mobile business

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (SS 15)

Network Security I

Dr. Jetzabel Serna-Olvera
@sernaolverajm
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

mobile business

Agenda

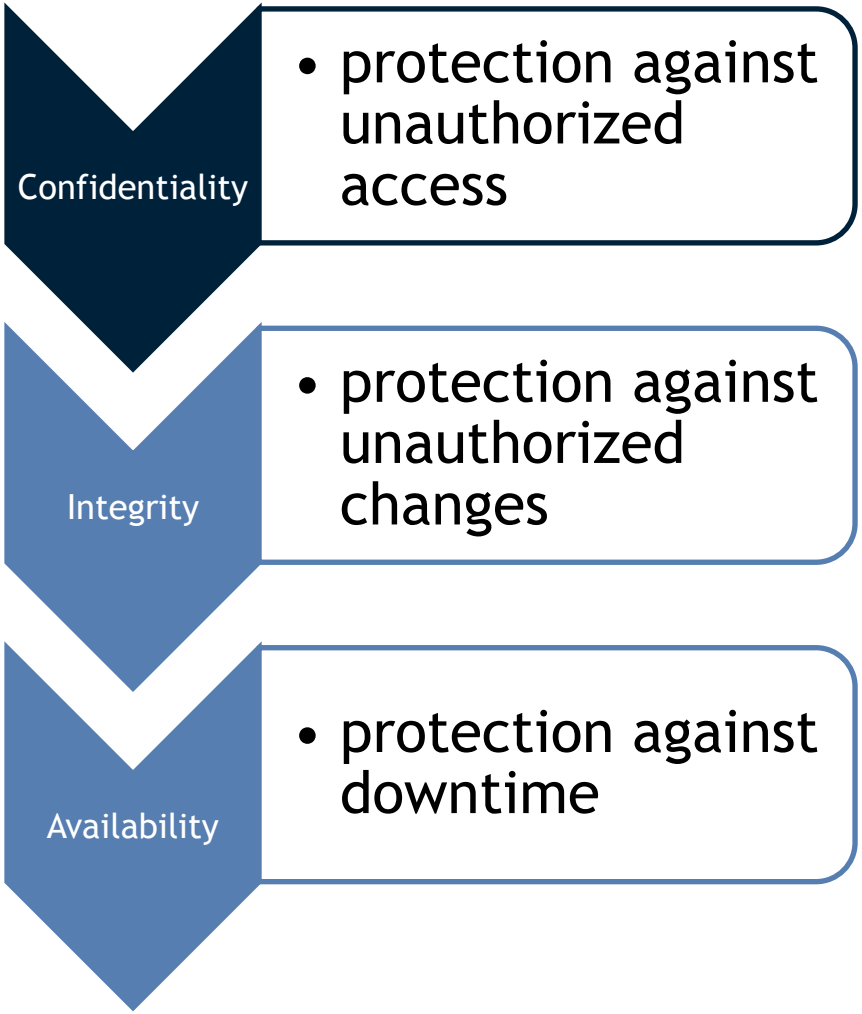
- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security

mobile business

Introduction

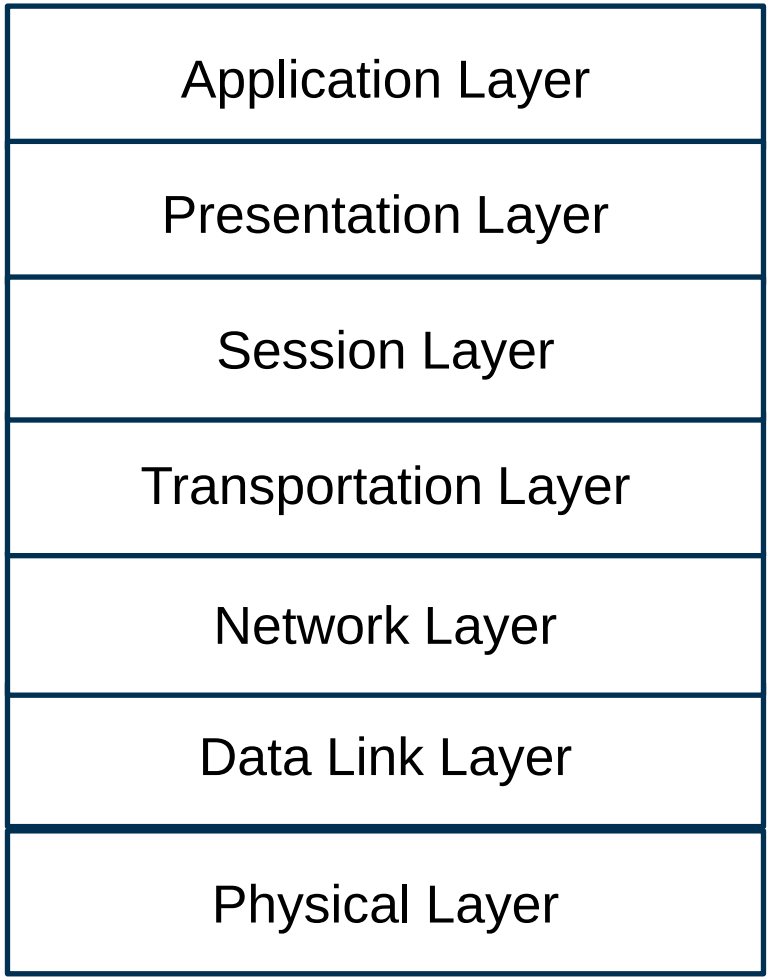
- **Network security** is the **control of** unwanted intrusion, misuse, modification, damage or denial of a computer network and network-accessible resources. [Ba10]
- Network security is the process of taking physical and software preventative measures to protect the networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. [SANS]

Network Security Goals



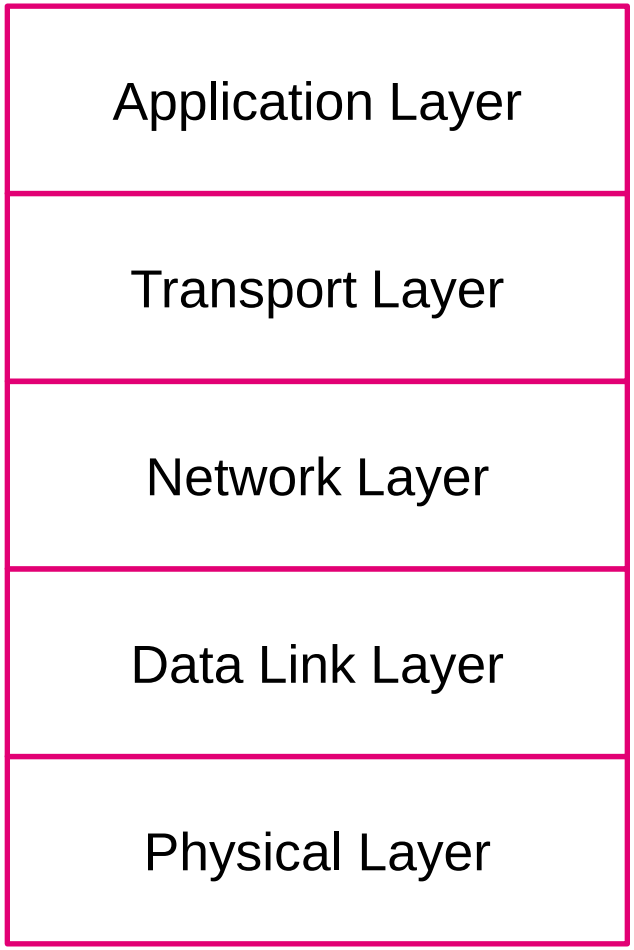
- Ensure the confidentiality of resources
- Protect the integrity of data
- Maintain availability of the IT infrastructure
- Ensure the privacy of personally identifiable data
- Enforce access control
- Monitor IT for policy violations
- Support business tasks and the overall mission of the organization

ISO/OSI Reference Model



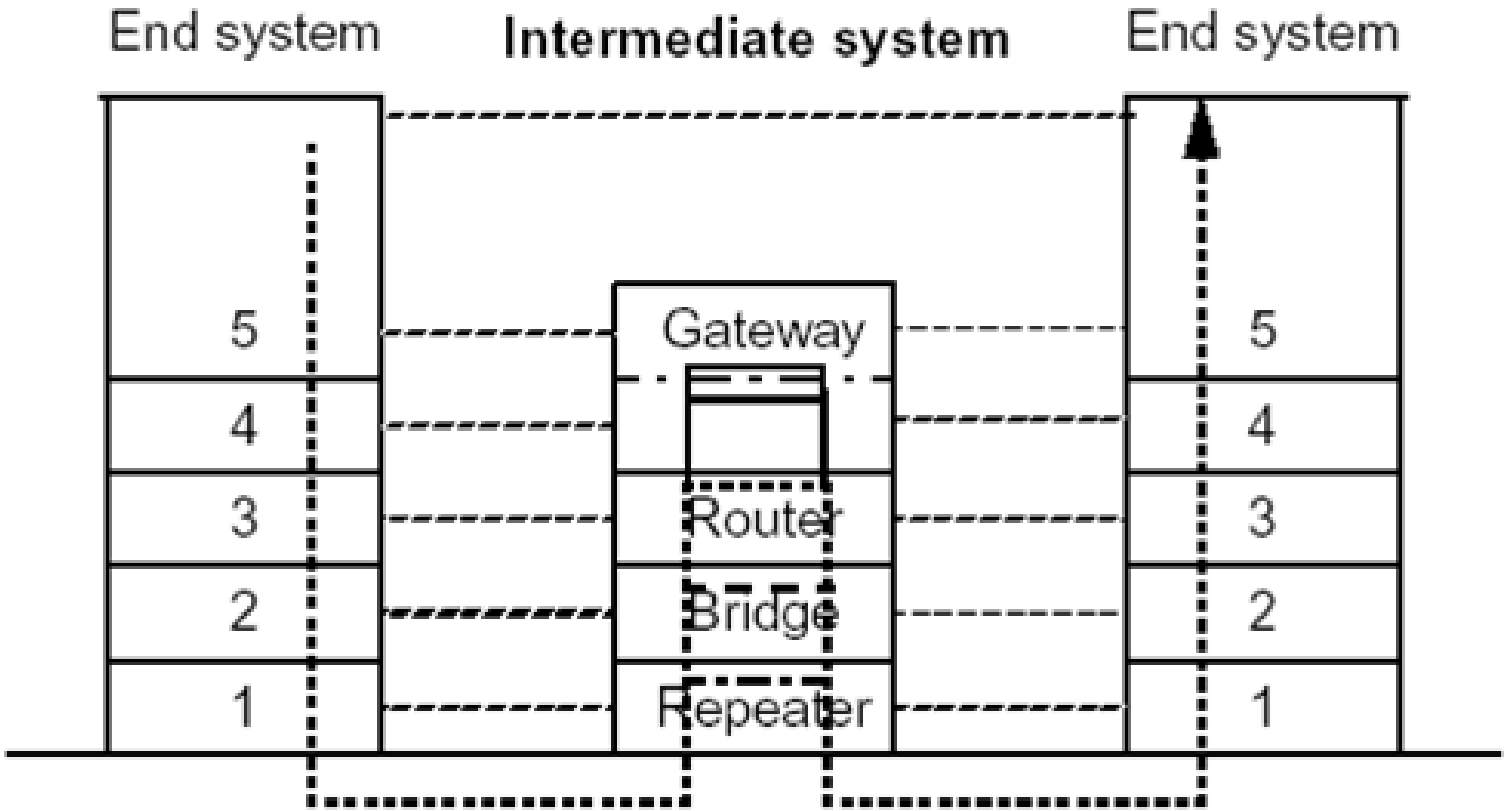
- Information technology — Open Systems Interconnection — Basic Reference Model
- „7-Layer-Model“
  - First version ISO/IEC 7498-1:1984
  - Current version ISO/IEC 7498-1:1994

Internet Reference Model



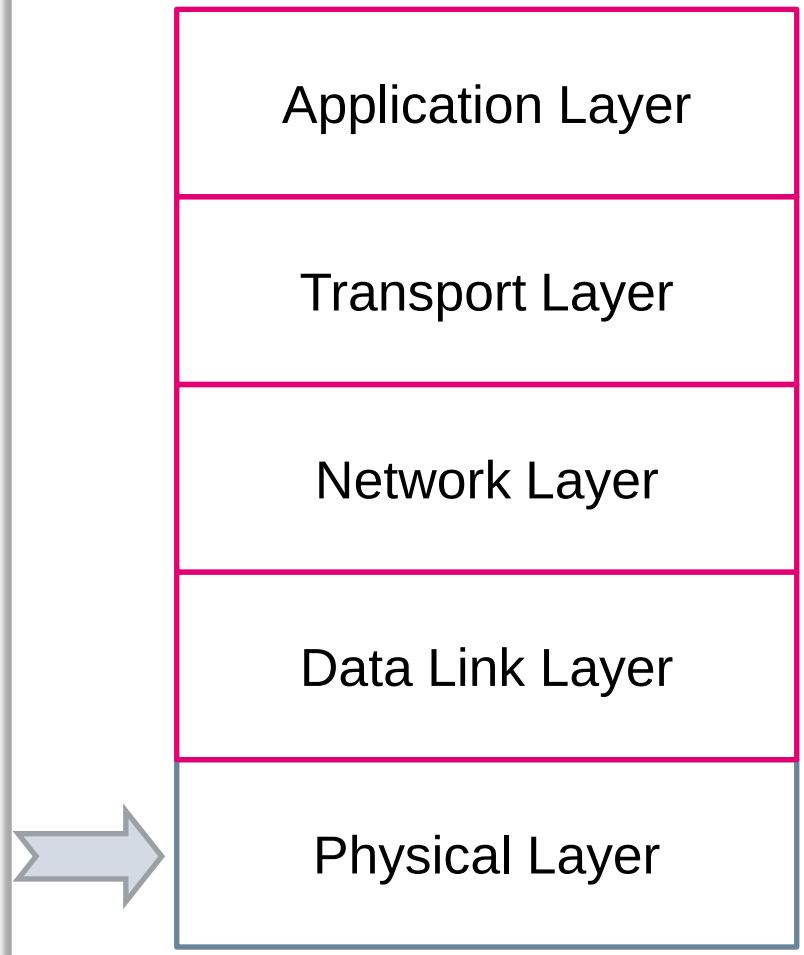
[Ta96]

Communication Example



[Ta96]

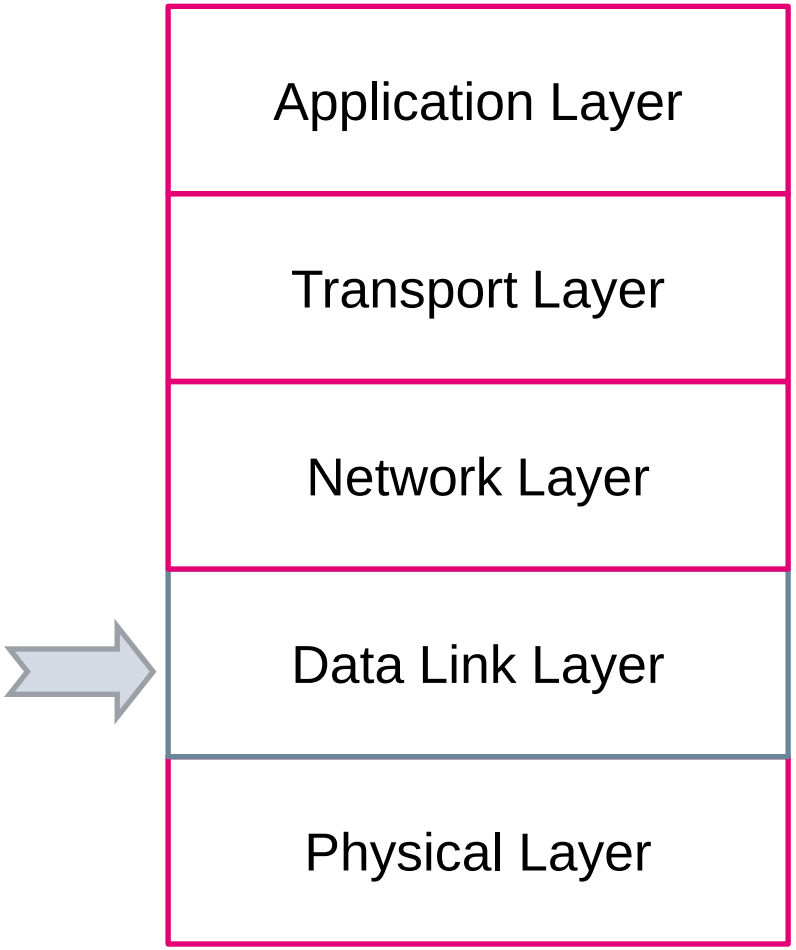
Physical Layer



Tasks:

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

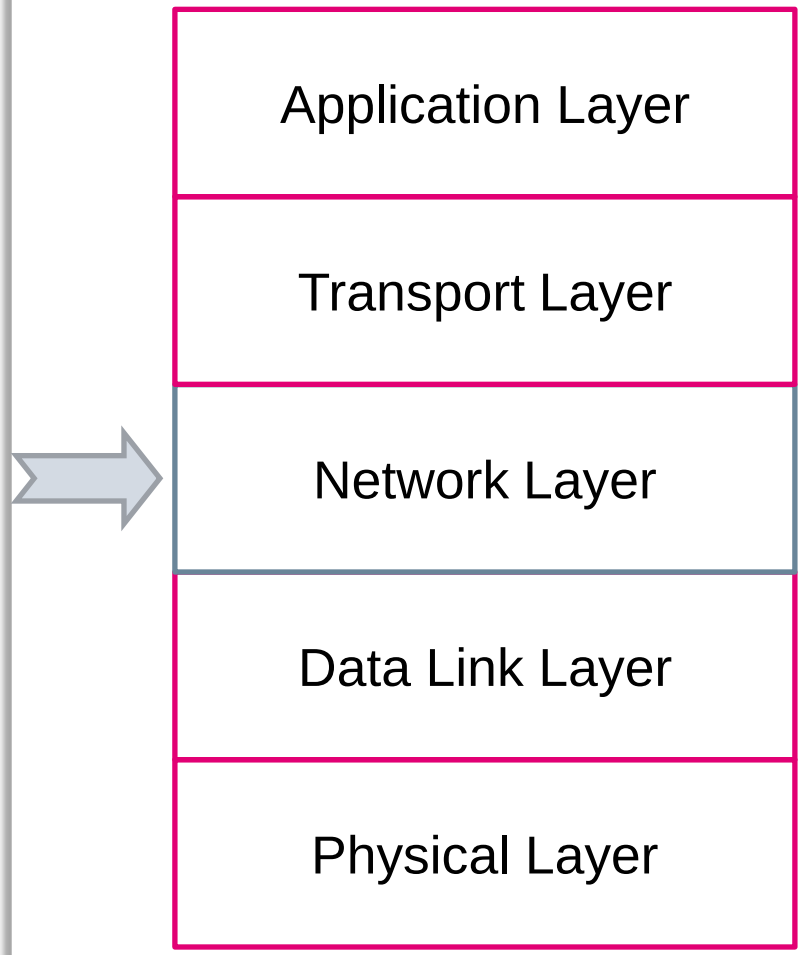
Data Link Layer



Tasks:

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

Network Layer

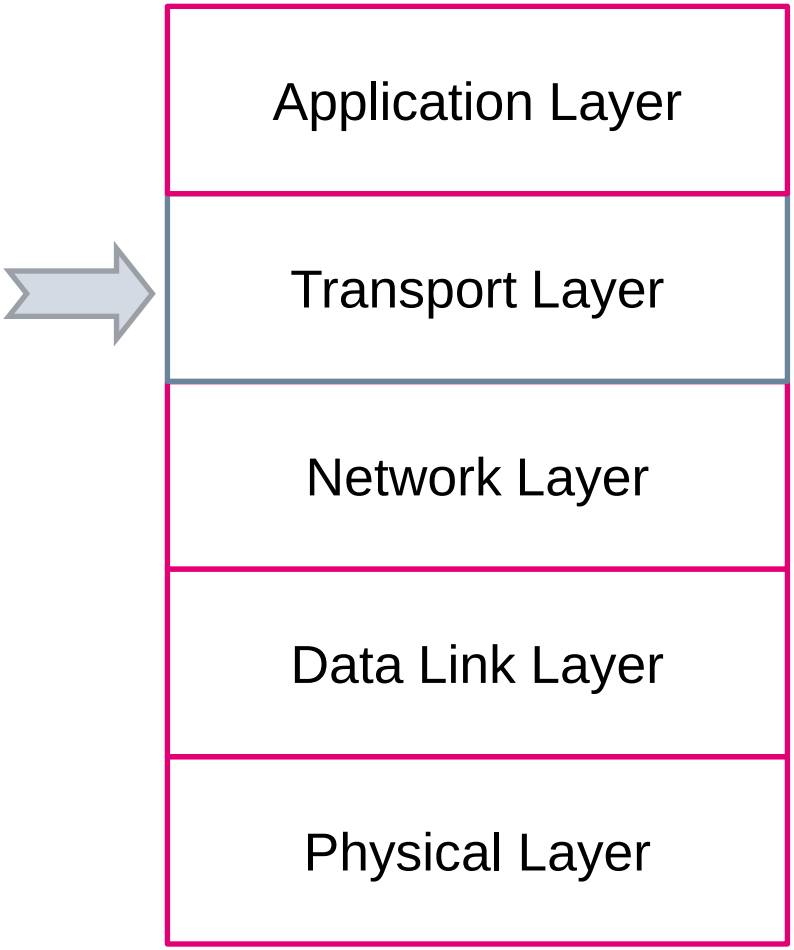


Tasks:

- End-to-end connections between systems
- Routing
- Addressing
- Typically connectionless

For example: IP

Transport Layer

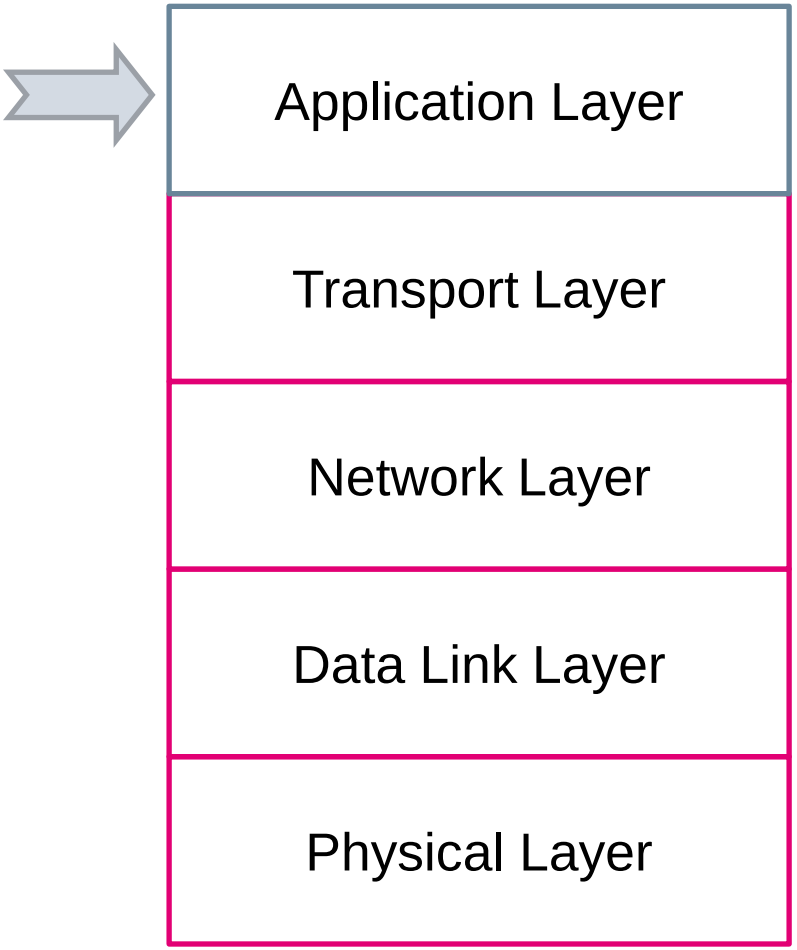


Tasks:

- Connection between source and target
- Optimisation of quality of service and service costs
- Flow control
- Connection management

For example: TCP, UDP

Application Layer



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

mobile business

Agenda

- Introduction
- Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Threats
- Wireless / Mobile Security

mobile business

Agenda

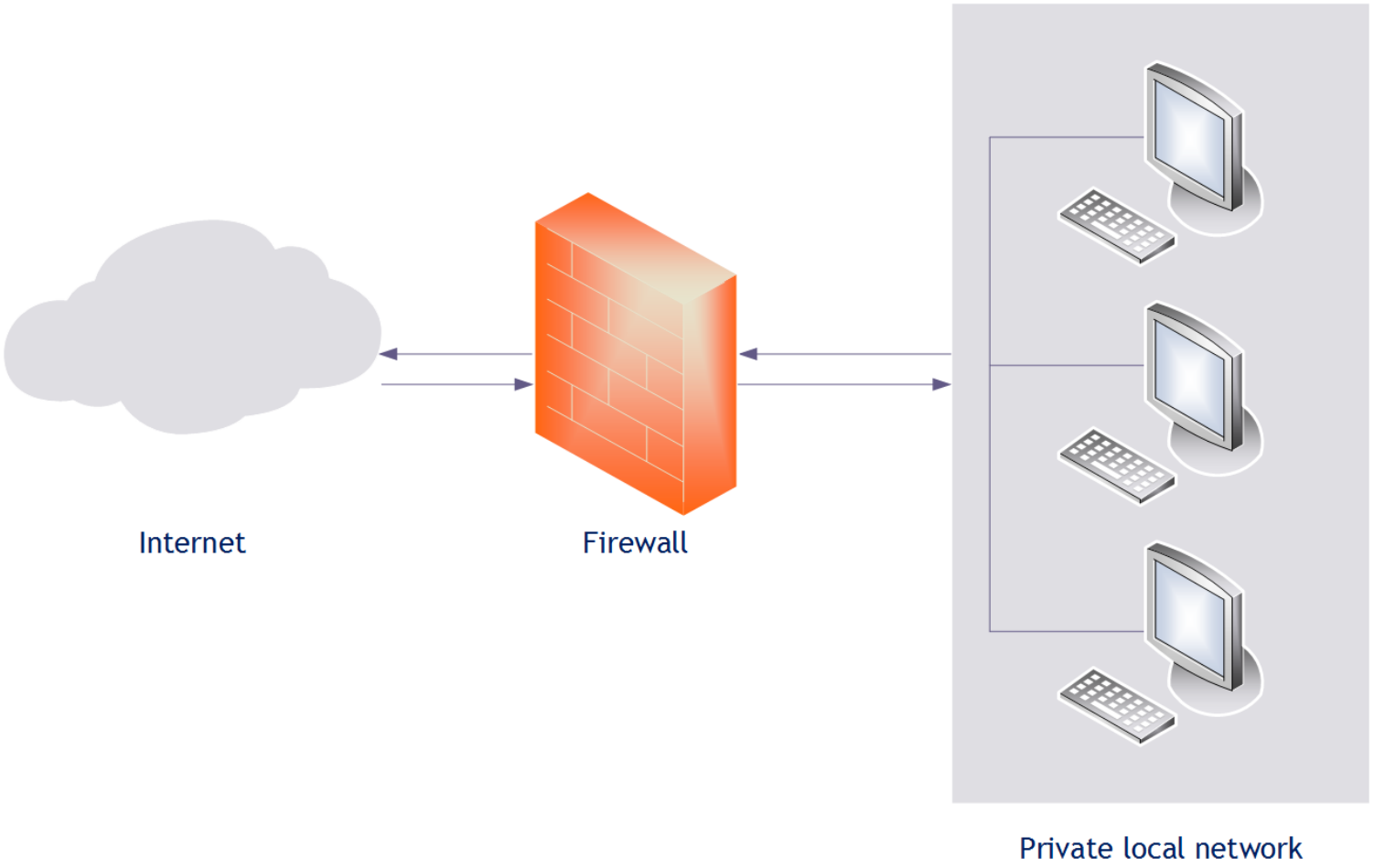
- Introduction
- Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
- Security Threats
- Wireless / Mobile Security

mobile business

Firewall

- A firewall is a network security device controlling traffic flow between two parts of a network. [Go06]
- A firewall is a host that mediates access to a network, allowing and disallowing certain types of access on the basis of a configured security policy. [Bi05]

Firewall



Based on [Bi05]

Types of firewalls

- 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.

[Bi05]

mobile business

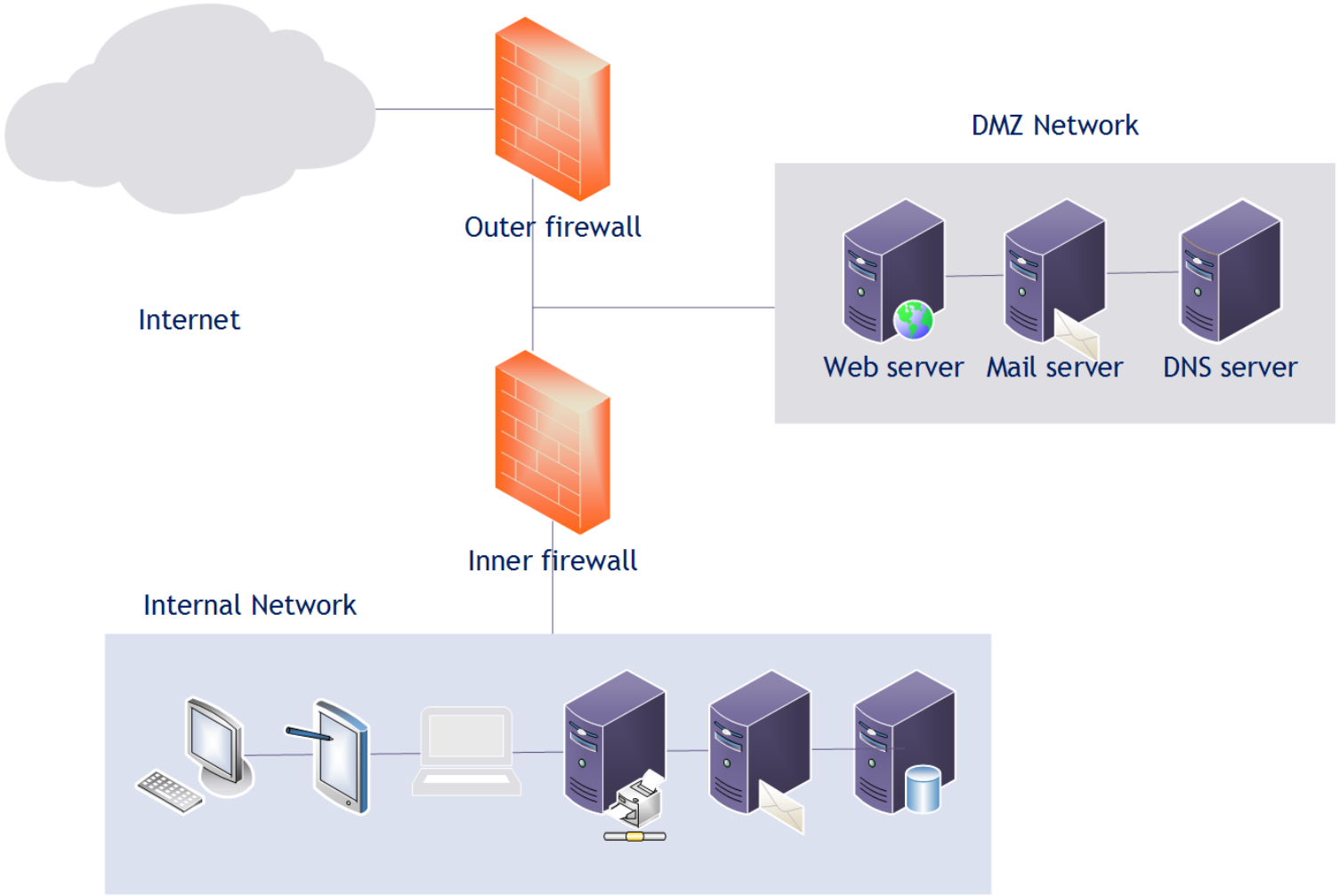
Agenda

- Introduction
- Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
- Security Threats
- 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 DMZ.
- 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.

Network using a DMZ



mobile business

Agenda

- Introduction
- Security Components
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
- Security Threats
- 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.
2. The actions of users and processes do not include sequences of commands to subvert the security policy of the system.
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.

Goals of Intrusion Detection Systems

- 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.

[Bi05]

Anomaly Detection

- *Anomaly detection* analyzes a set of characteristics of the system, and compares their behavior with a set of expected values ("normal" activity).
- It reports when the computed statistics do not match the expected measurements (a deviation of normality could be an intrusion).

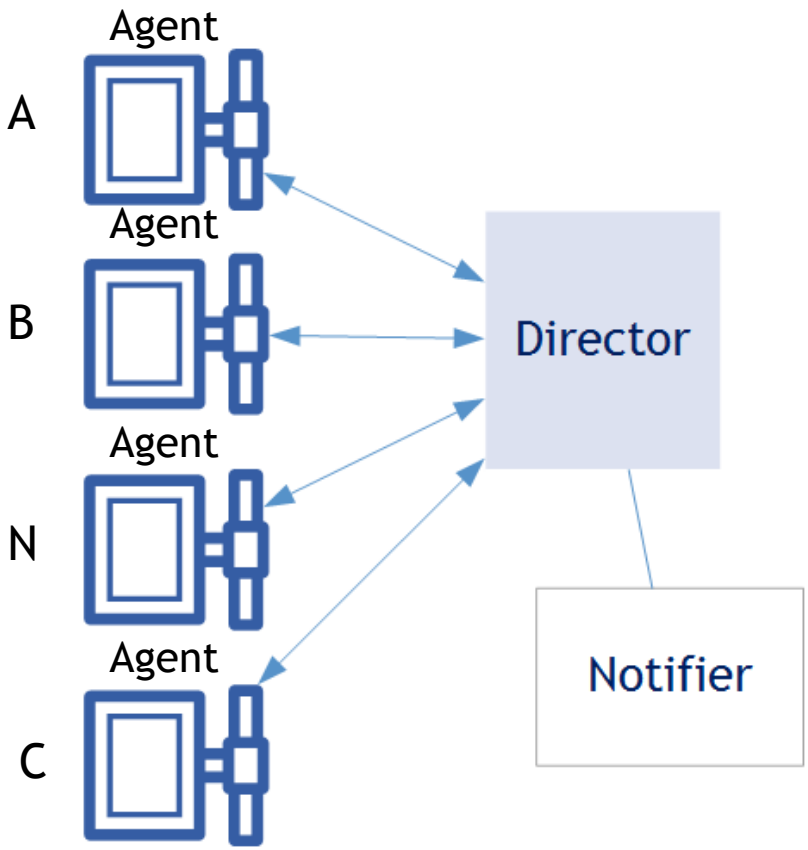
[Bi05]

Misuse Detection

- Misuse detection (based on rules) 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.

[Bi05]

Intrusion Detection System



[Bi05]

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

Source [http://cliparts.co]

mobile business

Agenda

- Introduction
- Security Components
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Security Threats
- Wireless / Mobile Security

mobile business

Agenda

- Introduction
- Security Components
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Security Threats
- Wireless /Mobile Security

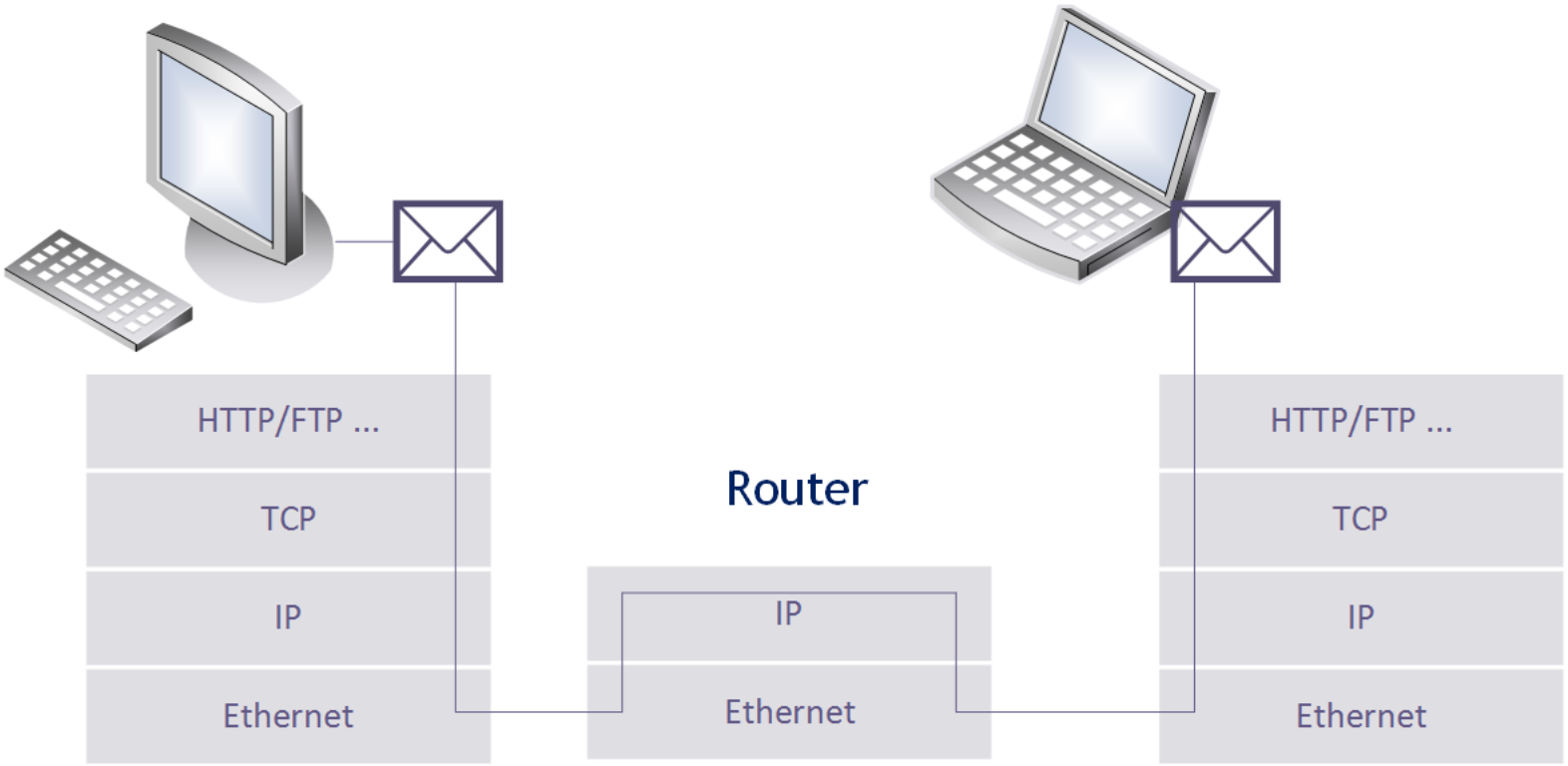
mobile business

VPN

- A virtual private network (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.

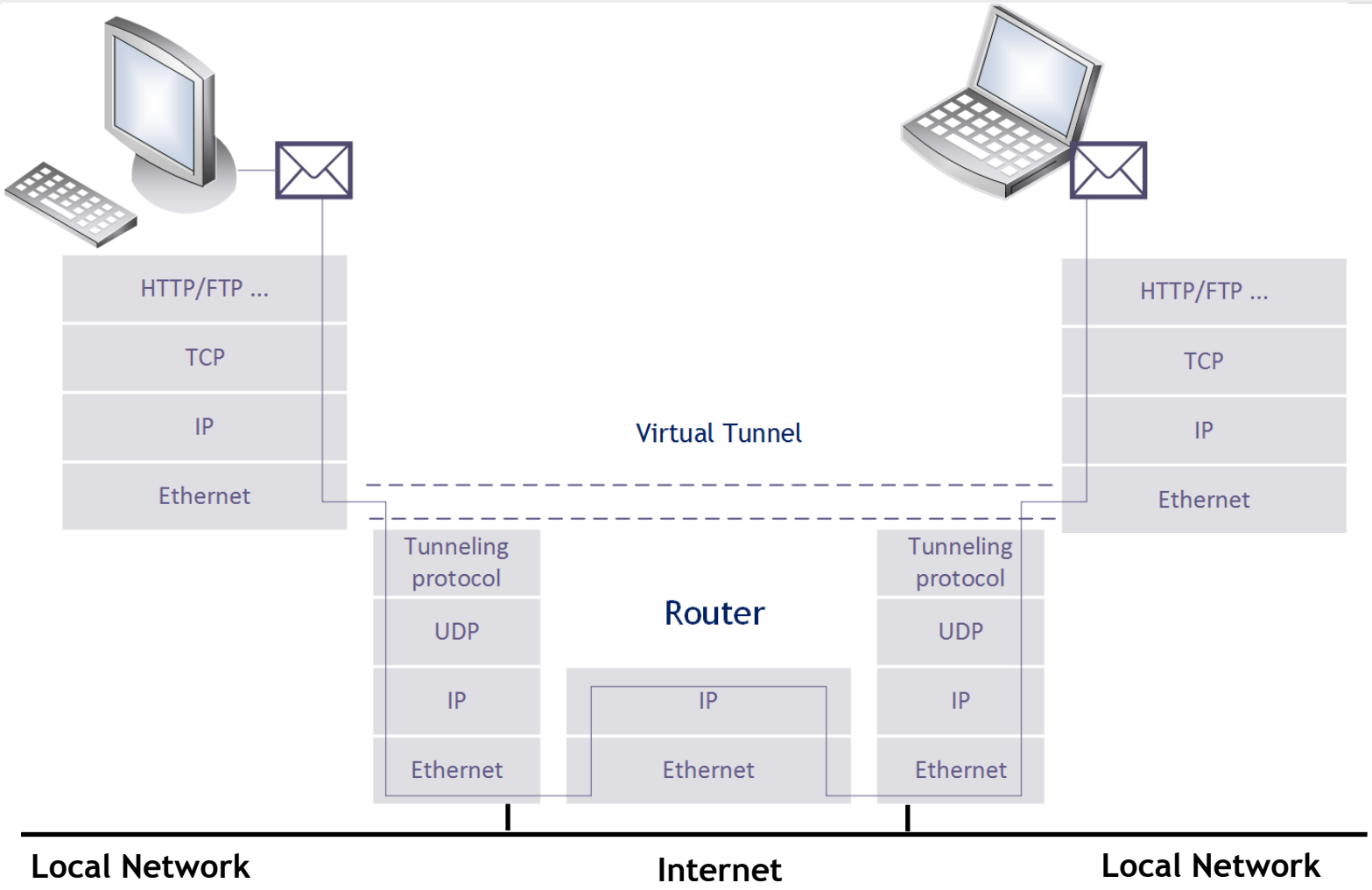
[Ba10]

Communication without a VPN



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

VPN



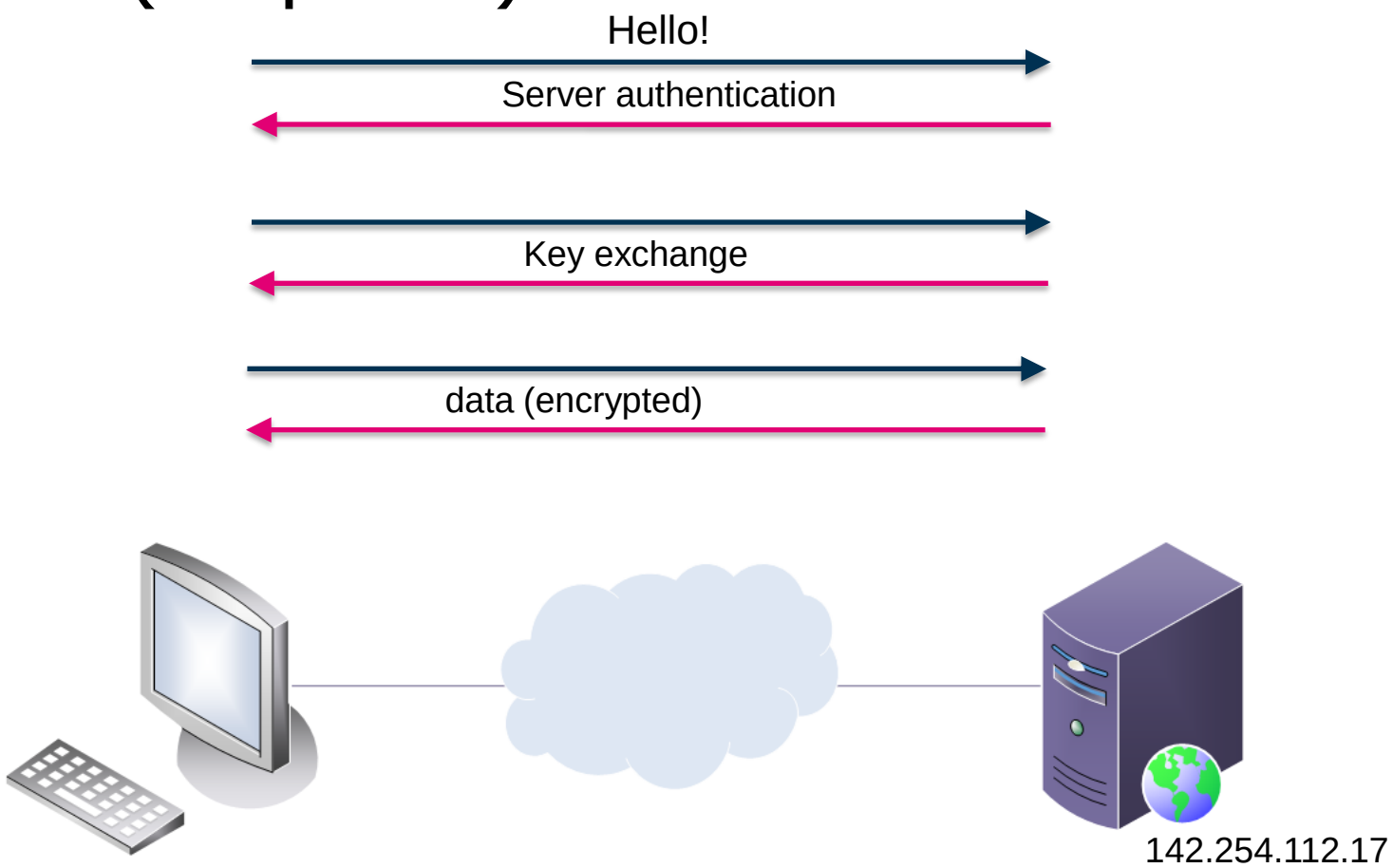
[Based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

mobile business

Agenda

- Introduction
- Security Components
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Security Threats
- Wireless /Mobile Security

SSL/TLS (simplified):



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

SSL/TLS

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]

Heartbleed (1)

- Serious vulnerability in the popular OpenSSL cryptographic software library
- OpenSSL is an open-source implementation of the SSL/TLS protocol.
- 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.

based on [www.heartbleed.com]

Heartbleed (2)

- Heartbleed is **not** a design flaw in SSL/TLS protocol, but it is an **implementation problem** in the OpenSSL library.
- CVE-2014-0160 is the official reference to this bug (www.cve.mitre.org).

mobile business

Agenda

- Introduction
- Security Components
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Security Threats
- Wireless / Mobile Security

mobile business

IPSec

- Internet Protocol Security (IPSec) is a standards-based protocol designed specifically for securing Internet Protocol (IP) communications.
- IPSec has protocols that can establish:
  - mutual authentication
  - cryptographic key negotiation

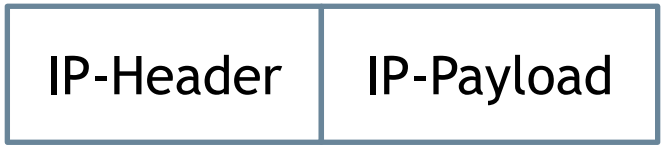
mobile business

Components

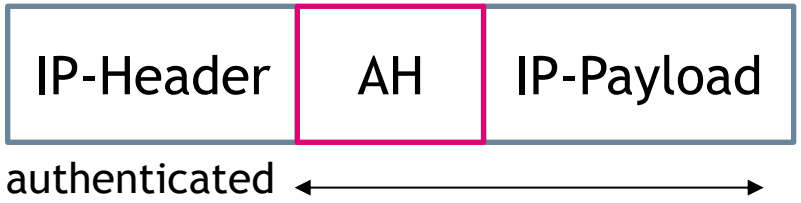
- The Authentication Header (AH): provides integrity protection and data origin authentication.
- Encapsulating Security Payload (ESP): provides confidentiality and integrity.
- Internet Key Exchange (IKE): negotiates, creates, and manages security associations.

IPsec
Authentication Header (AH)

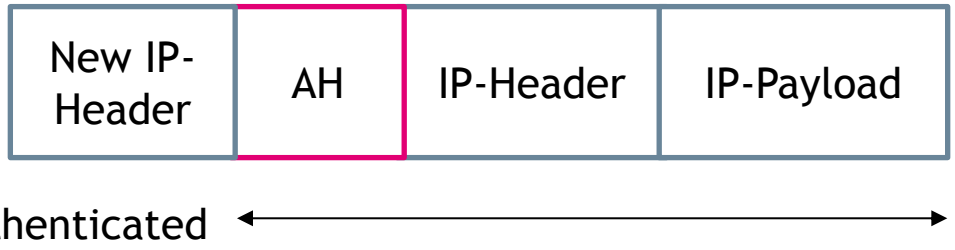
Data Packet



AH-Transport-Mode



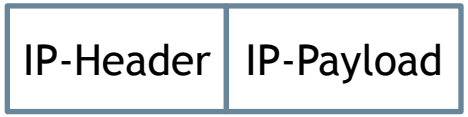
AH-Tunneling-Mode



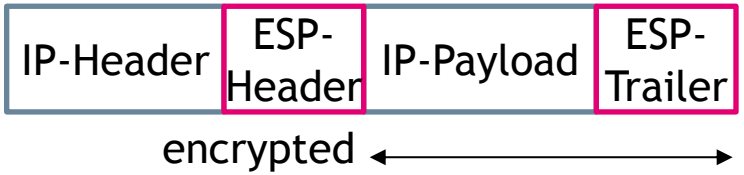
Based on [J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Encapsulating Security Payload (ESP)

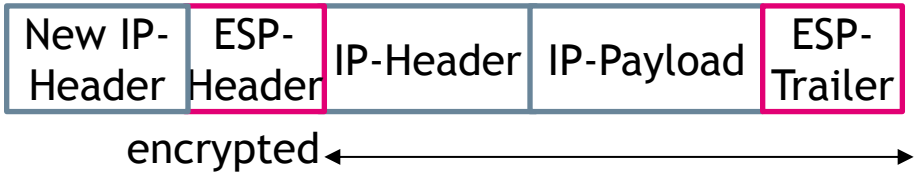
- Data Packet



- ESP-Transport-Mode



- ESP-Tunnel-Mode



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

mobile business

Agenda

- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security

Network Security Threats and Issues

- A threat is an undesirable negative impact on your assets. A threat materializes when an attack succeeds.
- An attack is a sequence of steps until the final target is reached.
- An attacker can be passive or active
  - Passive: listens to traffic
  - Active: may modify, insert new messages, or corrupt network management information

[Go06]

Attack Tool

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

- Example: *Rootkits*
  - Exist for many versions of operating systems, e.g., Unix.
  - 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.

[Bi05]

Malware

- Malicious Software
  - Virus
  - Trojans
  - Worms
  - Spyware
  - Ransomware
  - Backdoor

[Bi05]

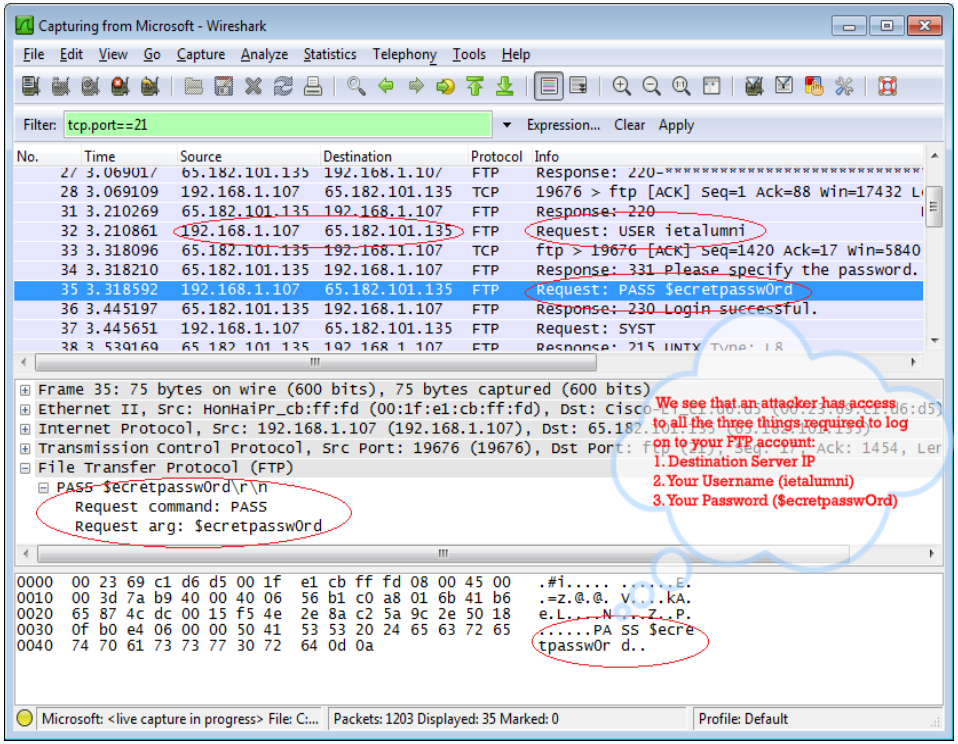
Eavesdropping

- Eavesdropping is listening in on communications (passive attack).
- Any communication performed in plain is subject to interception, e.g., HTTP.

[Ba10]

Sniffing Tool - Wireshark

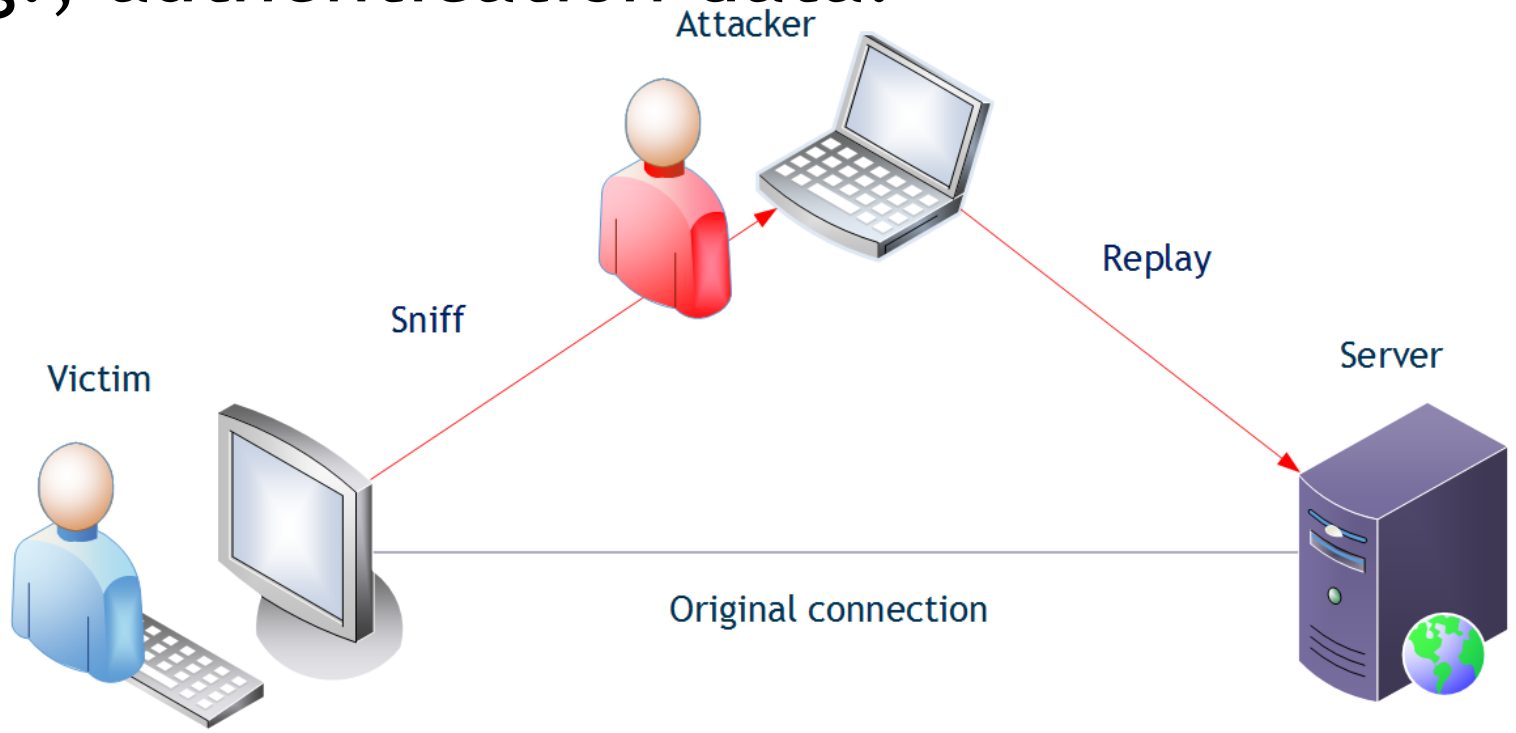
Eavesdropping can be done using a packet capturing tool (sniffer), e.g., Wireshark.



Source [http://engineering.deccanhosts.com/]

Replay Attacks

- A replay attacks is a retransmission of captured communications (valid data) e.g., authentication data.



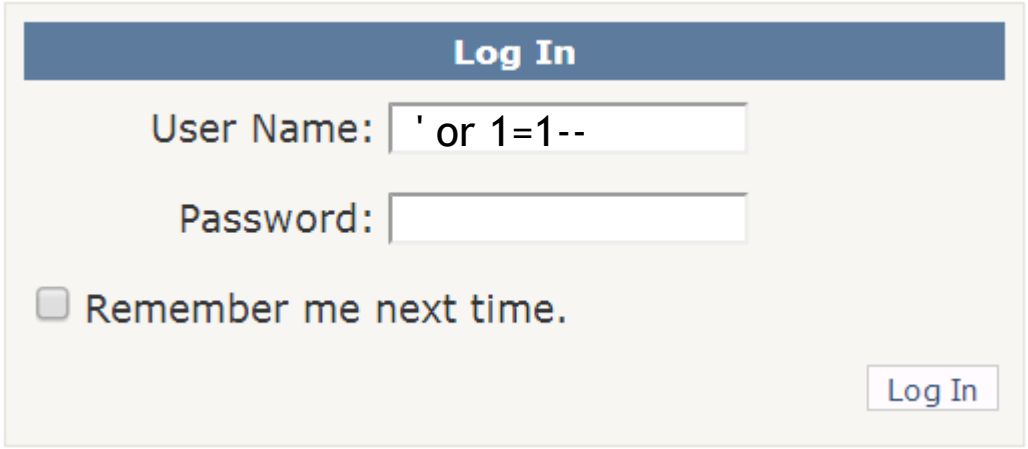
[Ba10]

Insertion Attacks

- 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.

[Ba10]

SQL Injection



1=1 always true

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

Commented line, because "-- "
is used for Comment in SQL

Source [http://www.c-sharpcorner.com/]

Buffer Overflow

- 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.

[Ba10]

mobile business

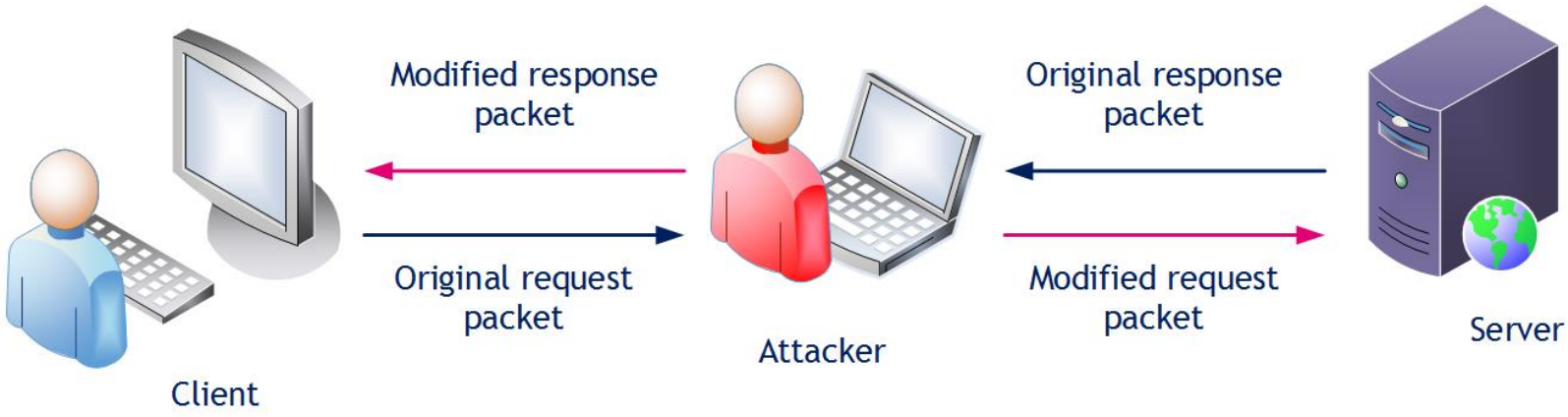
XSS (Cross-Site Scripting)

- Cross-site scripting (XSS) is similar to SQL injection, but it attacks future visitors to a Web page rather than grant access to the back-end database.
- An XSS attack submits script code to a benign or trusted Web site.
- Non-persistent requires a user to visit the crafted link.

[Ba10]

Man-in-the-Middle

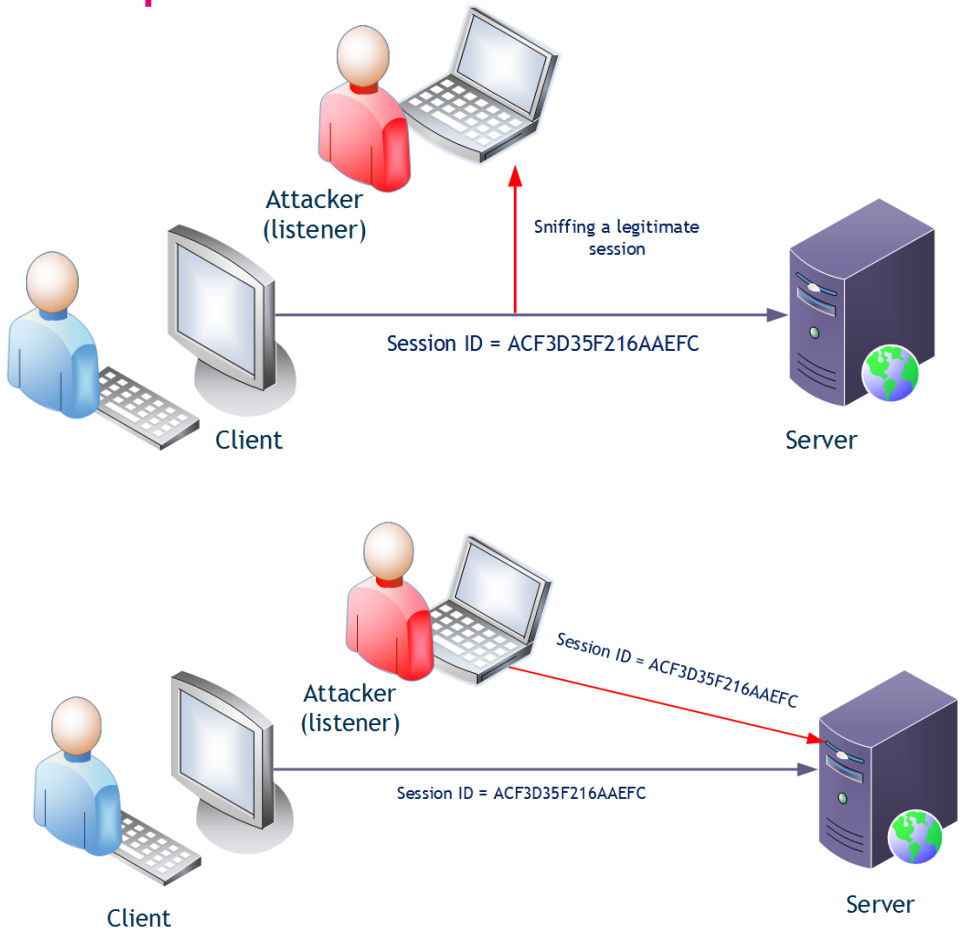
- Man-in-the-middle Attacks occur when a hacker intervenes in a communication session between a client and a server.



[Ba10]

Session Hijacking

Example:



- Step 1 - The attacker uses a sniffer to capture a valid token session called "Session ID",
- Step 2 – the attacker uses the valid token session to gain unauthorized access to the Web Server

Source [OWASP.org]

mobile business

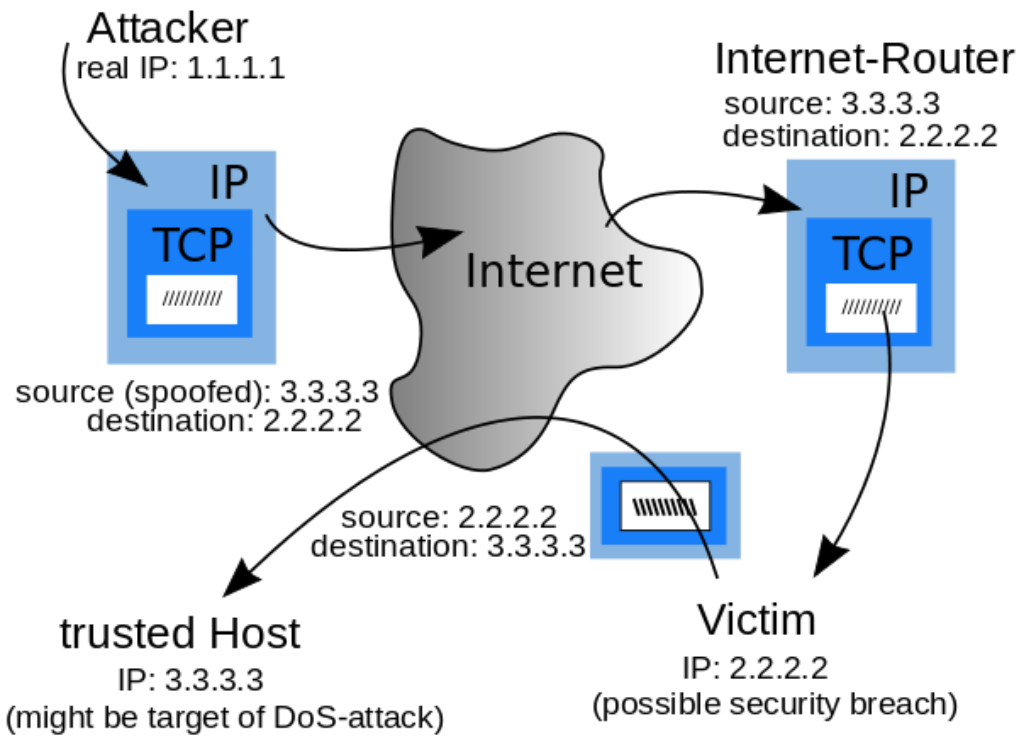
Spoofing

- Spoofing: falsification of information, an attack in which the client is given false information that leads the client to request a session with the hacker's computer rather than the real server.
- Examples: MAC spoofing, DNS spoofing, proxy manipulation.

[Ba10]

IP-Spoofing

- IP spoofing is the creation of IP packets with a forged source IP address.
- Attacker sends IP-packets with a faked sender address.



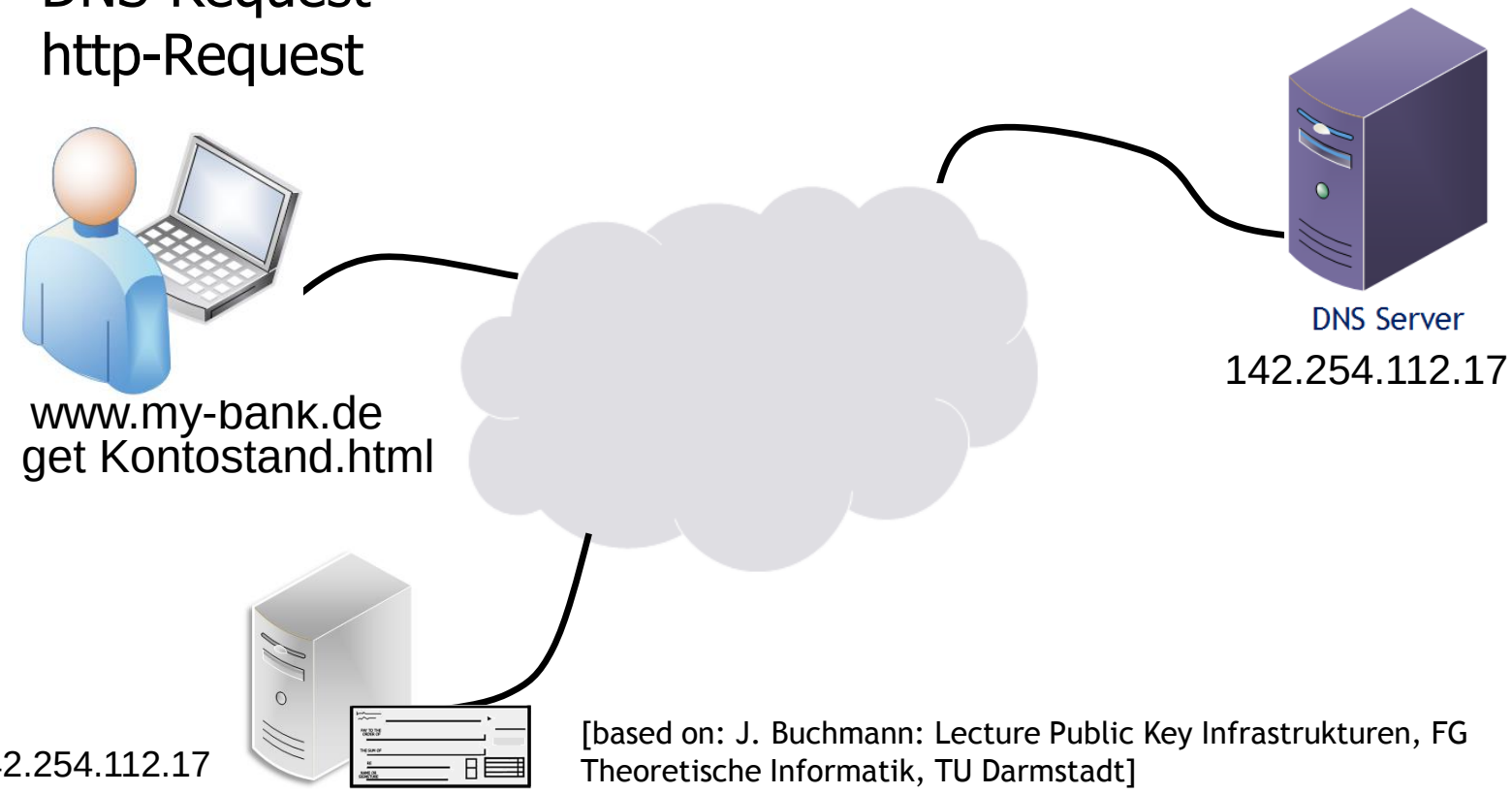
Source [Wikipedia]

Example: Online-Banking

www.my-bank.de/Kontostand.html

Actions of the browser:

1. DNS-Request
2. http-Request



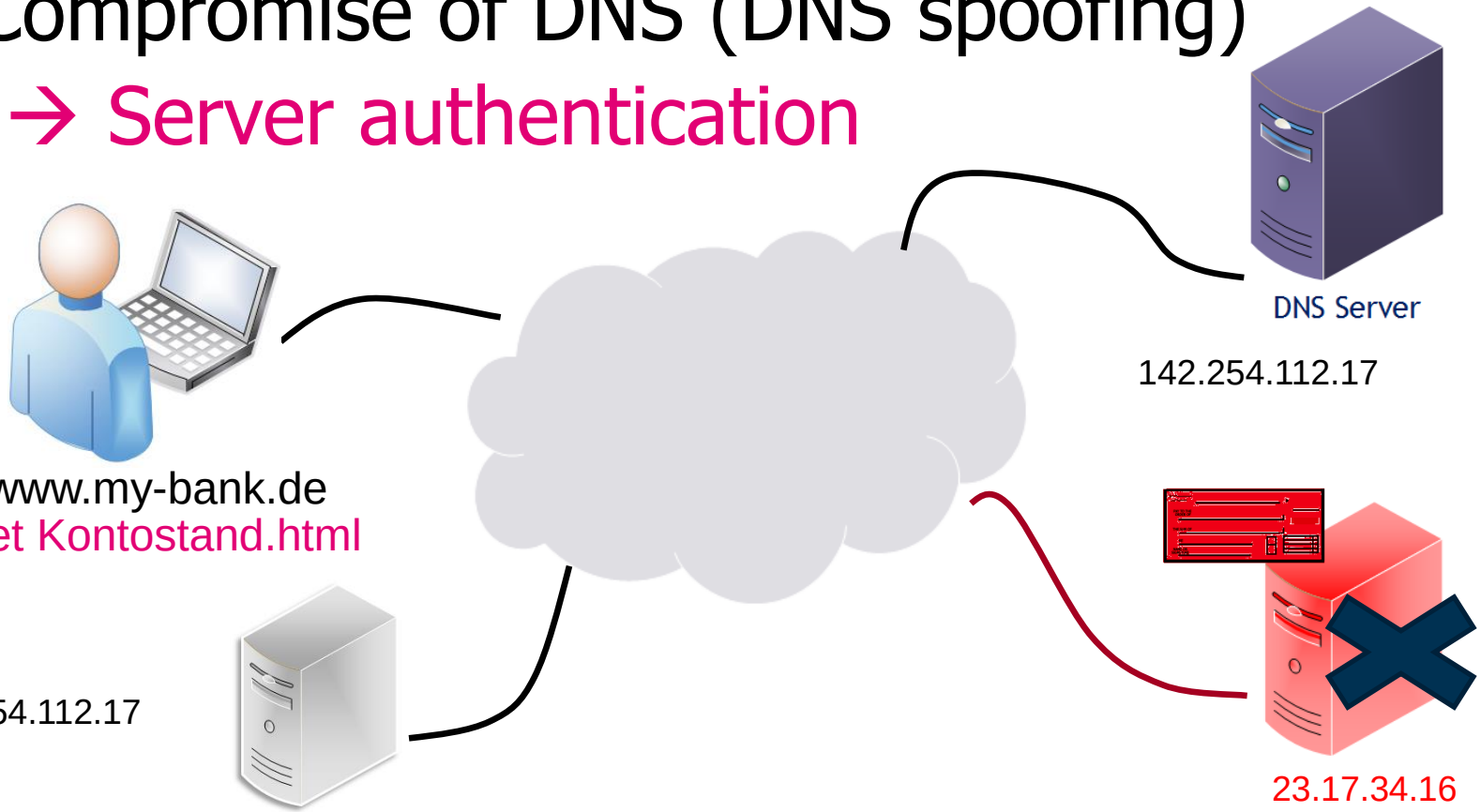
[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

DNS spoofing

Possible attacks:

1. Compromise of DNS (DNS spoofing)

   → Server authentication



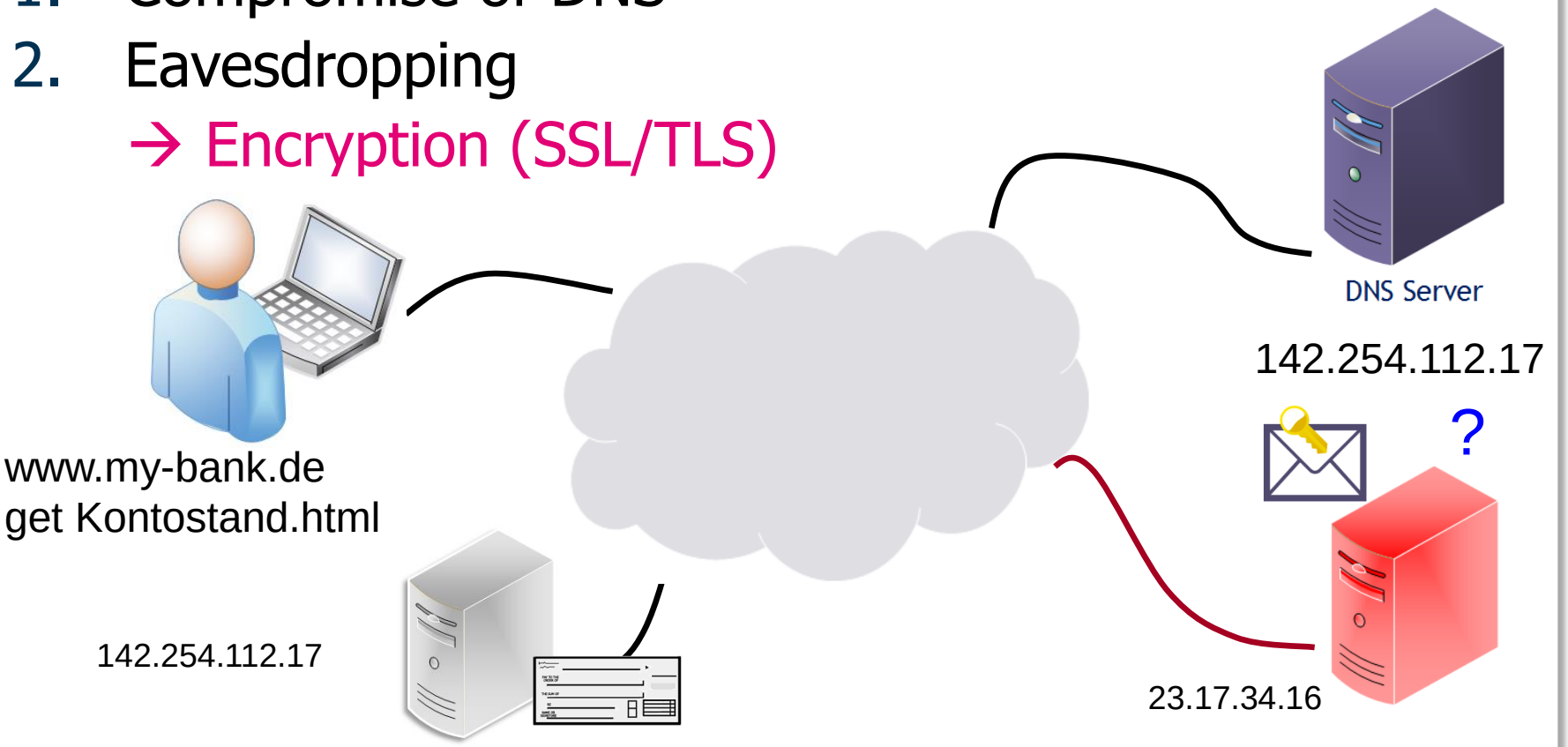
[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

HTTP sniffing

Possible attacks:

1. Compromise of DNS
2. Eavesdropping

   → Encryption (SSL/TLS)



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

Network and Resource Availability Threats

- An availability attack aims at preventing legitimate access or use of resources to delay of interrupt business, e.g., denial of service.
- Denial of Service (DoS) attacks interrupt the normal patterns of traffic, communication and response.

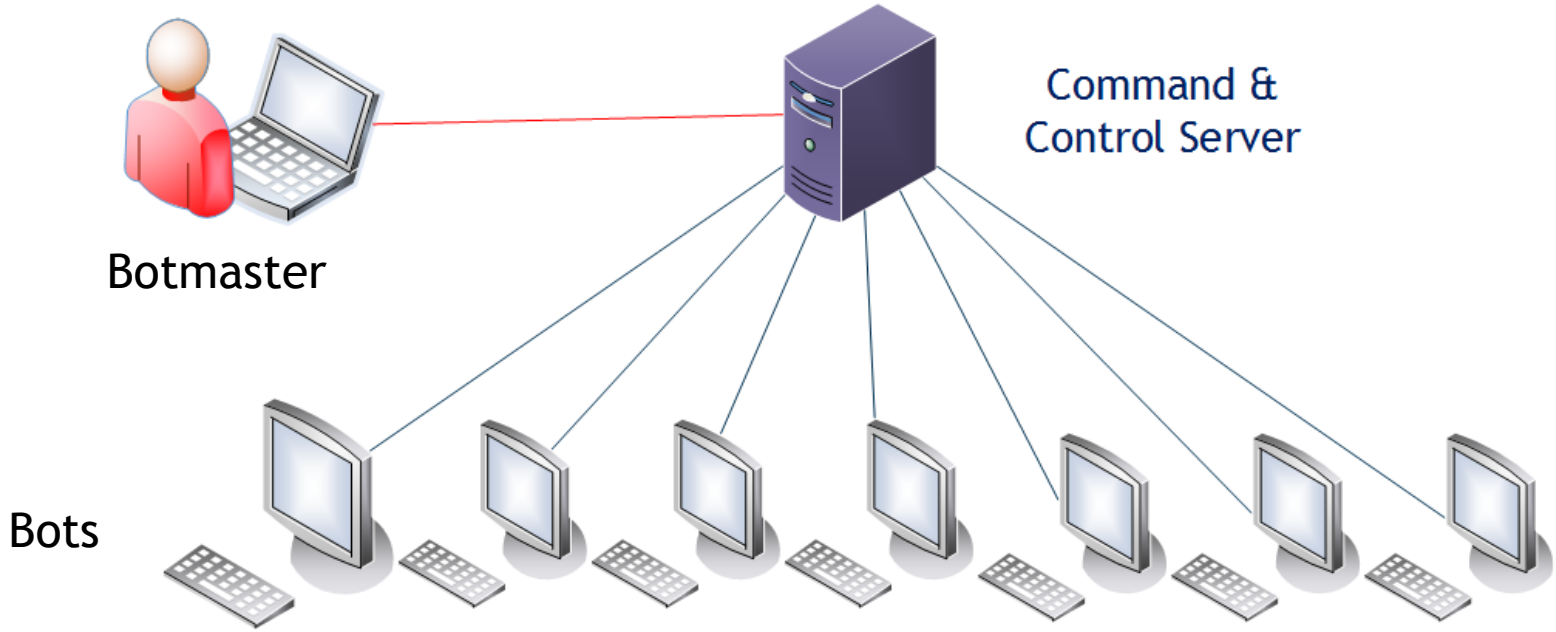
[Ba10]

Distributed Denial of Service (DDoS)

- Distributed denial of service (DDoS) attacks advance DoS attacks through massive distributed processing and sourcing.
- Based on agents, bots and zombies – malicious code implanted on victim systems across the Internet.

Botnets (1)

Type 1: based on one or more C&C, every bot is directly connected with Command & Control server.

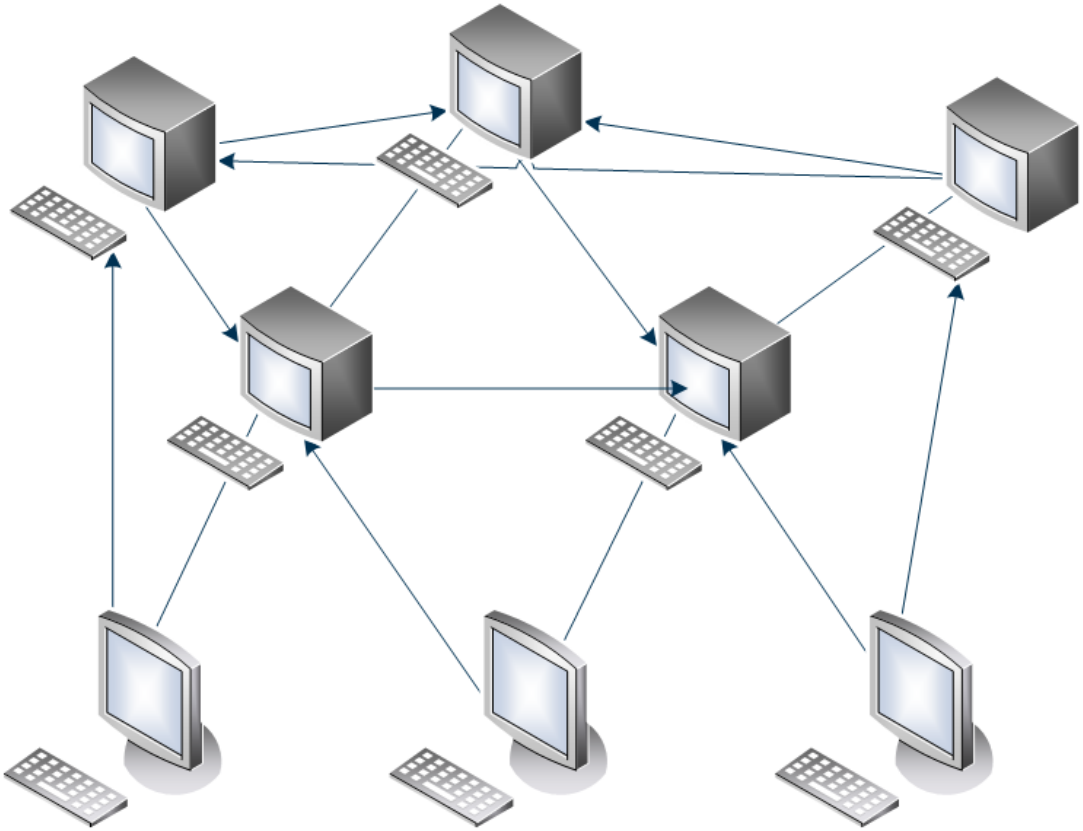


Botnets (2)

Type 2: Peer-to-Peer botnets, bots compose a mesh structure in which commands are also transmitted from the zombie to the zombie.

Servant bots

Client bots



mobile business

References

- **[De87] Dorothy Denning:** "An Intrusion- Detection Model", IEEE Transactions on Software Engineering, 13 (2), pp. 222-232
- **[Ta96] A.S. Tanenbaum:** Computer Networks, 3rd Edition, 1996 [4th edition available]
- **[Bi05] Matt Bishop:** *Introduction to Computer Security.* Boston: Addison Wesley, 2005, pp. 455-516
- **[Go06] Gollmann, Dieter.** *Computer Security, 2nd Edition.* Chichester, New York, Weinheim, Brisbane, Singapore, Toronto: John Wiley & Sons, 2006.
- **[Ba10] Jones & Bartlett:** Network Security, Firewalls, and VPNs
- **[He14] Heartbleed:** "The Heartbleed Bug", www.heartbleed.com

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Jetzabel M. Serna-Olvera
Goethe University Frankfurt
E-Mail: Jetzabel.Serna-Olvera@m-chair.de
WWW: www.m-chair.de