

Application Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
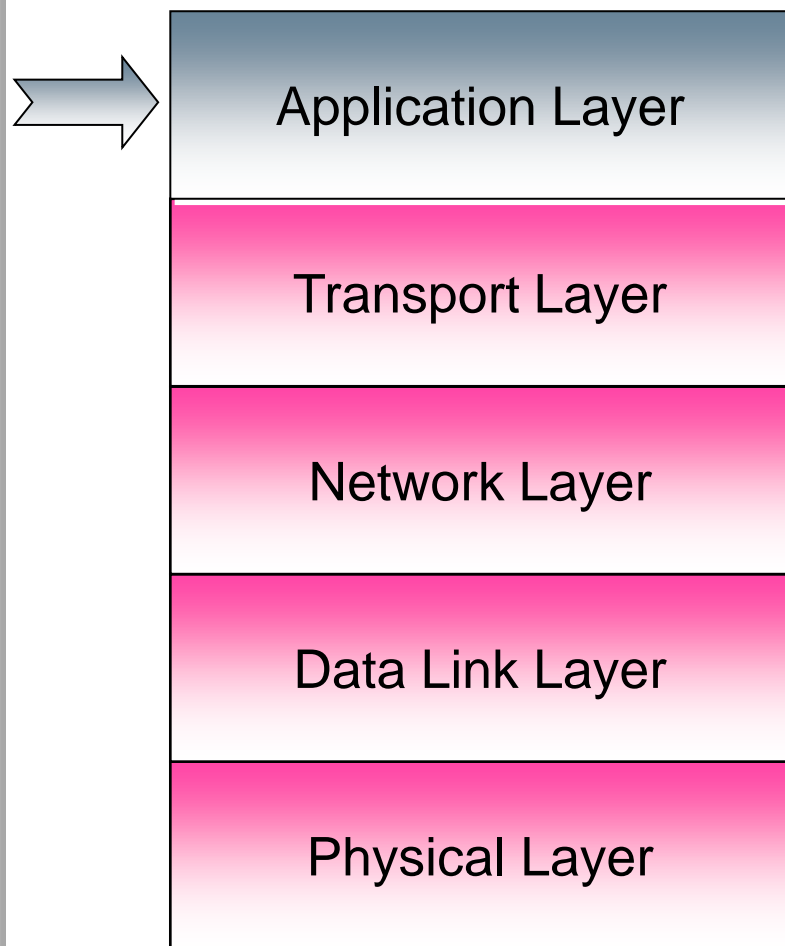
Tasks:

- provides services to the user/applications
- Examples (service/protocol): E-Mail / SMTP, WWW / HTTP, file transfer / FTP

SMTP: Simple Mail Transfer Protocol

HTTP: Hyper Text Transfer Protocol

FTP: File Transfer Protocol

Agenda

- Introduction
- Infrastructure Security Components
    - Firewalls
    - Demilitarized Zone
    - Intrusion Detection
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security

- Introduction
- Infrastructure Security Components
    - Firewalls
    - Demilitarized Zone
    - Intrusion Detection
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security

- „A firewall is an internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be *inside* the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be *outside* the firewall)." [RFC 2828]

Private local network

Firewall

Internet
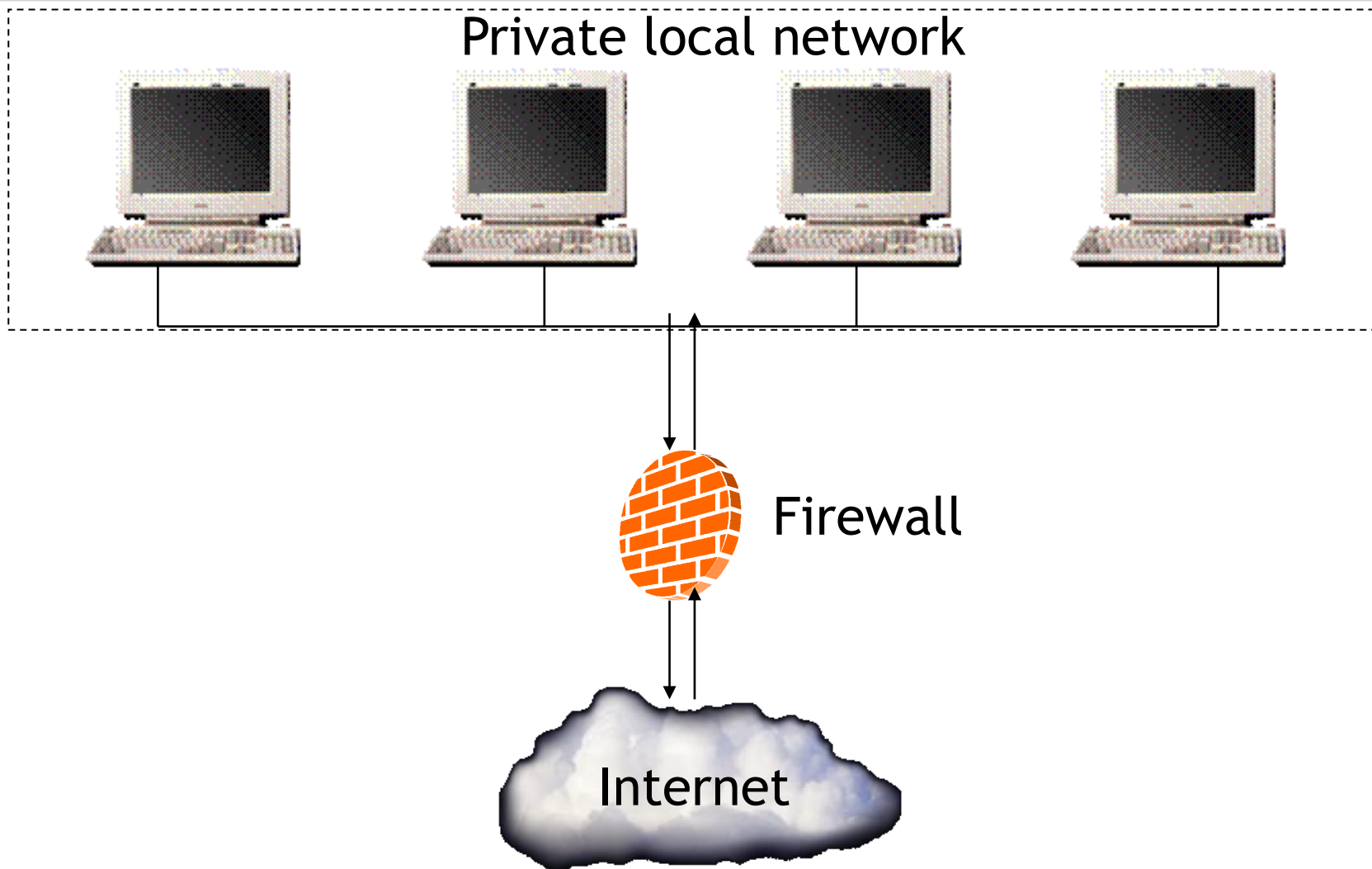
- Filtering firewall: perform access control on the basis of attributes of the packet headers.

- Application-level firewall (proxy firewall): uses proxies to perform access control. A proxy firewall adds to a filtering firewall the ability to base access on content.

[Based on Bi05]

Agenda

- Introduction
- Infrastructure Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security

Demilitarized Zone (DMZ)

- The DMZ is a portion of a network, that separates a purely internal network from an external network. [Bi05]
- The "outer firewall" sits between the Internet and the internal network.
- The DMZ provides limited public access to various servers.
- The "inner firewall" sits between the DMZ and the subnets not to be accessed by the public.
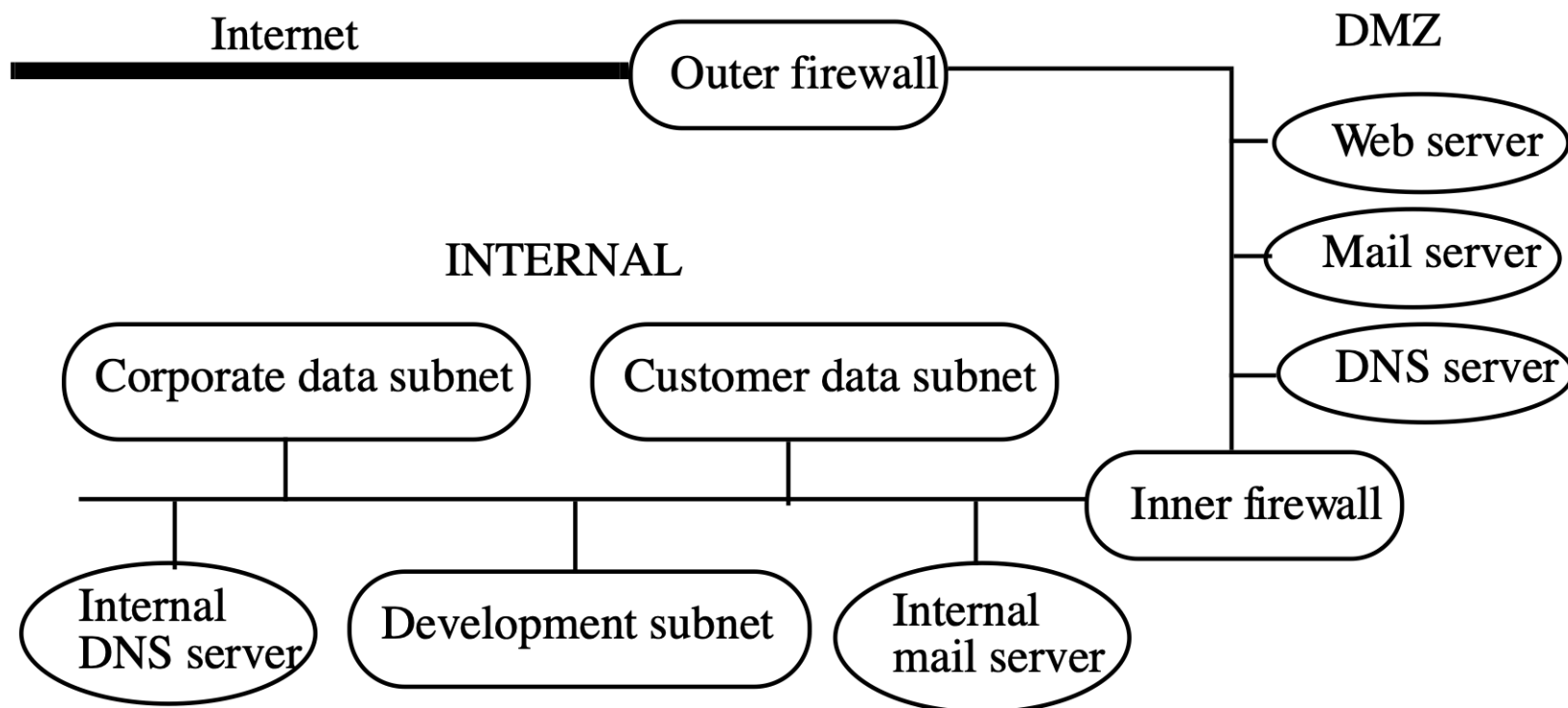
Internet — Outer firewall

DMZ
- Web server
- Mail server
- DNS server

INTERNAL

Corporate data subnet — Customer data subnet

Inner firewall

Internal DNS server — Development subnet — Internal mail server

[Based on Bi05]

Browser

HTTP(S) HTML

DMZ

Web Application Server - Corporate Access Point

JAAS

Mapping Service

App

HTTP(S) HTML

Security Module

Challenge Provider

Information Provider System

R/3

RFC/SNC

DB
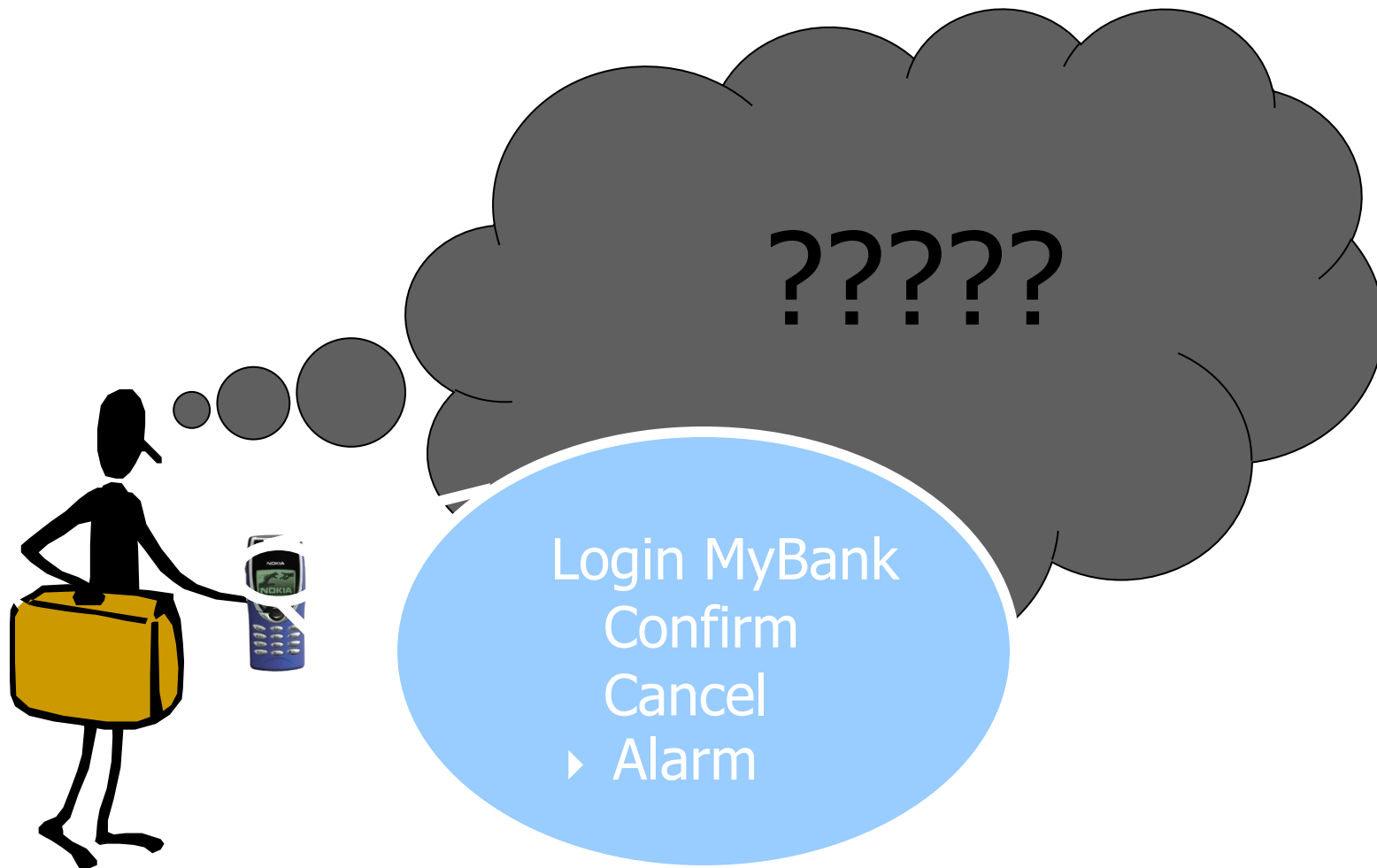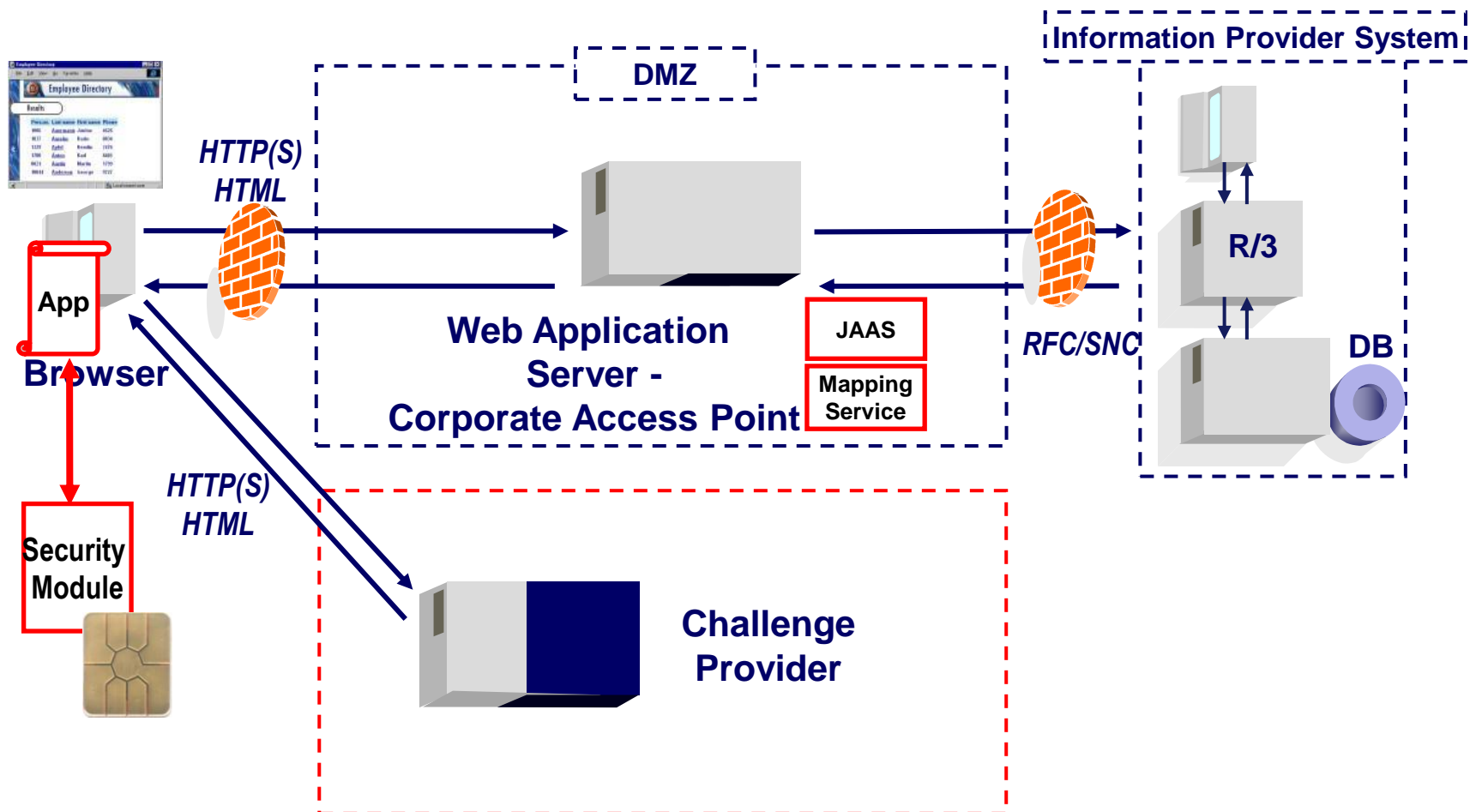
JAAS = Java Authentication and Authorization Service

- Introduction
- Infrastructure Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security

Computer System Characteristics

Computer systems that are not under attack exhibit several characteristics [Bi05]:

(1) The actions of users and processes generally conform to a statistically predictable pattern. A user who does only word processing when using the computer is unlikely to perform a system maintenance function.

(2) The actions of users and processes do not include sequences of commands to subvert the security policy of the system. In theory, any such sequence is excluded; in practice, only sequences known to subvert the system can be detected.

(3) The actions of processes conform to a set of specifications describing actions that the processes are allowed to do (or not allowed to do).

Denning [De87] hypothesized that systems under attack fail to meet at least one of these characteristics.

- An *attack tool* is an automated script designed to violate a security policy.

- Example: *Rootkits*
  - Exist for many versions of operating systems, i.e. Unix (but not only).
  - Can be designed to sniff passwords from the network and to conceal their presence.
  - Include tools to automate the installation procedure and has modified versions of system utilities.
  - Installer is assumed to have *root* privileges (hence the name - *root*kit).
  - Can eliminate many errors arising from incorrect installation and perform routine steps to clean up detritus of the attack.

[Based on Bi05]

- Detect a wide variety of intrusions:
  - Inside and outside attacks
  - Known and previously unknown attacks should be detected.
  - Adapt to new kinds of attacks
- Detect intrusions in a timely fashion
- Present the analysis in a simple, easy to understand format
- Be accurate:
  - False positives reduce confidence in the correctness of the results.
  - False negatives are even worse, since the purpose of an IDS is to report attacks.

[Based on Bi05]

- *Anomaly detection* analyzes a set of characteristics of the system and compares their behavior with a set of expected values.

- It reports when the computed statistics do not match the expected measurements.

[Based on Bi05]

- *Misuse detection* determines whether a sequence of instructions being executed is known to violate the site security policy being executed. If so, it reports a potential intrusion.

- Example: *Network Flight Recorder (NFR)*

[Based on Bi05]

Network Flight Recorder (NFR)

- NFR has three components:
  - The *packet sucker* reads packets off the network.
  - The *decision engine* uses filters written in a language called N-code to extract information.
  - The *backend* writes the data generated by the filters to disk.

[Based on Bi05]

- *Specification-based detection* determines whether or not a sequence of instructions violates a specification of how a program, or system, should execute. If so, it reports a potential intrusion.

- Example threat source to be controlled: *The Unix program rdist* (Rdist is a program to maintain identical copies of files over multiple hosts.)

[Based on Bi05]

- An *autonomous agent* is a process that can act independently of the system of which it is a part.

- Example: *The Autonomous Agents for Intrusion Detection (AAFID)*

[Based on Bi05]

Intrusion Detection System

Agent

A

Agent

B

Agent

N

Agent

C

Director

Notifier
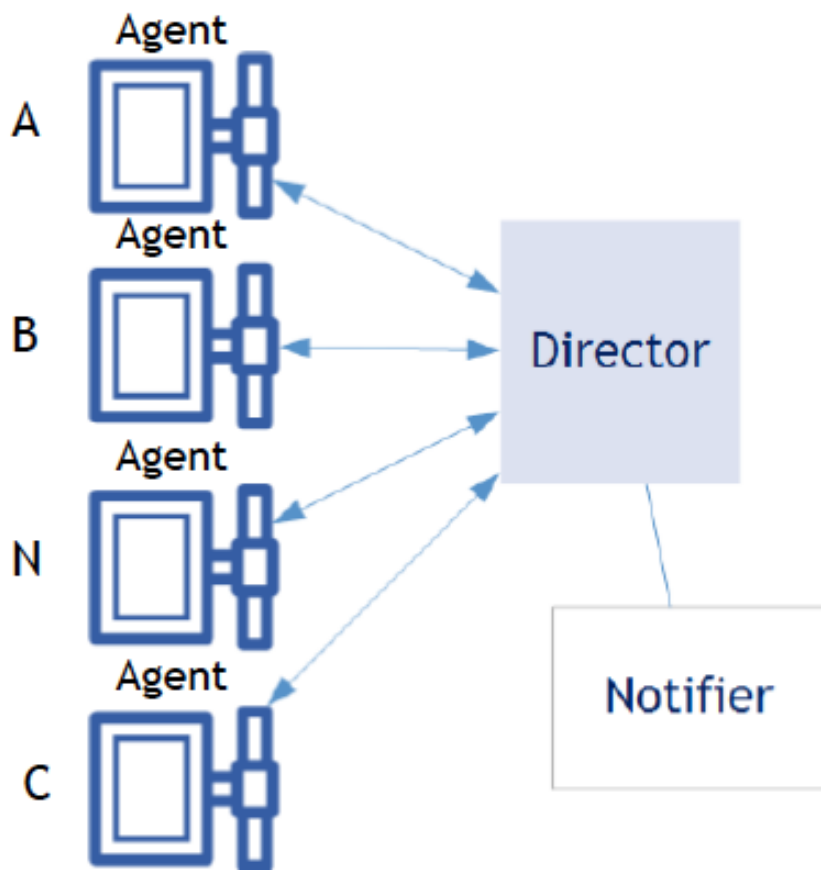
[Bi05]

- Host-based IDS: looks for attack signatures in log files of hosts
- Network-based IDS: looks for attack signatures in network traffic
- Honeypots

[Honeypot]

- **Introduction**
- **Infrastructure Security Components**
  - **Firewalls**
  - **Demilitarized Zone**
  - **Intrusion Detection**
- **Security Protocols**
  - **Virtual Private Networks**
  - **Secure Socket Layer**
  - **IPsec**
- **Application Layer Security**
- **Wireless / Mobile Security**

- **Introduction**
- **Infrastructure Security Components**
    - Firewalls
    - Demilitarized Zone
    - Intrusion Detection
- **Security Protocols**
    - Virtual Private Networks
    - Secure Socket Layer
    - IPsec
- **Application Layer Security**
- **Wireless / Mobile Security**

- A VPN is a mechanism to establish a remote access connection across an intermediary network.

- A VPN uses tunneling or encapsulation protocols. In many cases, the tunneling protocol employs encryption.

[Based on Ba10]

Router

| HTTP/ FTP/... |
| TCP |
| IP |
| Ethernet |

| IP |
| Ethernet |

| HTTP/ FTP/... |
| TCP |
| IP |
| Ethernet |

[Based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Virtual Tunnel

Router

| HTTP/ FTP/... |
| TCP |
| IP |
| Ethernet |

| Tunnelling Protocol |
| UDP |
| IP |
| Ethernet |

| IP |
| Ethernet |

| Tunnelling Protocol |
| UDP |
| IP |
| Ethernet |

| HTTP/ FTP/... |
| TCP |
| IP |
| Ethernet |

Local Network   **Internet**   **Local Network**

[Based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]
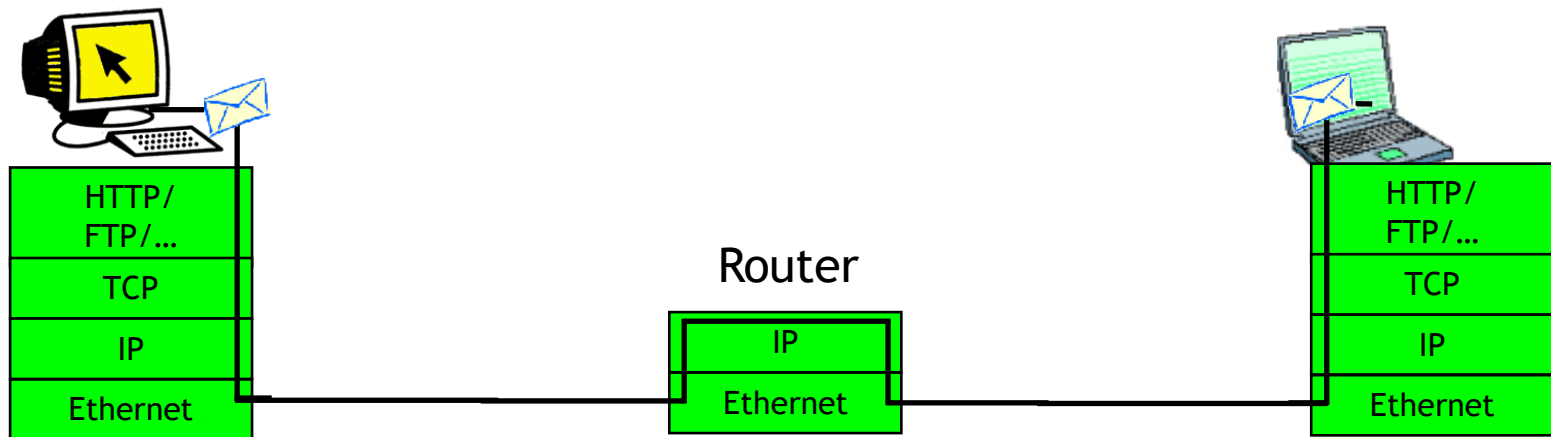
- **Introduction**
- **Infrastructure Security Components**
  - **Firewalls**
  - **Demilitarized Zone**
  - **Intrusion Detection**
- **Security Protocols**
  - **Virtual Private Networks**
  - **Secure Socket Layer**
  - **IPsec**
- **Application Layer Security**
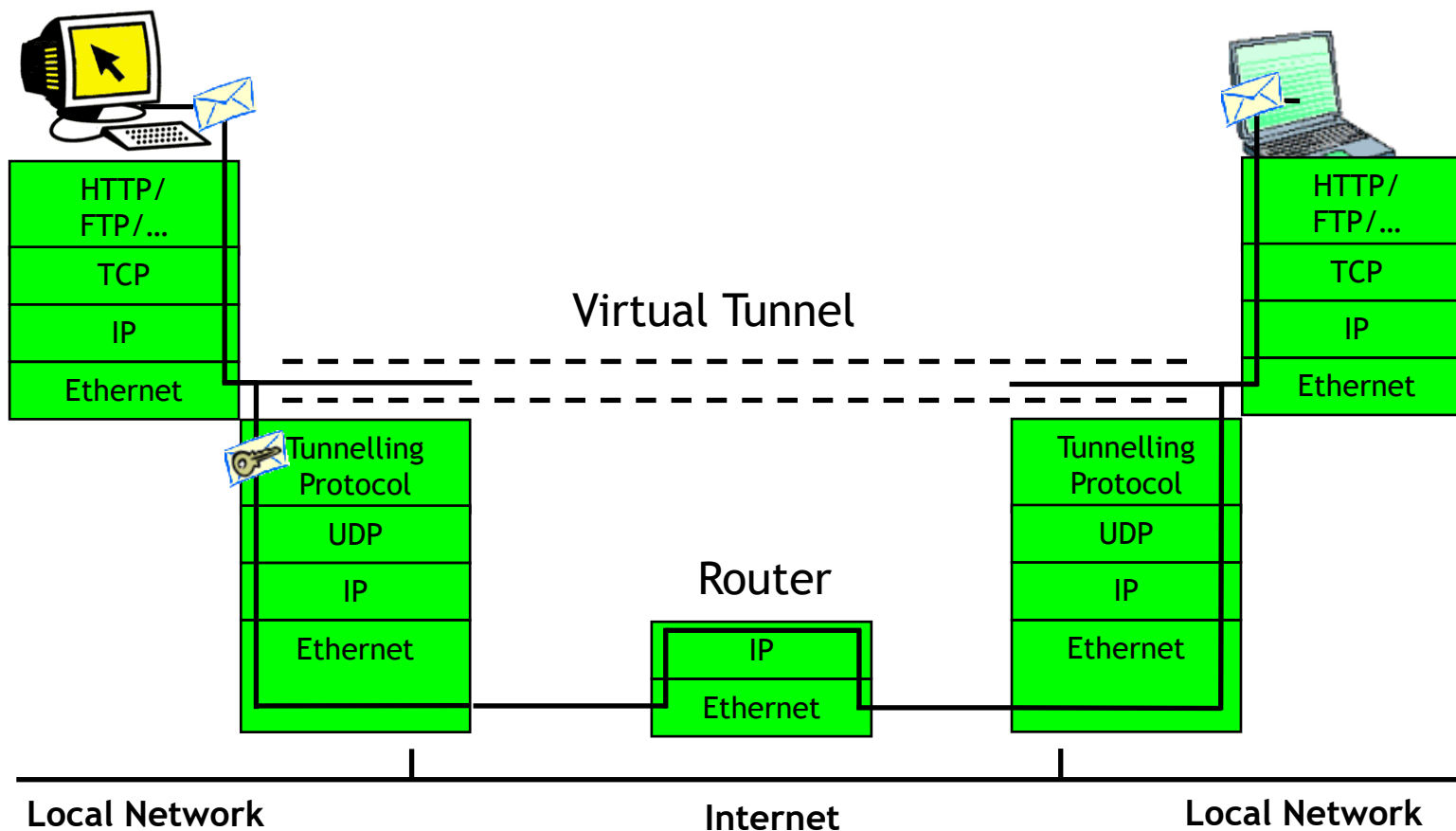- **Wireless / Mobile Security**

www.my-bank.de/Kontostand.html

Actions of the browser:
1. DNS-Request
2. http-Request

DNS server

142.254.112.17

www.my-bank.de
get Kontostand.html

142.254.
112.17

[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

43
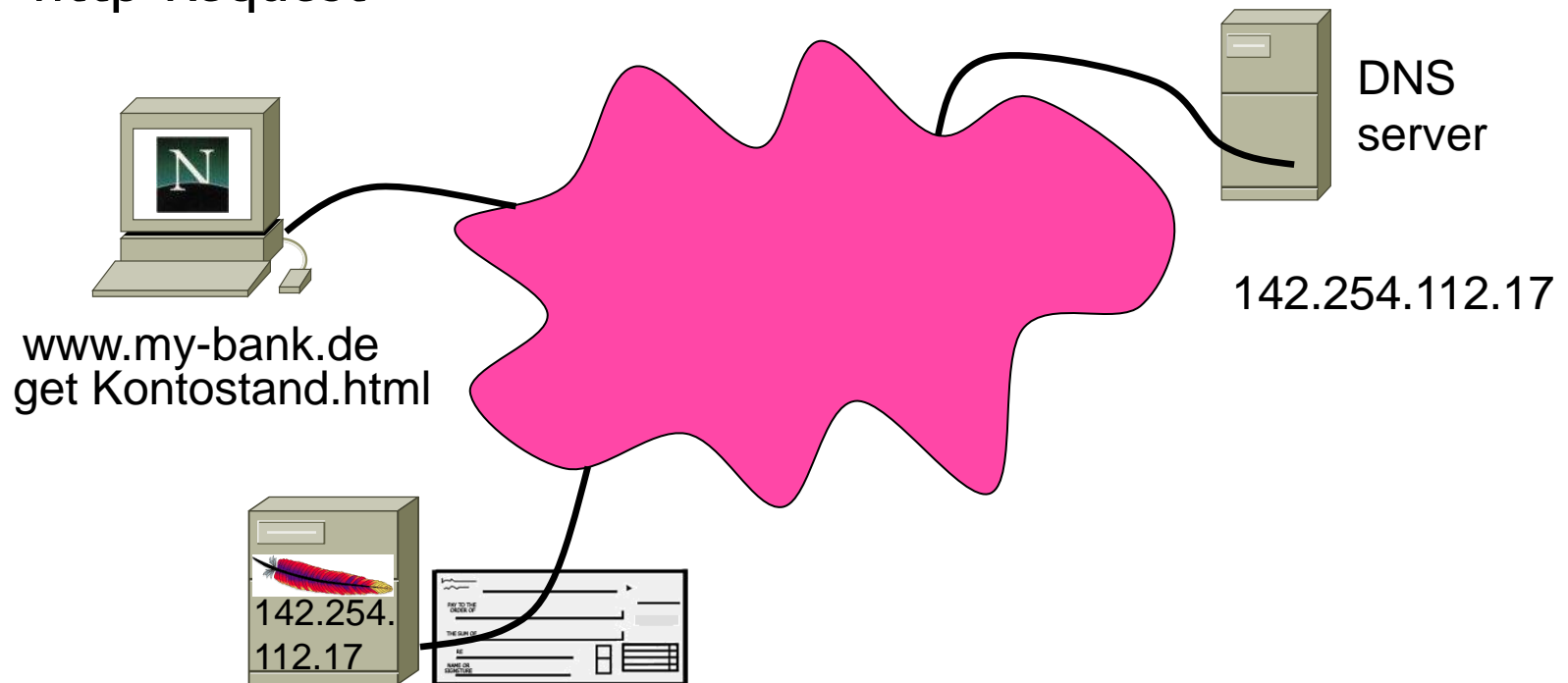
Possible attacks:

1. Compromise of DNS (DNS spoofing)

→ Server authentication
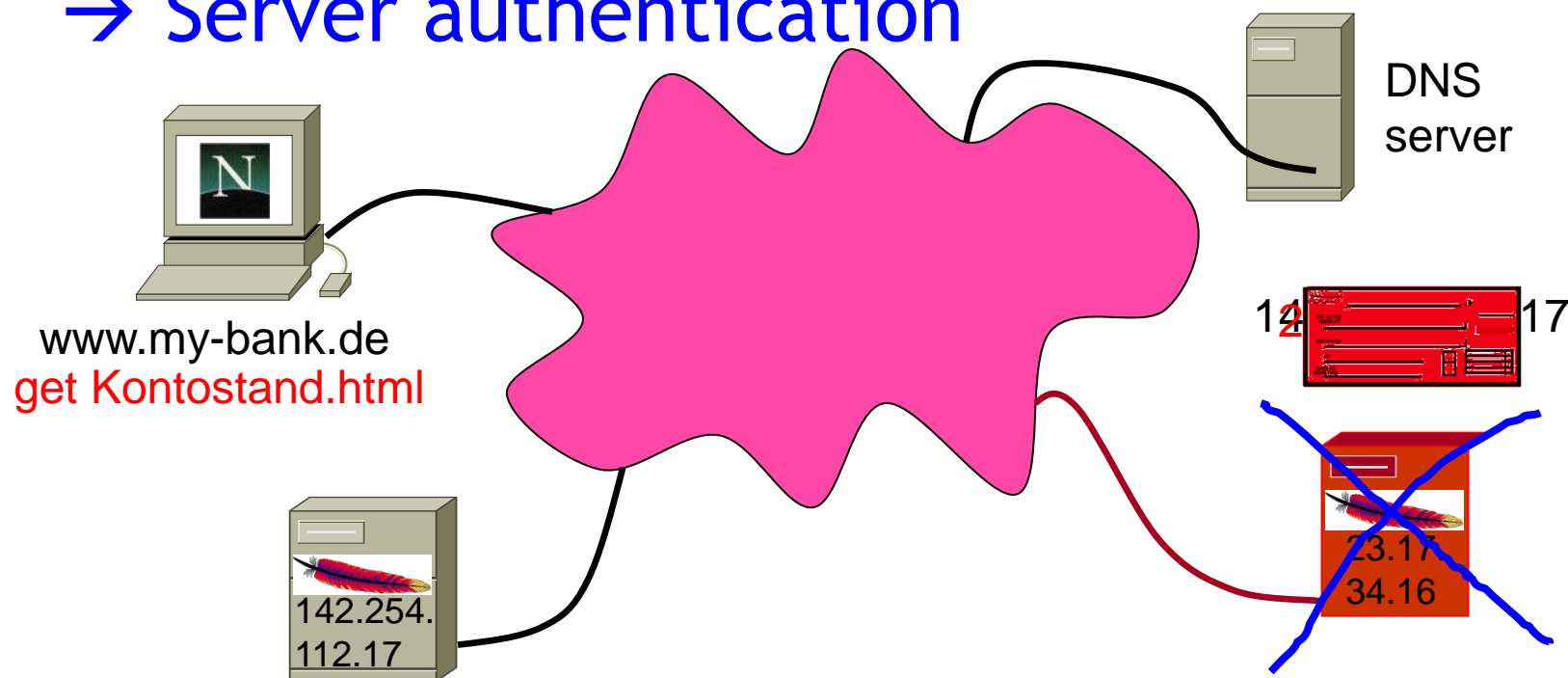
www.my-bank.de
get Kontostand.html

DNS server

142.254.112.17

[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Possible attacks:

1. Compromise of DNS
2. Eavesdropping
   → Encryption (SSL/TLS)
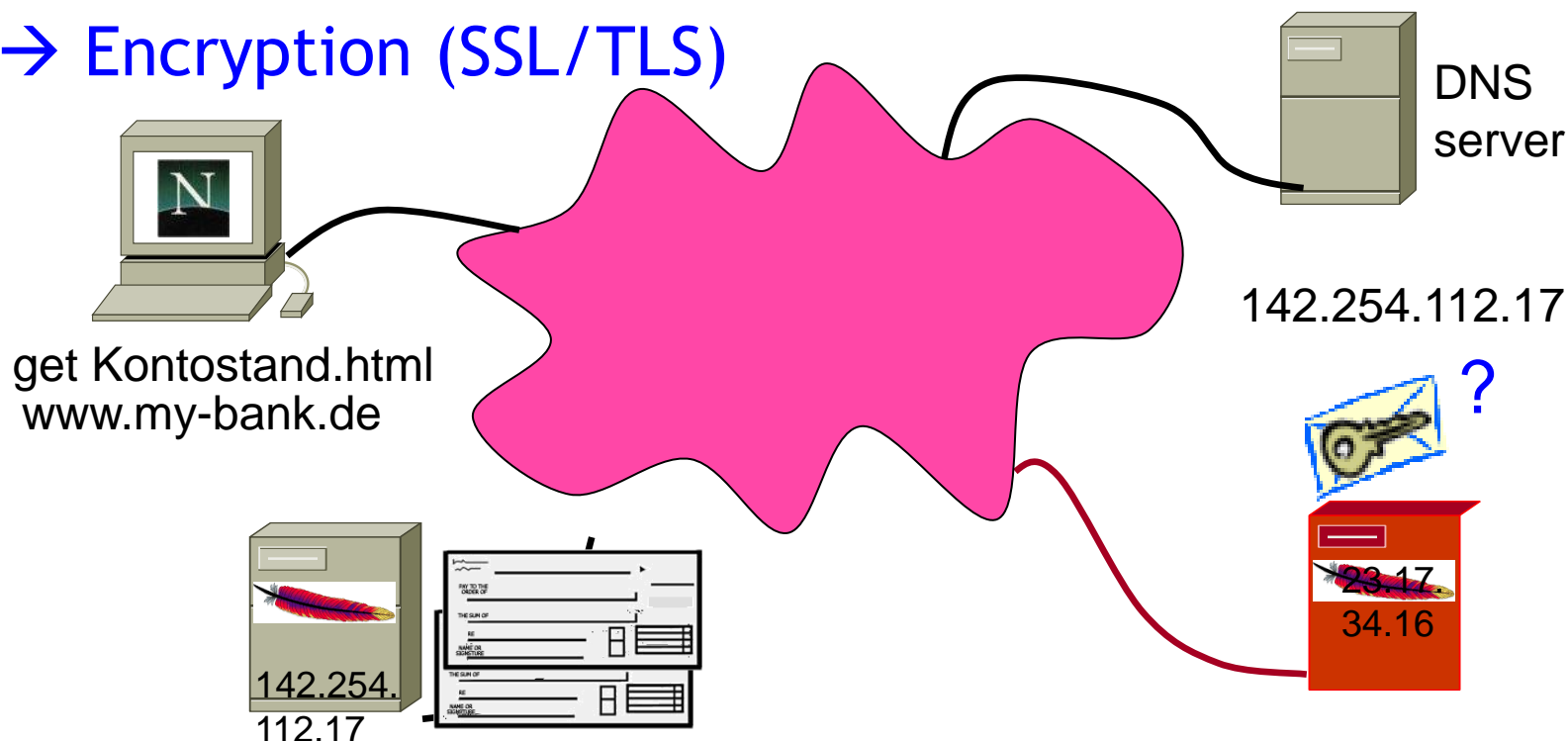
get Kontostand.html
www.my-bank.de

DNS server

142.254.112.17

?

142.254.
112.17

23.17
34.16

[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

SSL/TLS (simplified):

Hello!

Server authentication

Key exchange

data (encrypted)

142.254.
112.17

[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]
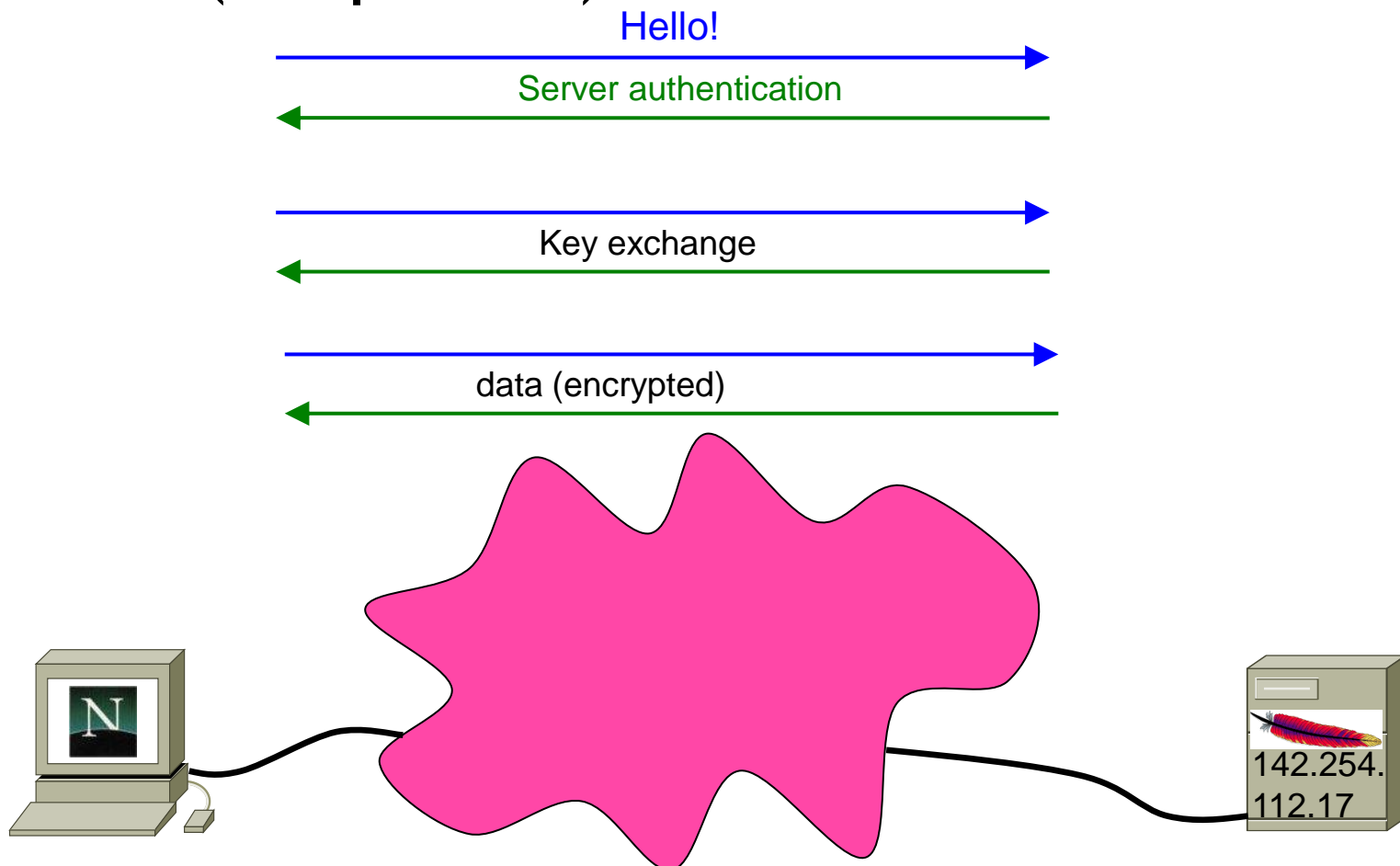
SSL/TLS:

- Server- and client-authentication

- Key exchange for symmetric encryption

- MACs to secure integrity

Security Goal	http	https (SSL/TLS)
Authenticity	✗	✓ (mostly server only)
Non-Repudiation	✗	✗
Confidentiality	✗	✓
Integrity	✗	✓
Date documentation	✗	✗

Based on [J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

- Serious vulnerability in the popular OpenSSL cryptographic software library

- OpenSSL is an open-source implementation of the SSL/TLS protocol.

- Heartbleed is **not** a design flaw in SSL/TLS protocol, but it is an **implementation problem** in the OpenSSL library.

- When the vulnerability is exploited, it leads to the leak of memory contents from the server to the client and from the client to the server.

- CVE-2014-0160 is the official reference to this bug (www.cve.mitre.org).

based on [www.heartbleed.com]

- Introduction
- Infrastructure Security Components
    - Firewalls
    - Demilitarized Zone
    - Intrusion Detection
- Security Protocols
    - Virtual Private Networks
    - Secure Socket Layer
    - IPsec
- Application Layer Security
- Wireless / Mobile Security

- Attacker is able to eavesdrop IP packets.
- Ideally: at the gateway of sender or recipient

Based on: [J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]
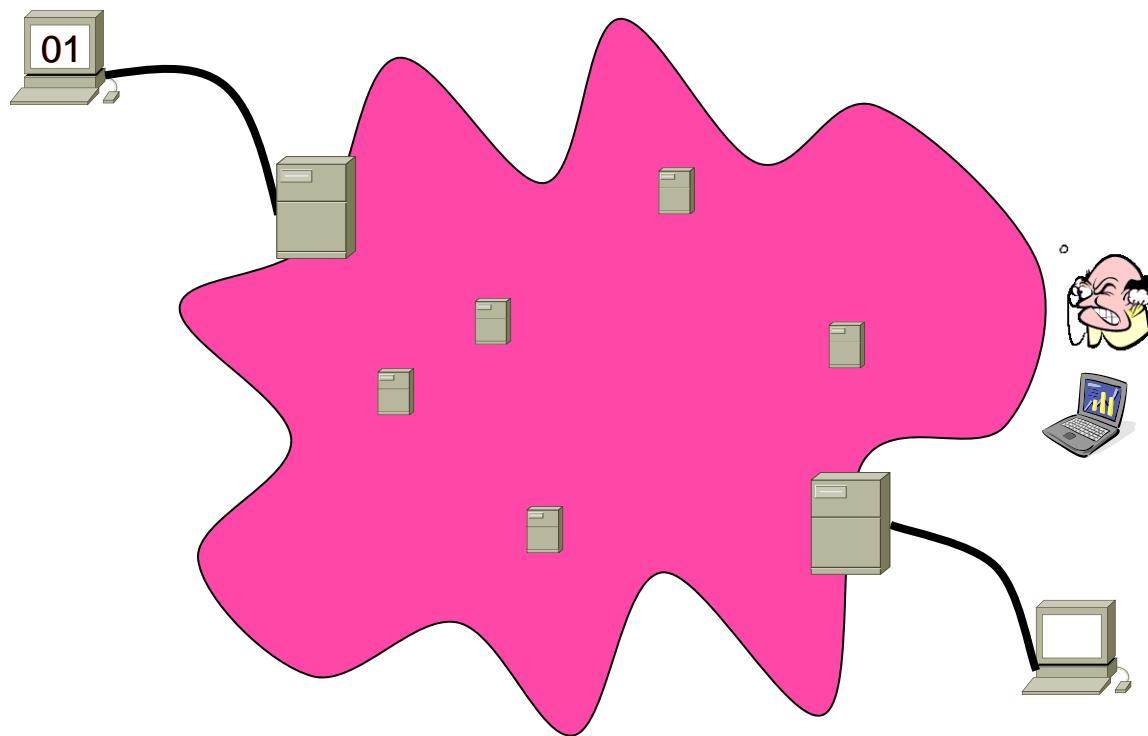
Encapsulating Security Payload (ESP)

- **Data Packet**

IP-Header	IP-Payload

- **ESP-Transport-Mode**

IP-Header	ESP-Header	IP-Payload	ESP-Trailer

encrypted ←——————————→

- **ESP-Tunnel-Mode**

New IP-Header	ESP-Header	IP-Header	IP-Payload	ESP-Trailer

encrypted ←——————————→

[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]
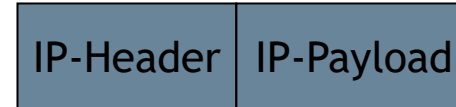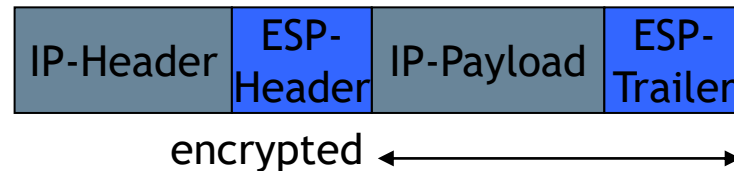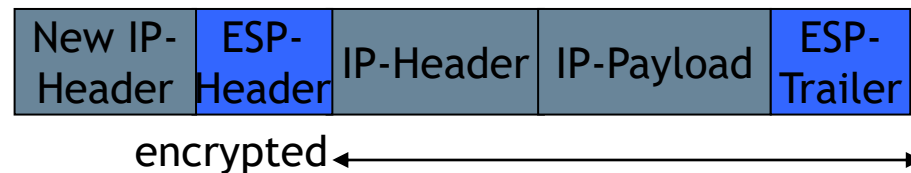
- Attacker sends IP-packets with a faked sender address.

[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]
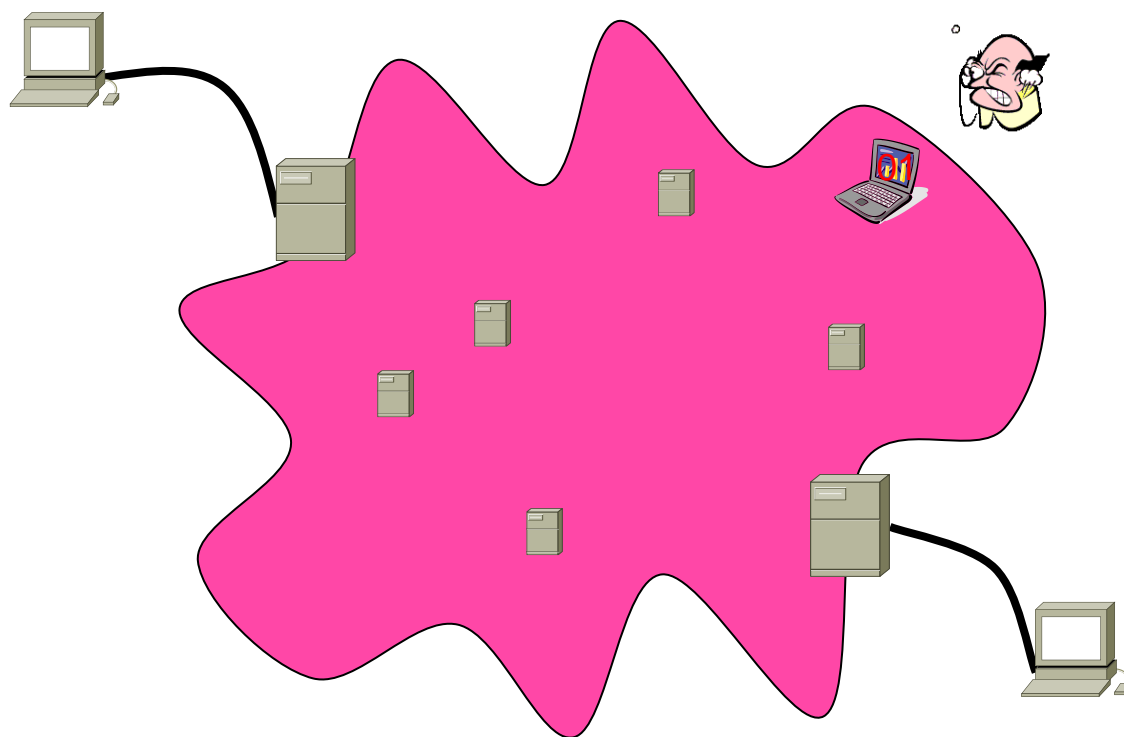
- Attacker impersonates the recipient.
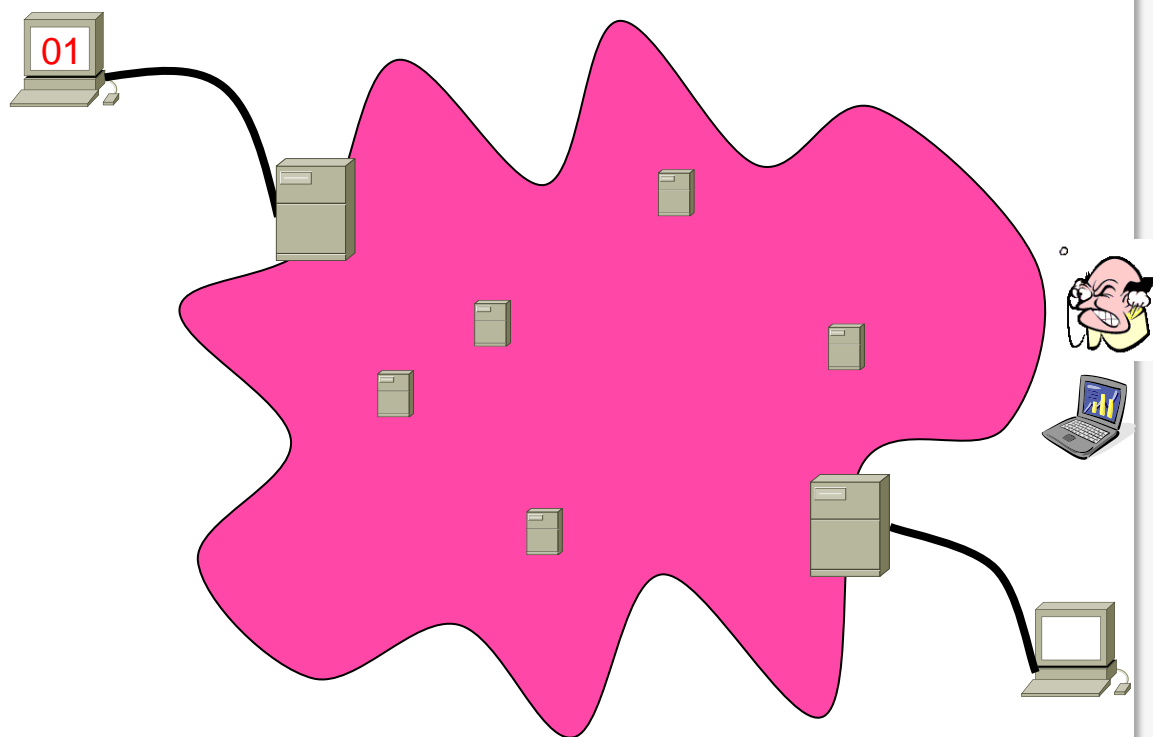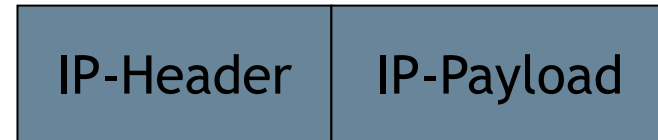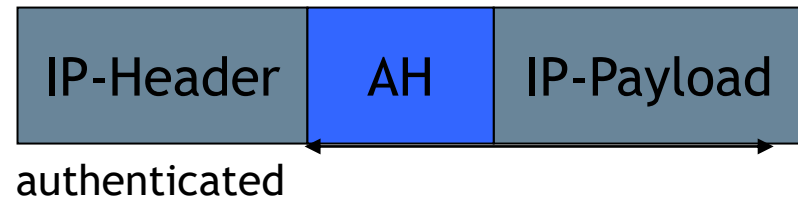
[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Data Packet

IP-Header	IP-Payload

AH-Transport-Mode

IP-Header	AH	IP-Payload

authenticated

AH-Tunneling-Mode

New IP-Header	AH	IP-Header	IP-Payload

authenticated

Based on [J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]
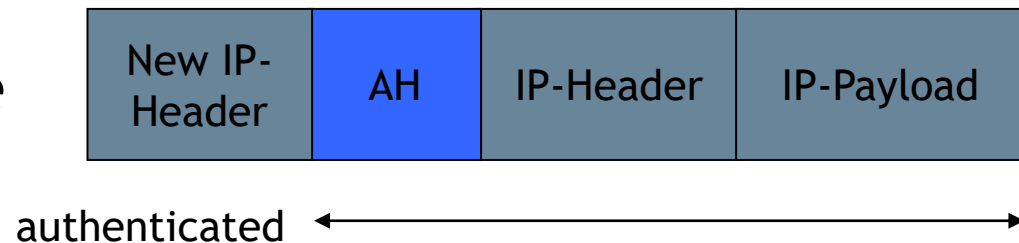
- **Introduction**
- **Infrastructure Security Components**
    - Firewalls
    - Demilitarized Zone
    - Intrusion Detection
- **Security Protocols**
    - Virtual Private Networks
    - Secure Socket Layer
    - IPsec
- **Application Layer Security**
- **Wireless / Mobile Security**

- Insertion attacks involve the introduction of unauthorized content or devices to an otherwise secured infrastructure, e.g., SQL injection.

- SQL injection is an attack that inserts unauthorized code into a script hosted on a Web site.

[Based on Ba10]

User Name: | ' or 1=1-- |

Password: | |

☐ Remember me next time.

Log In

1=1 always true
↓

select * from MyTable where Email=' ' or 1=1 --'and Password="

↑
Commented line, because "-- "

[C#C]

- A buffer is an area of memory designated to receive input (size set by the programmer).

- A buffer overflow is an attack against poor programming techniques and a lack of quality control. An attacker injects more data into a buffer than it can hold.

[Based on Ba10]

XSS (Cross-site Scripting)

- Similar to SQL injection, but attacks visitors to a website rather than grant access to the back-end database
- XSS Attack submits (attacking) script code to a benign or trusted website.
- User browser trusts web server and executes (attacking) script.
- How does script arrive on web server?
    - Persistent: Attacker modifies website, e.g. via misusing the comment function on e.g. a blog.
    - Non-persistent: Attacker makes user call the website with a special link including attacking code, e.g. via sending email with that link to the user.
- Fundamental problems
    - Websites don't check input properly.
    - Browsers trust websites too blindly.
- Work around
    - Users to check links before they click on them.

[Based on Ba10, Wikipedia]

Distributed Denial of Service (DDoS)

- Distributed denial of service (DDoS) attacks advance DoS attacks through massive distributed processing and sourcing.

- Bots (zombies): malicious code implanted on victim systems across the Internet with the Command and Control server controlling the bots

- Target systems: attacked by DDoS attacks

Type 1: Every bot is directly connected with Command & Control server.
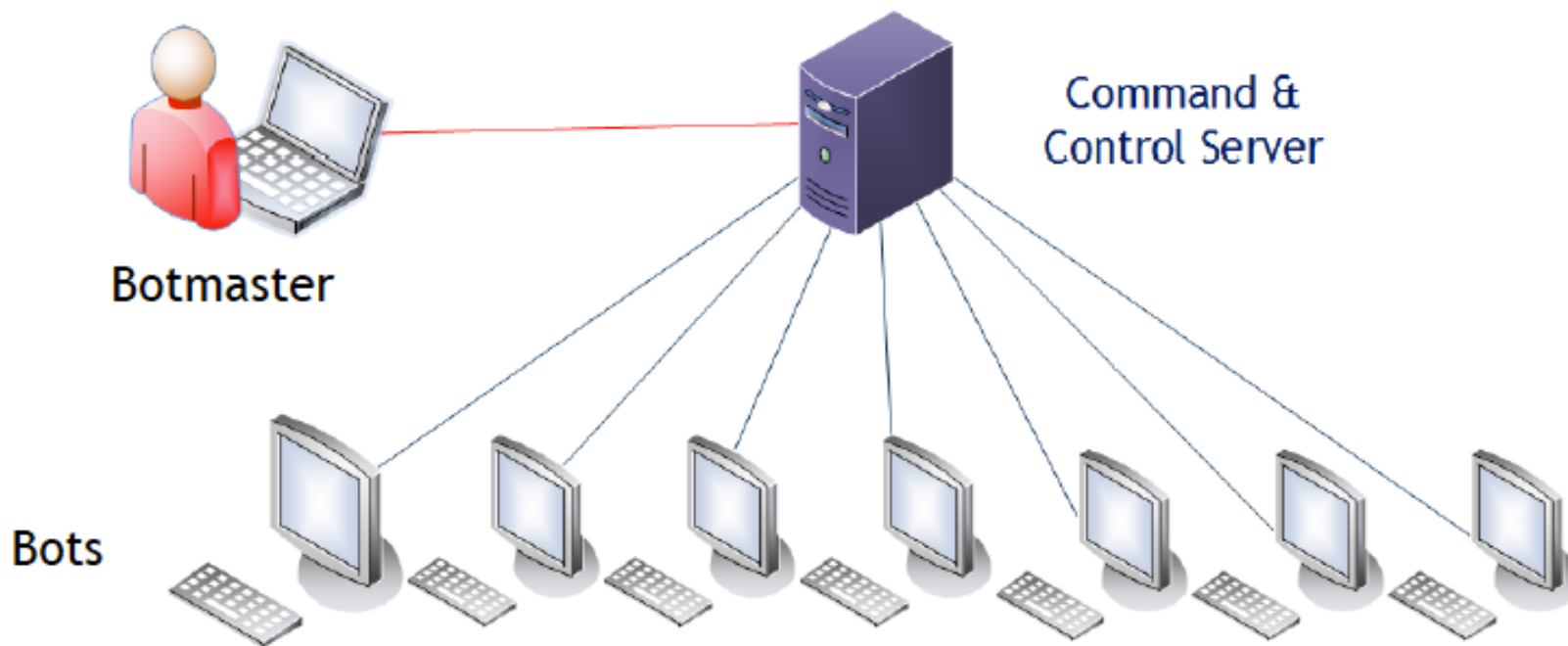
Type 2: Peer-to-Peer botnets, bots compose a mesh structure in which commands are also transmitted from bot to bot.
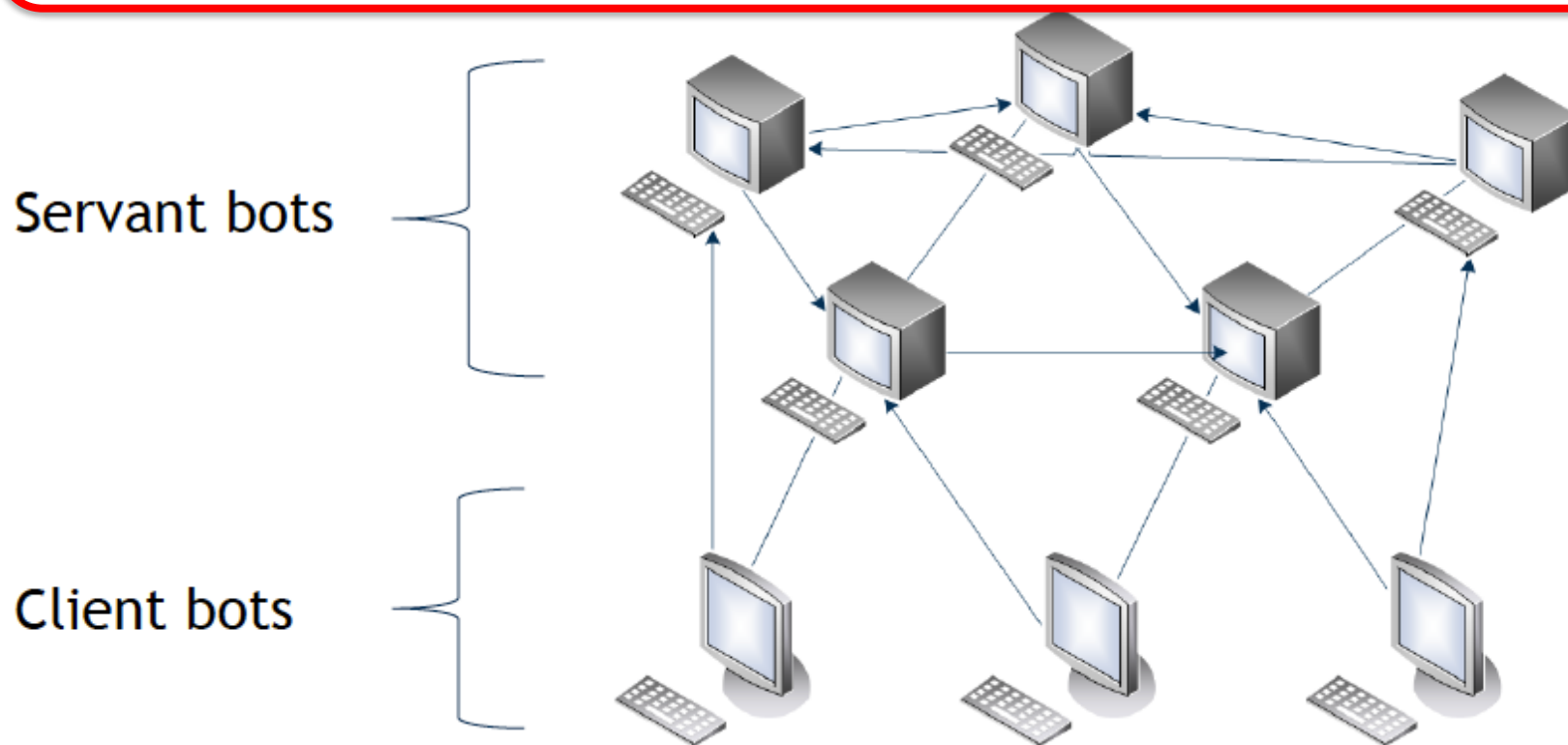
Servant bots

Client bots

- Introduction
- Infrastructure Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Application Layer Security
- Wireless / Mobile Security

References

- [Ba10] Jones & Bartlett: Network Security, Firewalls, and VPNs

- [Bi05] Matt Bishop: *Introduction to Computer Security*. Boston: Addison Wesley, 2005, pp. 455-516

- [C#C] How SQL Injection Is Possible In ASP.Net Websites, http://www.c-sharpcorner.com/UploadFile/75a48f/how-sql-injection-can-be-possible-in-asp-net-websites/, published on 2014-01-13, last time accessed on 2017-01-18

- [De87] Dorothy Denning: "An Intrusion- Detection Model", IEEE Transactions on Software Engineering, 13 (2), pp. 222-232

- [Hacker14] Hacker Lexicon: What Is End-to-End Encryption? https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/

- [He14] Heartbleed: "The Heartbleed Bug", www.heartbleed.com

- [Honeypot] Honey pot clip art http://cliparts.co/honey-pot-clip-art, last time accessed 2020-06-24

- [RFC 2828] Network Working Group: "Request for Comments 2828 - Internet Security Glossary", 2000, www.faqs.org/ftp/rfc/pdf/rfc2828.txt.pdf

- [SANS] Network Security Resources, https://www.sans.org/network-security/

- [Tan96] A.S. Tanenbaum: Computer Networks, 3rd Edition, 1996 [4th edition available]

- [Wikipedia] XSS - Cross-site scripting, https://en.wikipedia.org/wiki/Cross-site_scripting, last time accessed on 2017-01-17

- [Wireshark] Wireshark, https://en.wikipedia.org/wiki/Wireshark