

Information & Communication Security (WS 18/19)



Network Security I

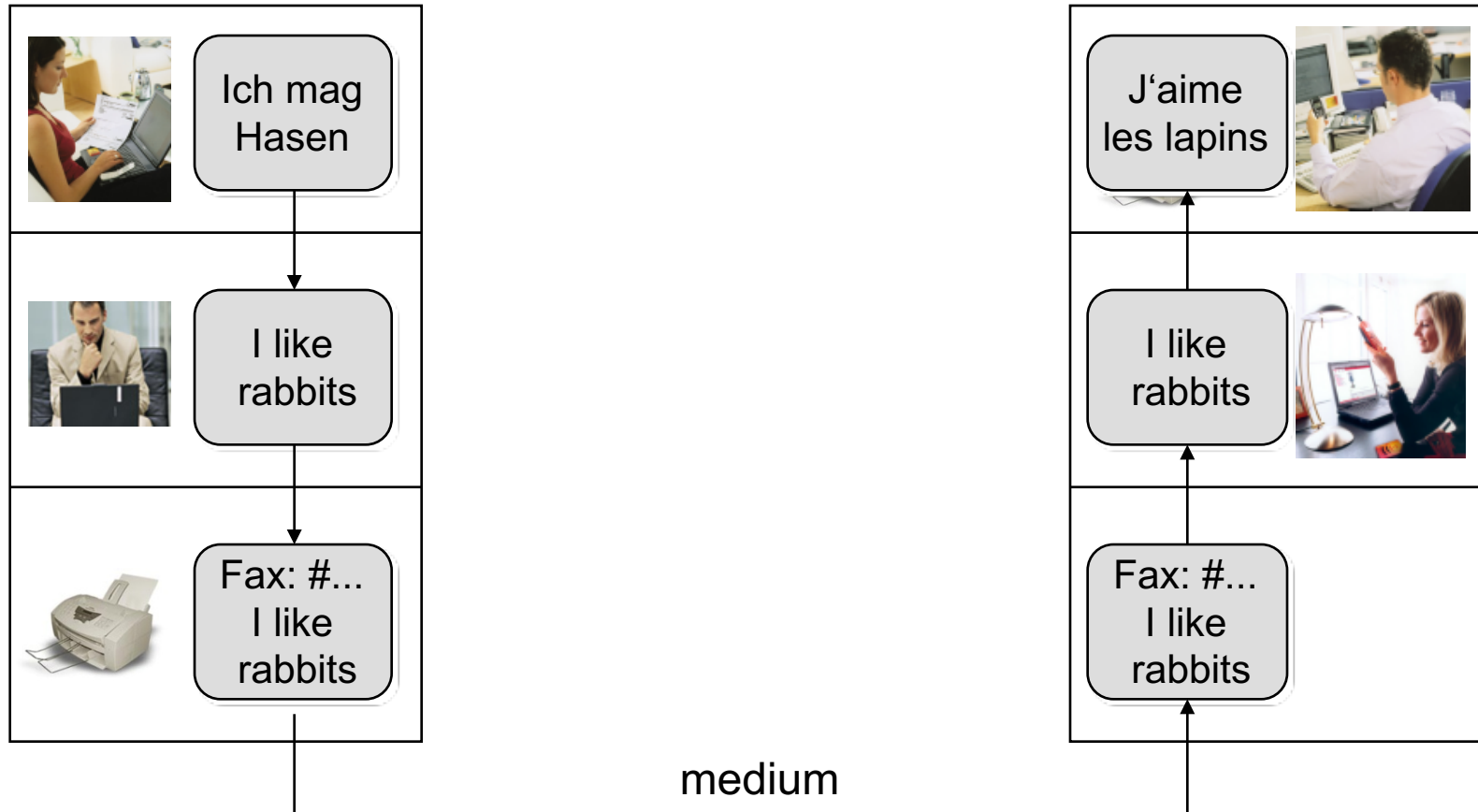
Prof. Dr. Kai Rannenber
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

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

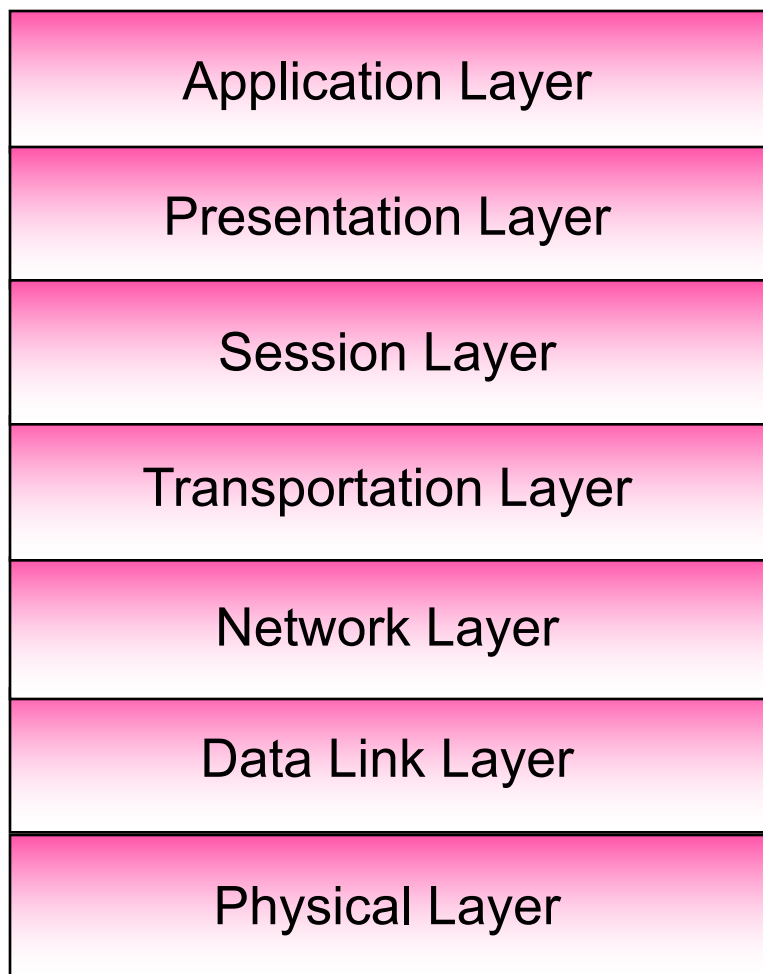
- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security

- **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

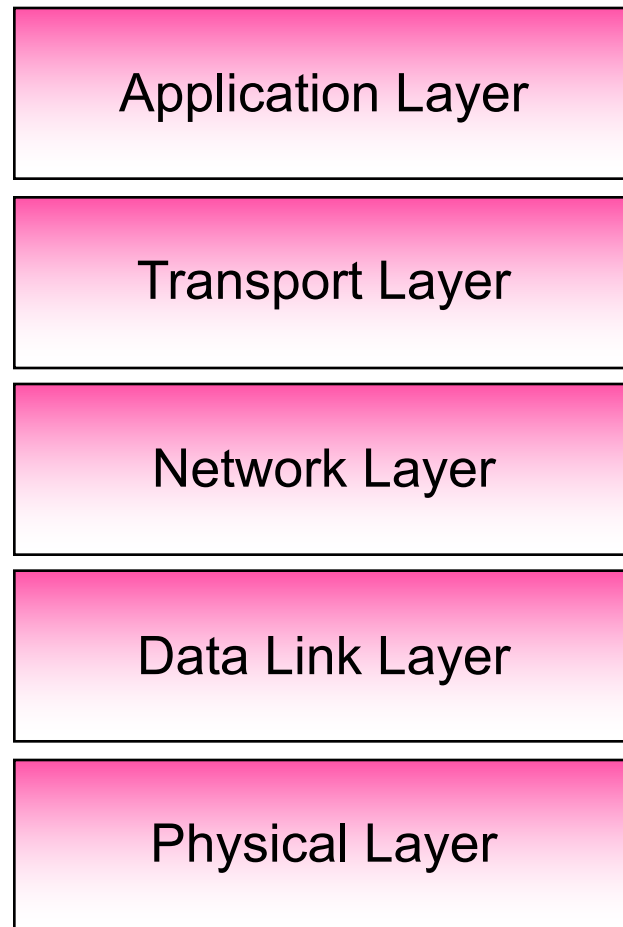


ISO/IEC OSI Reference Model

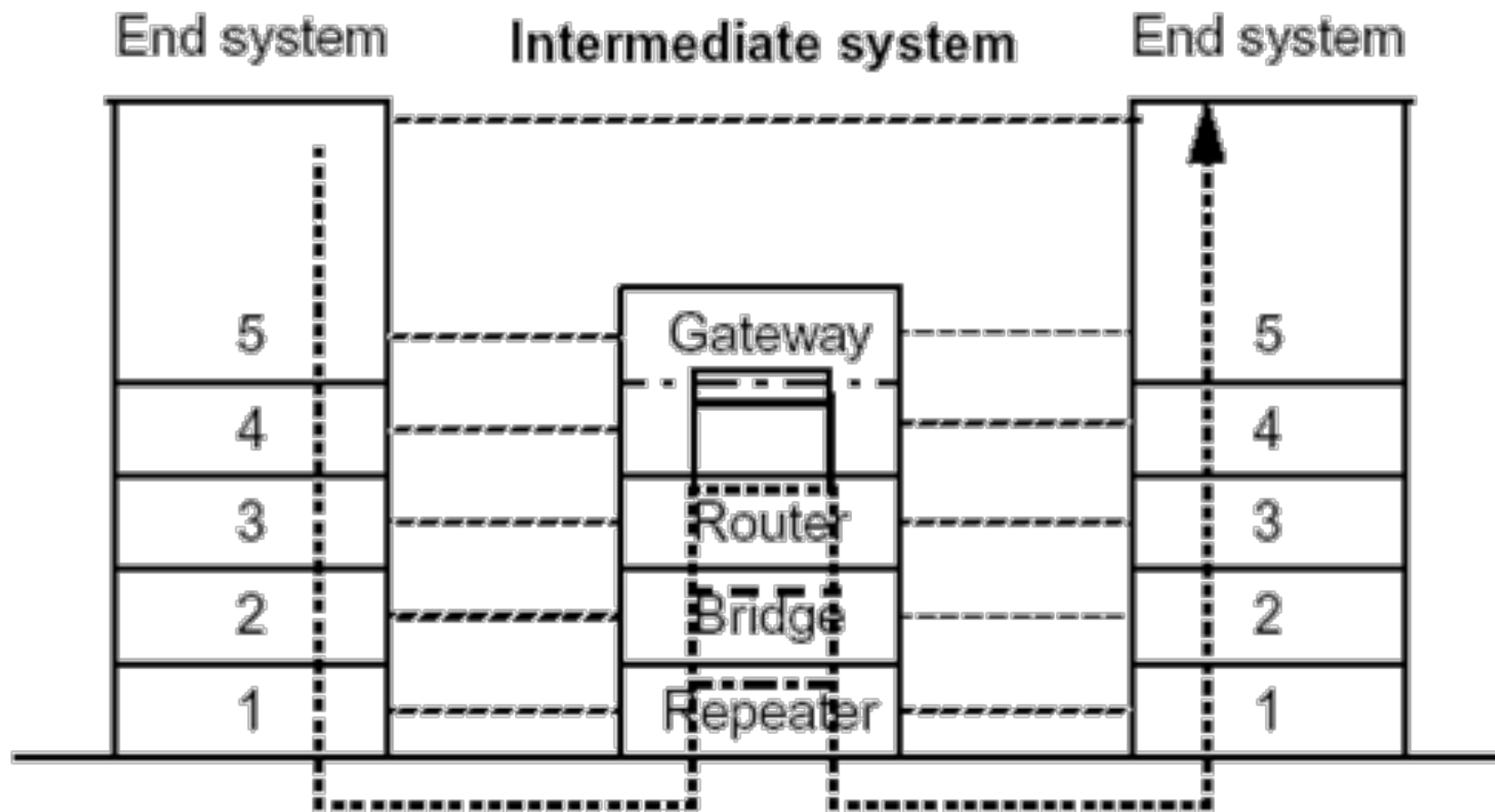


- Information technology – Open Systems Interconnection – Basic Reference Model
- 7-Layer-Model
 - First version
ISO/IEC 7498-1:1984
 - Current version
ISO/IEC 7498-1:1994

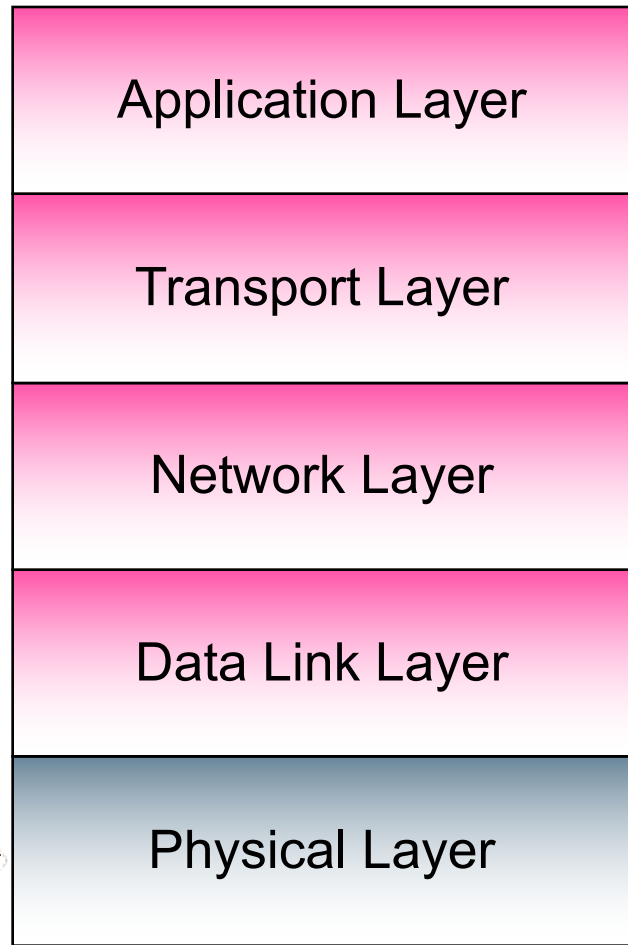
Internet Reference Model



Communication Example

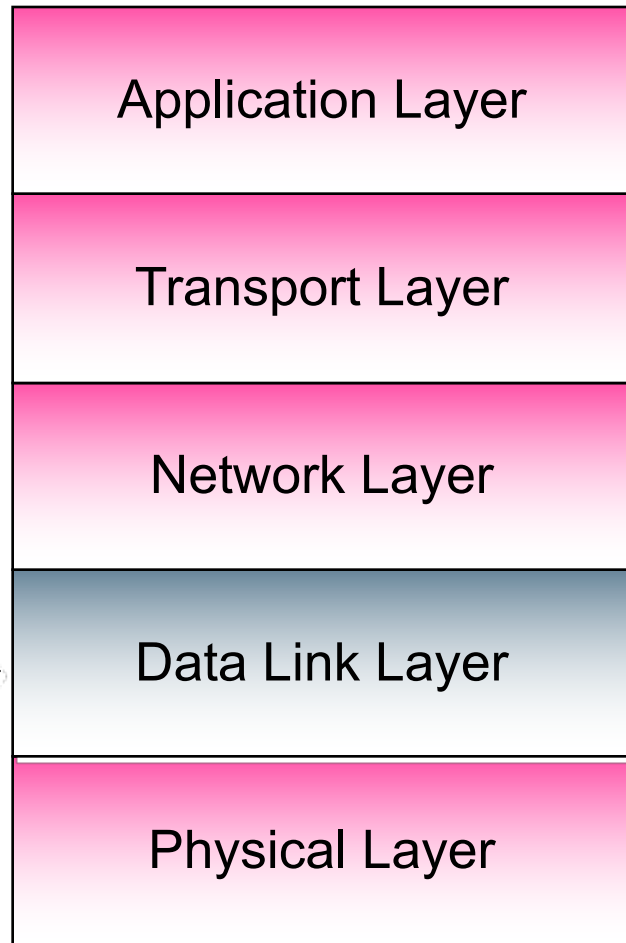


[Based on Tan96]



Tasks:

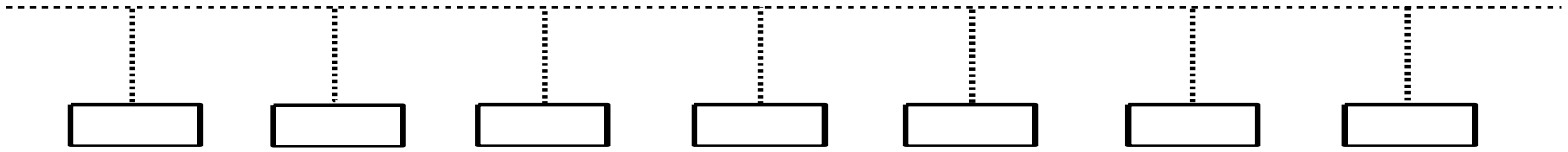
- Bit transfer
- Mechanic
(connector, medium)
- Electronic
(signal durability of a bit,
voltage)



Tasks:

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

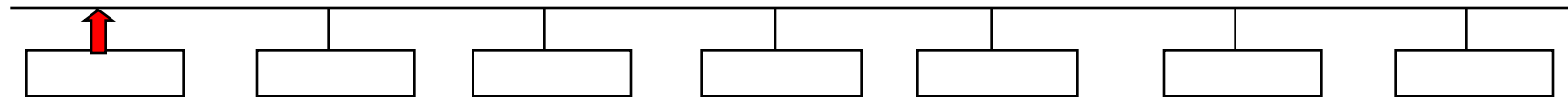
- **Bus-Network**



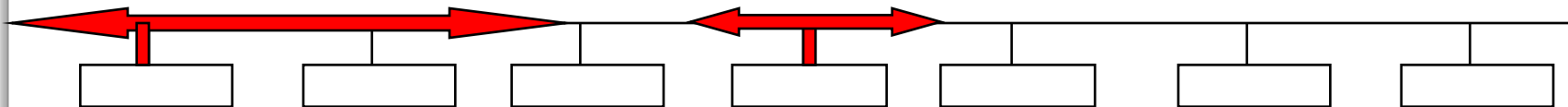
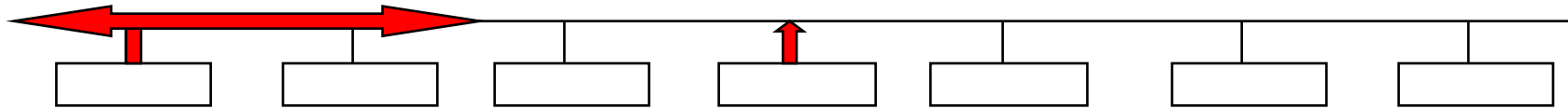
- Developed by XEROX
- Additional nodes can easily be added.
- Protocol: Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

CSMA/CD:

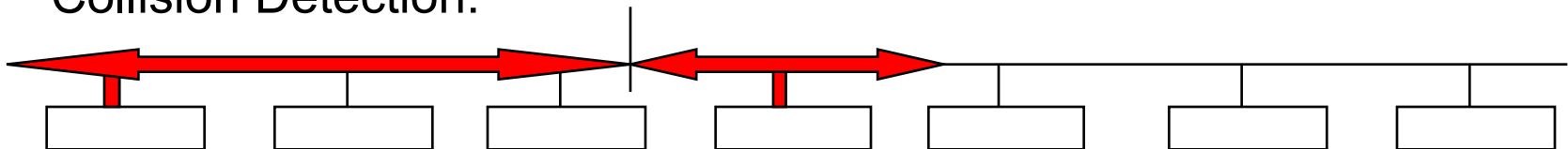
Carrier Sense:



Multiple Access:

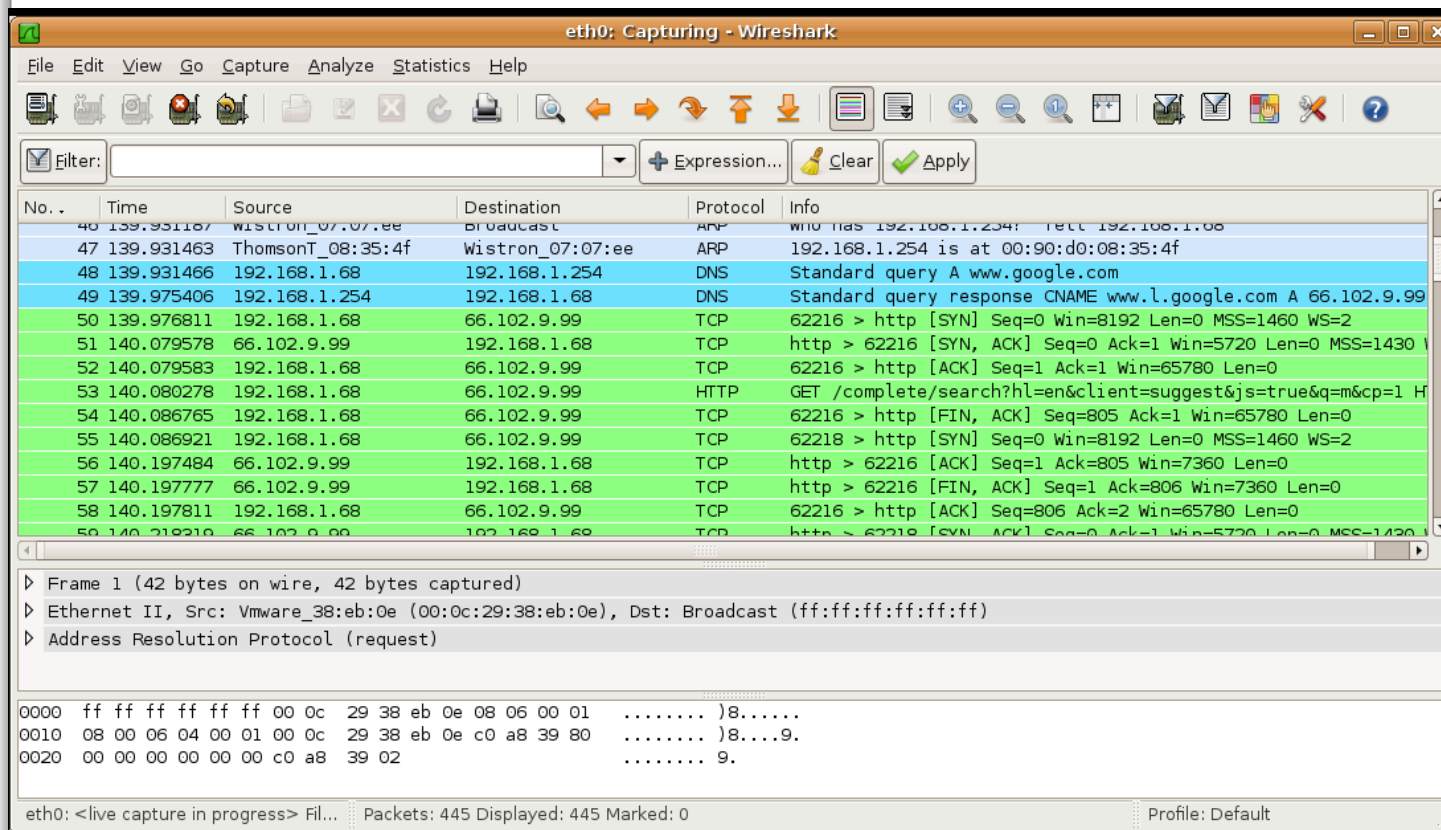


Collision Detection:



Eavesdropping of frames

i.e. Wireshark:



No. . .	Time	Source	Destination	Protocol	Info
47	139.931187	wistron_07:07:ee	broadcast	ARP	who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.218210	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

Frame 1 (42 bytes on wire, 42 bytes captured)

- Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

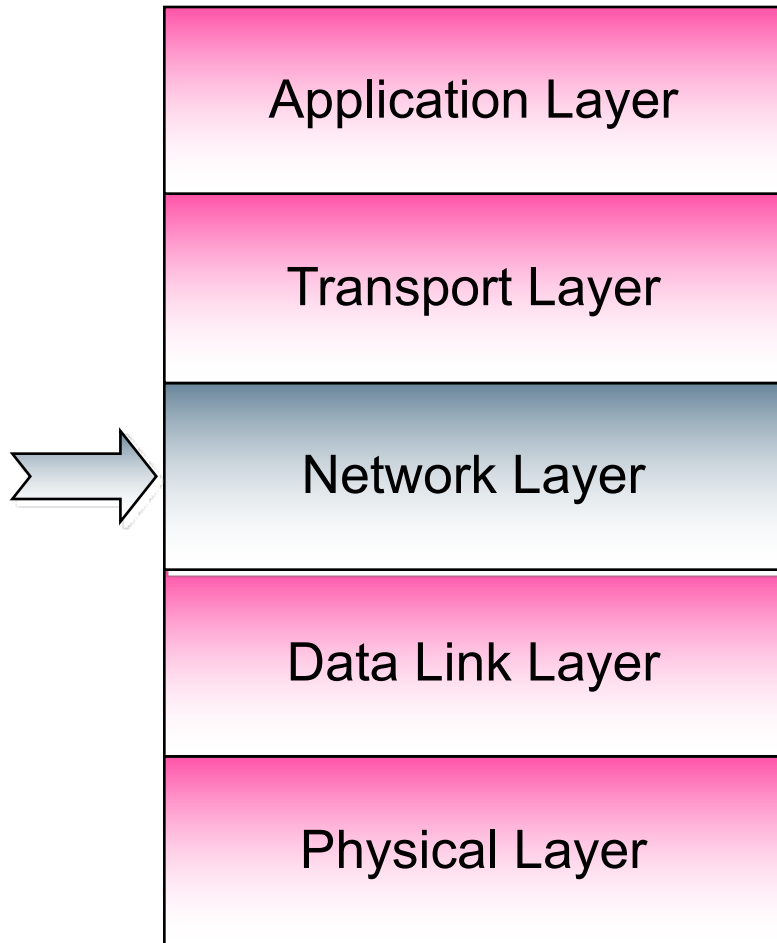
```

0000  ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01  ..... )8.....
0010  08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80  ..... )8....9.
0020  00 00 00 00 00 00 c0 a8 39 02  ..... 9.
  
```

eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

Meta-data of packets of higher protocol layers

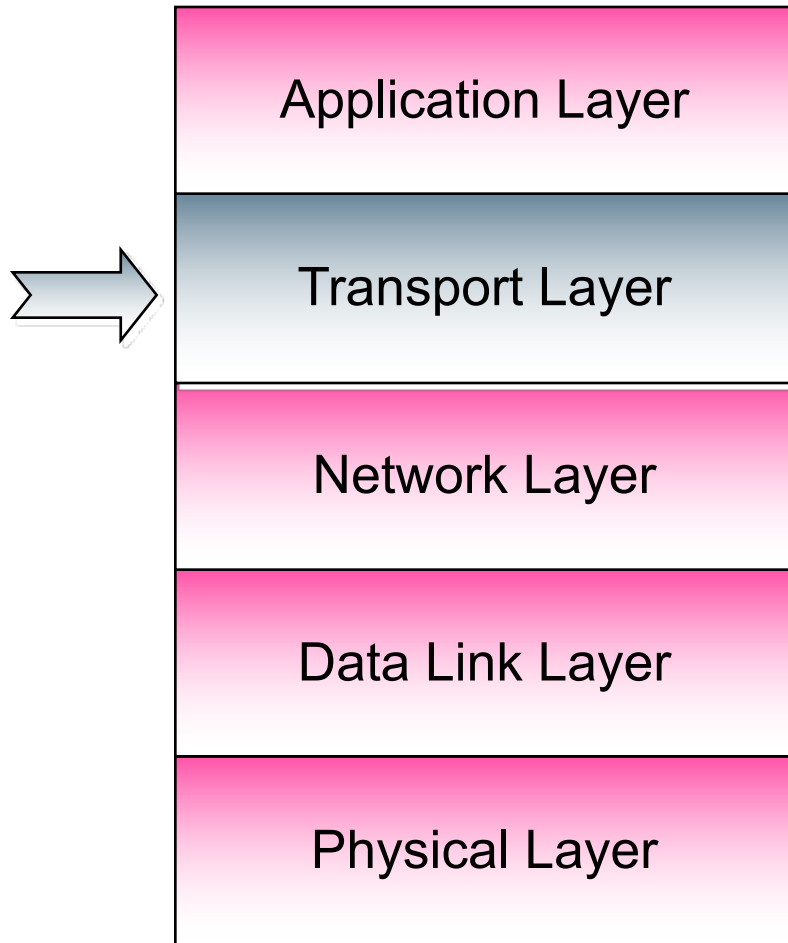
[Based on Wireshark]



Tasks:

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

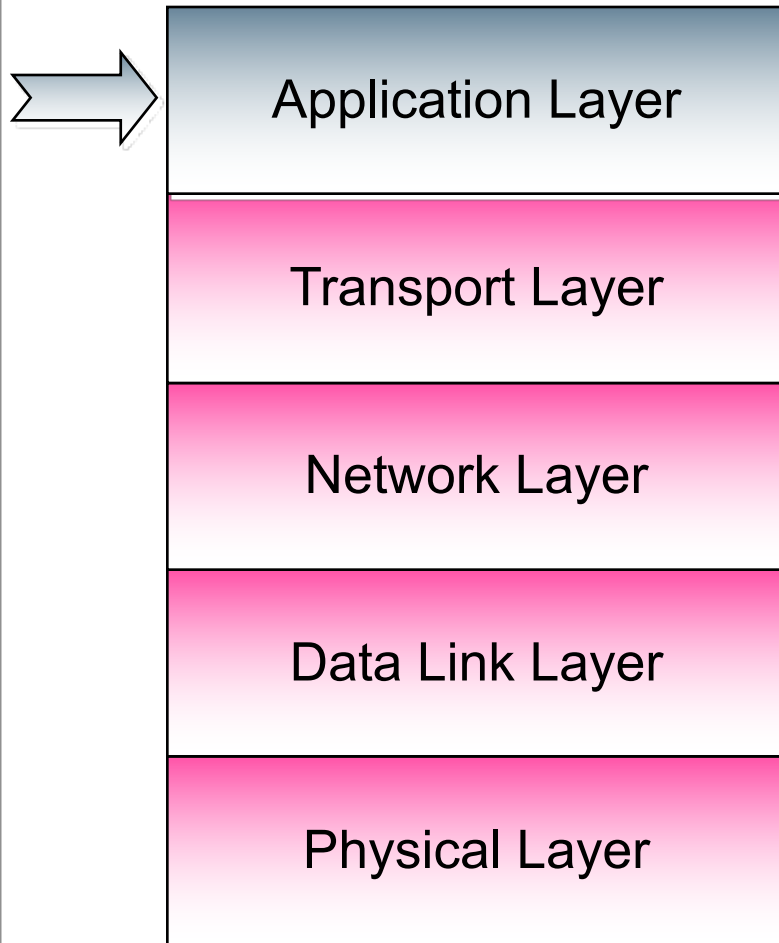
For example: IP



Tasks:

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

For example: TCP, UDP



Tasks:

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

SMTP: Simple Mail Transfer Protocol

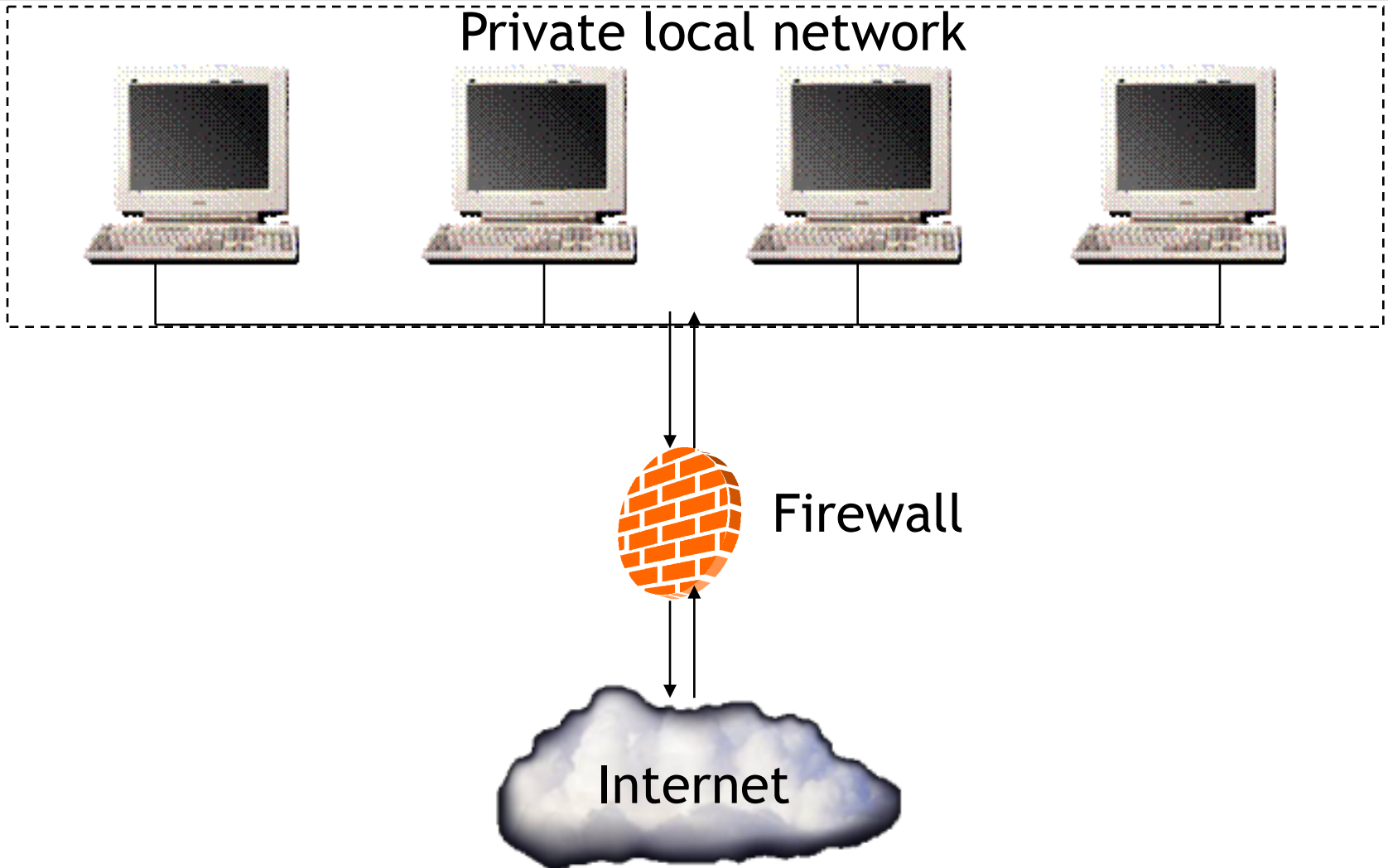
HTTP: Hyper Text Transfer Protocol

FTP: File Transfer Protocol

- 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]



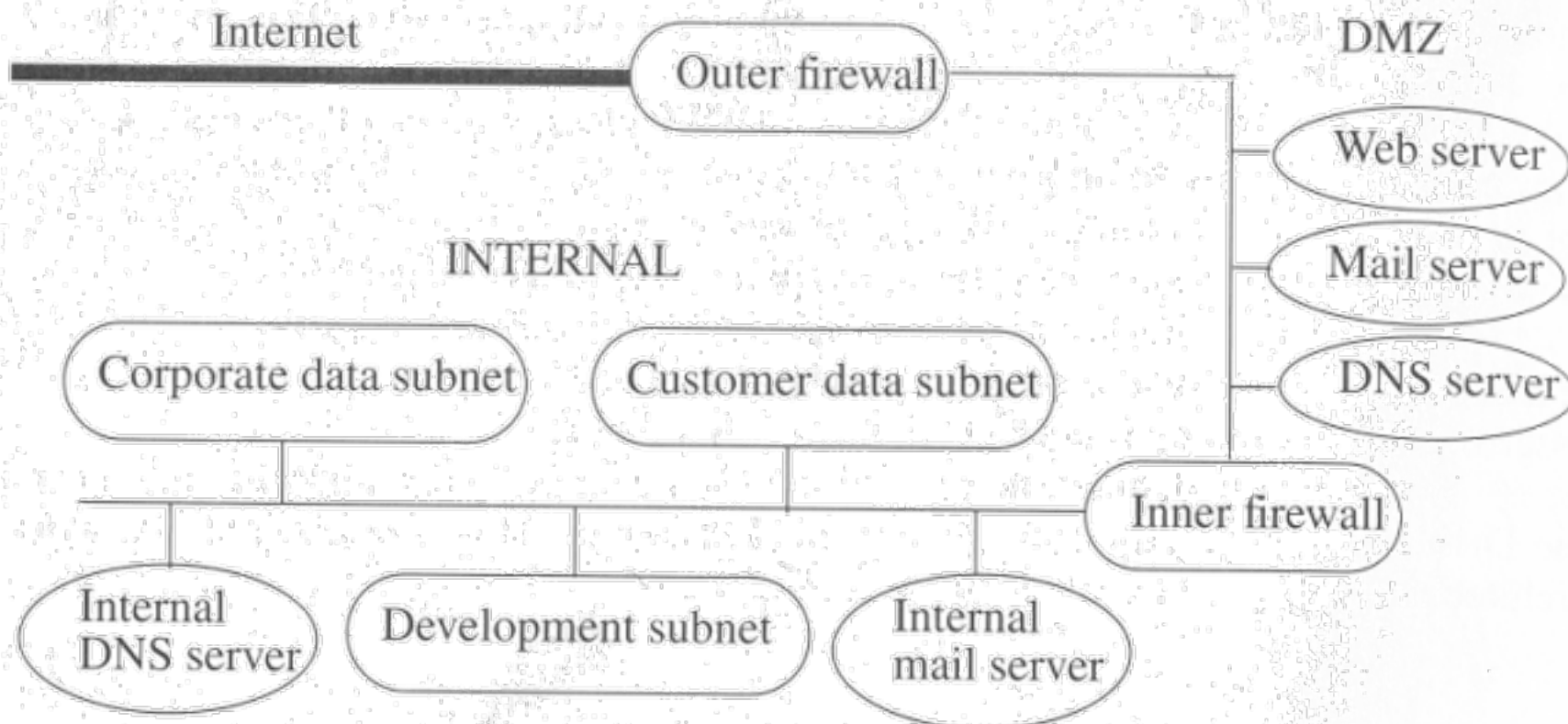
- Filtering firewall: perform access control on the basis of attributes of the packet headers.
- Application-level firewall (proxy firewall): uses proxies to perform access control. A proxy firewall adds to a filtering firewall the ability to base access on content.

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

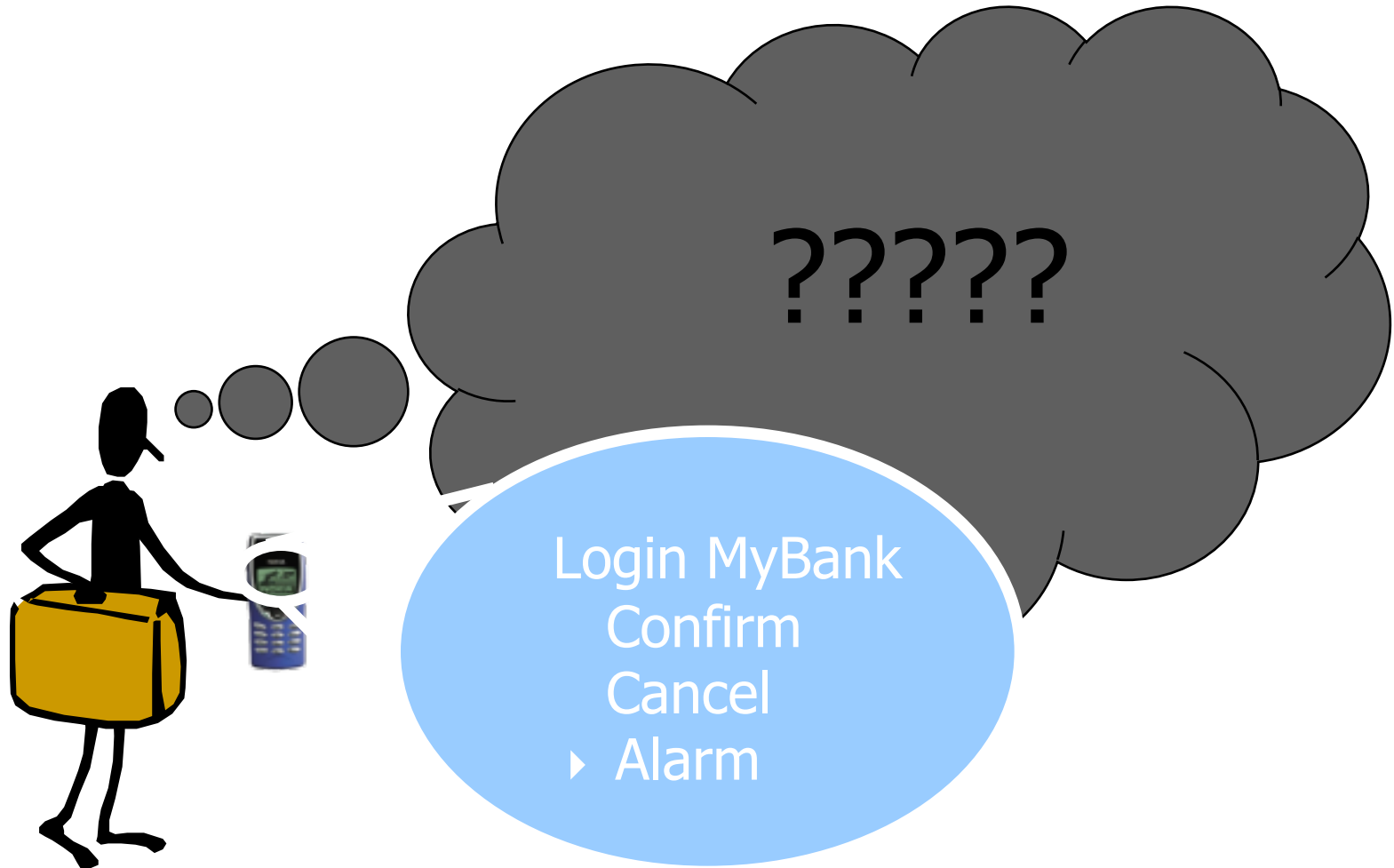
Demilitarized Zone (DMZ)

- 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.

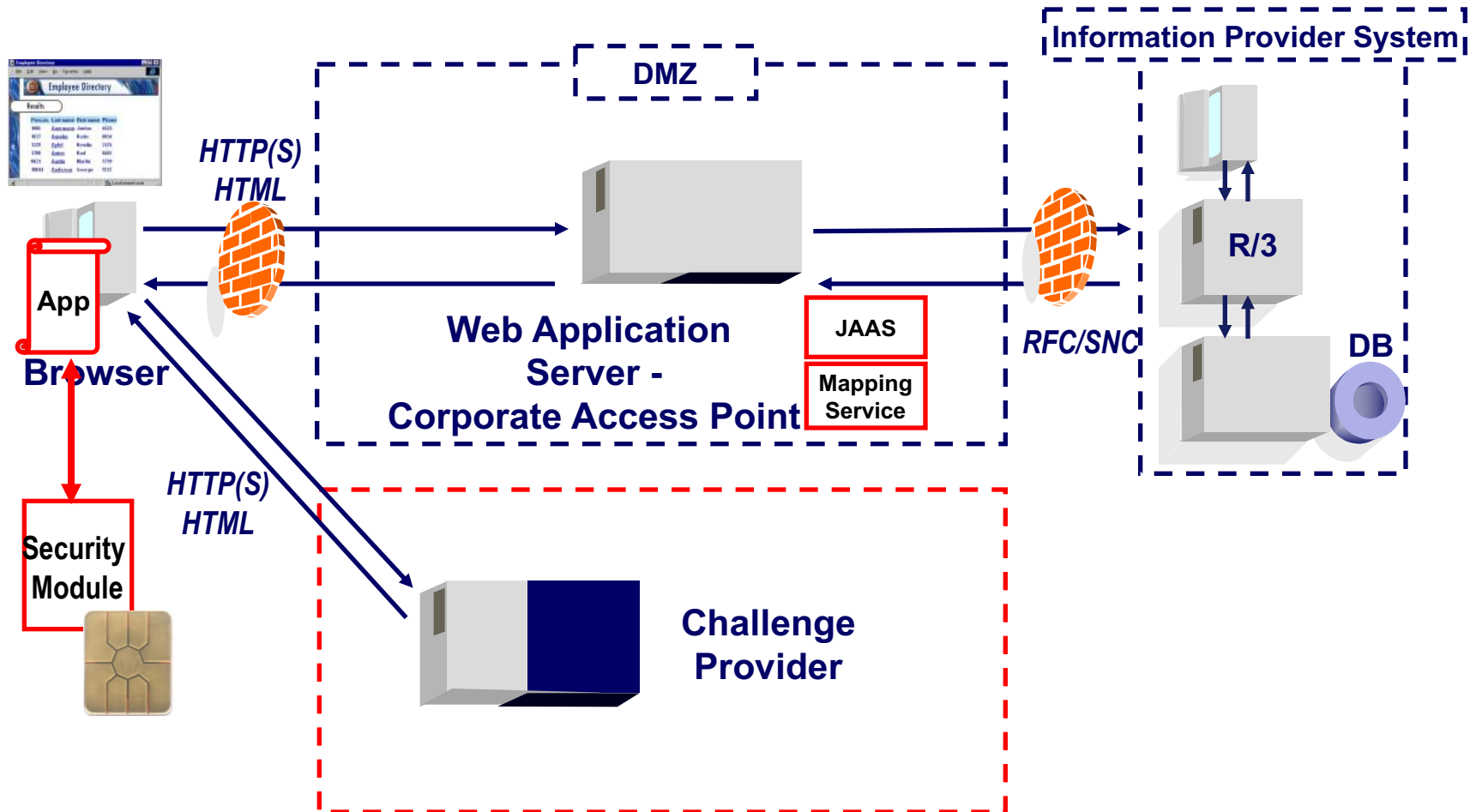
Network using a DMZ



Example: CamWebSIM Additional Channel for Login Authorisation - User view



Example: WiTness Security Module for Login Authorisation - System view



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 - *rootkit*).
 - Can eliminate many errors arising from incorrect installation and perform routine steps to clean up detritus of the attack.

- 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.

- *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.

- *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)*

Network Flight Recorder (NFR)

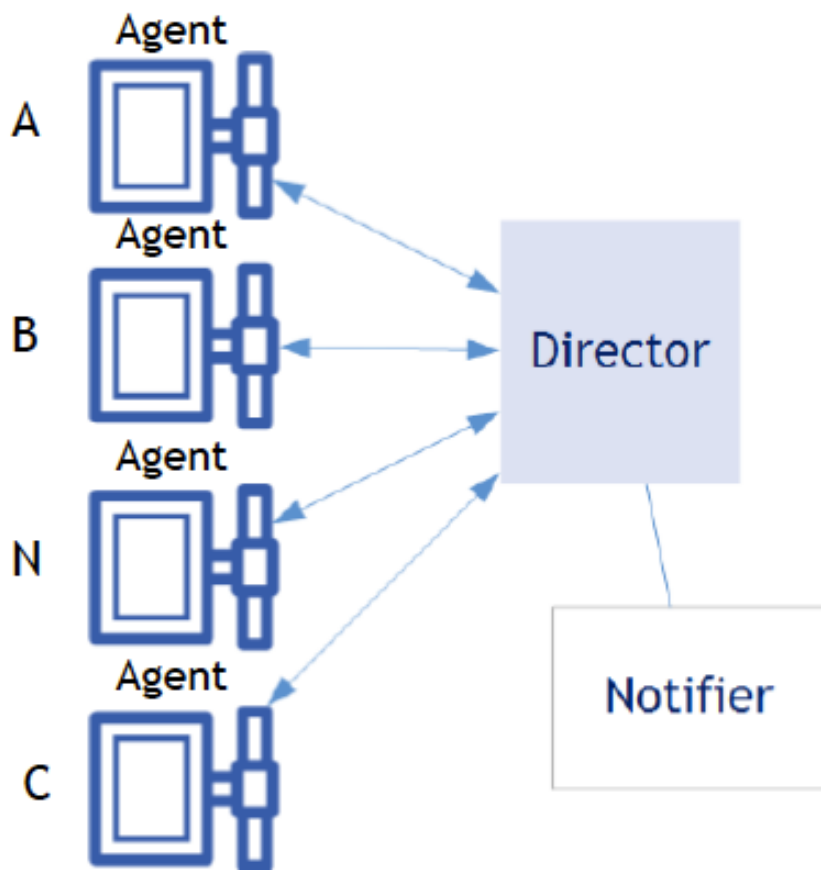
- NFR has three components:
 - The *packet sucker* reads packets off the network.
 - The *decision engine* uses filters written in a language called N-code to extract information.
 - The *backend* writes the data generated by the filters to disk.

Specification Based Detection

- *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.)

- 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)*

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



[Honeypot]

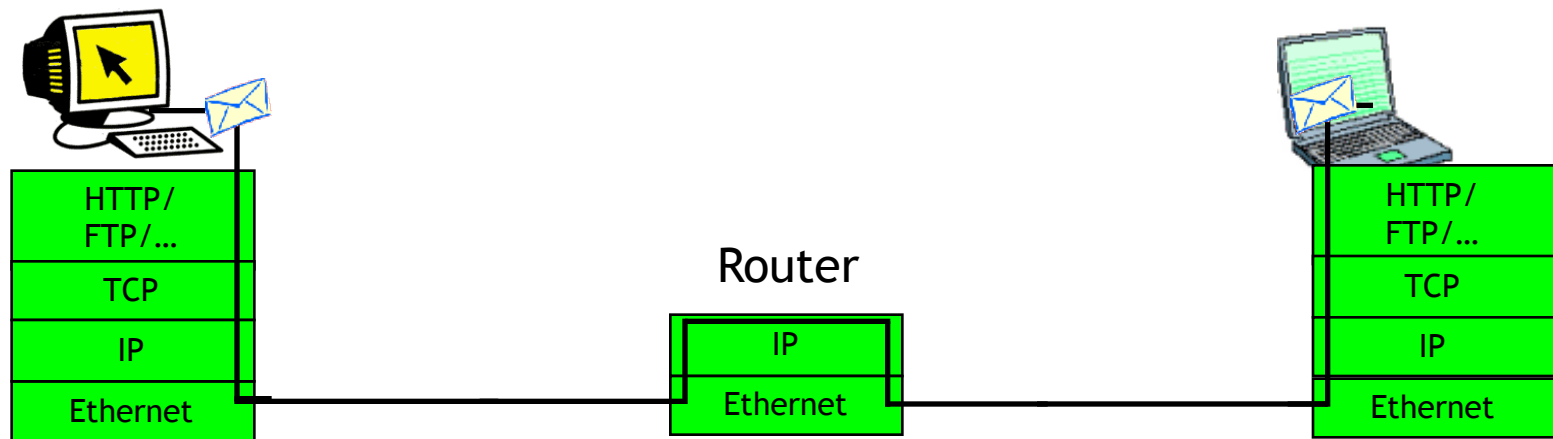
- Introduction
- Infrastructure Security Components
 - Firewalls
 - Demilitarized Zone
 - Intrusion Detection
- Security Protocols
 - Virtual Private Networks
 - Secure Socket Layer
 - IPsec
- Application Layer Security
- Wireless / Mobile Security

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

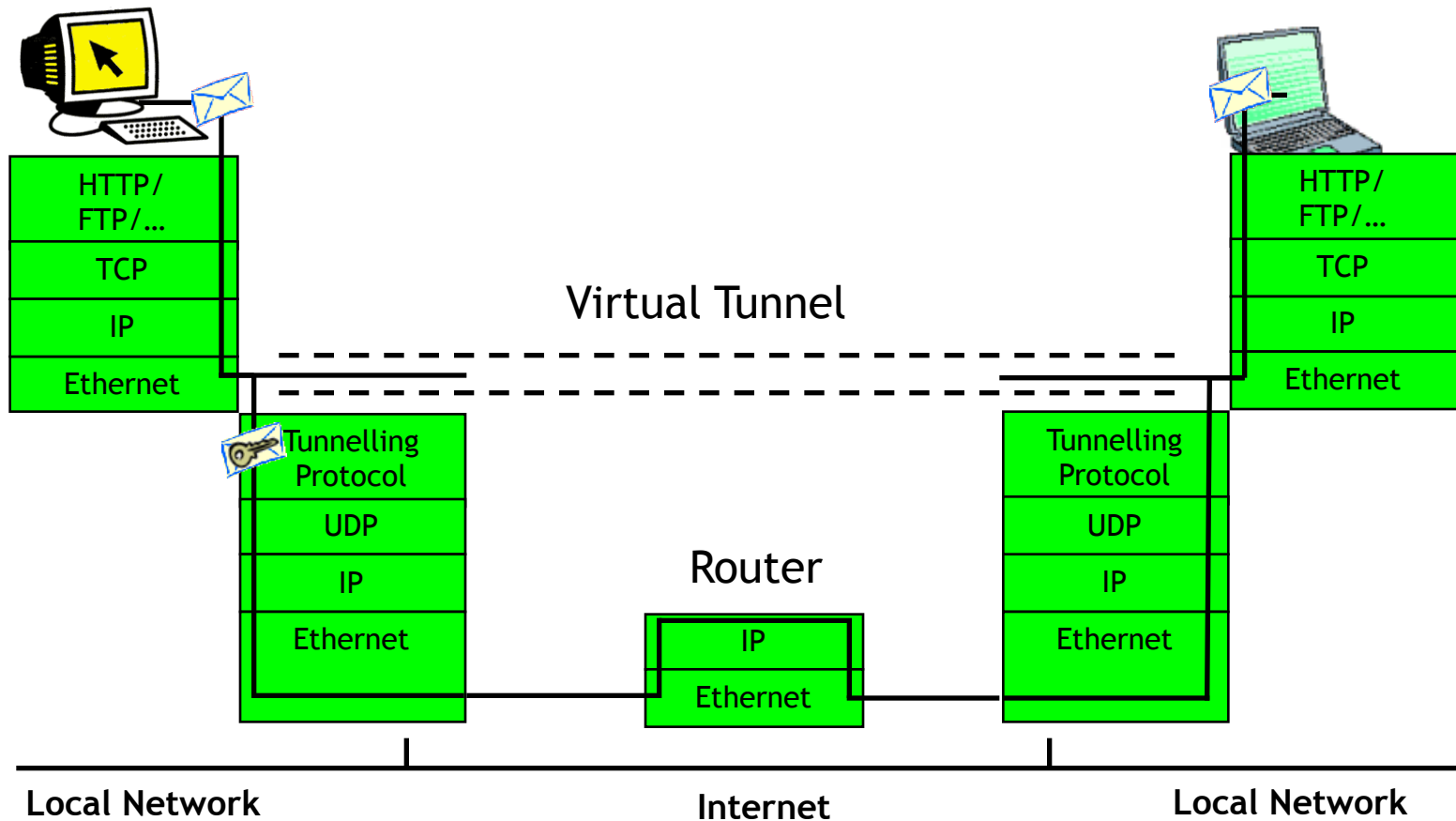
Virtual Private Network (VPN)

- 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.

Communication without a VPN



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



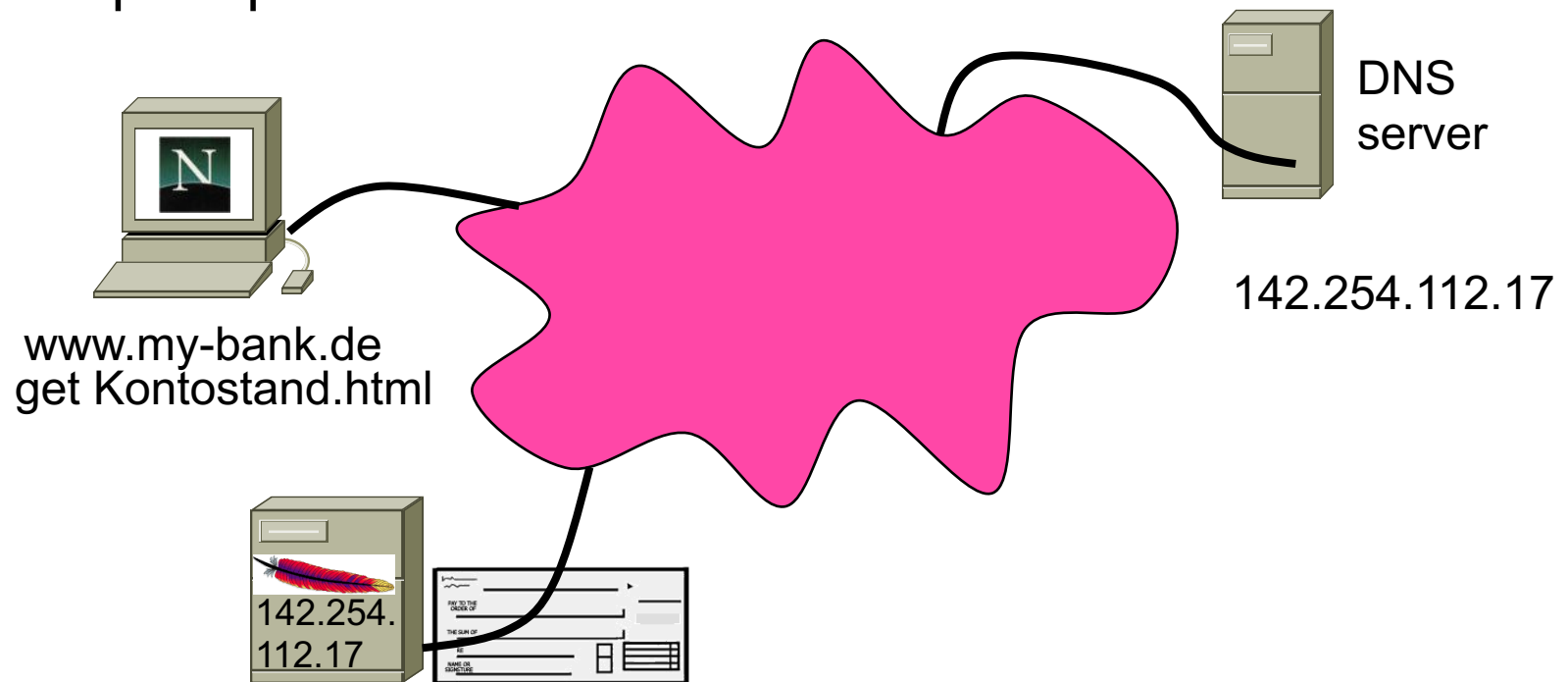
[Based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

- 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:

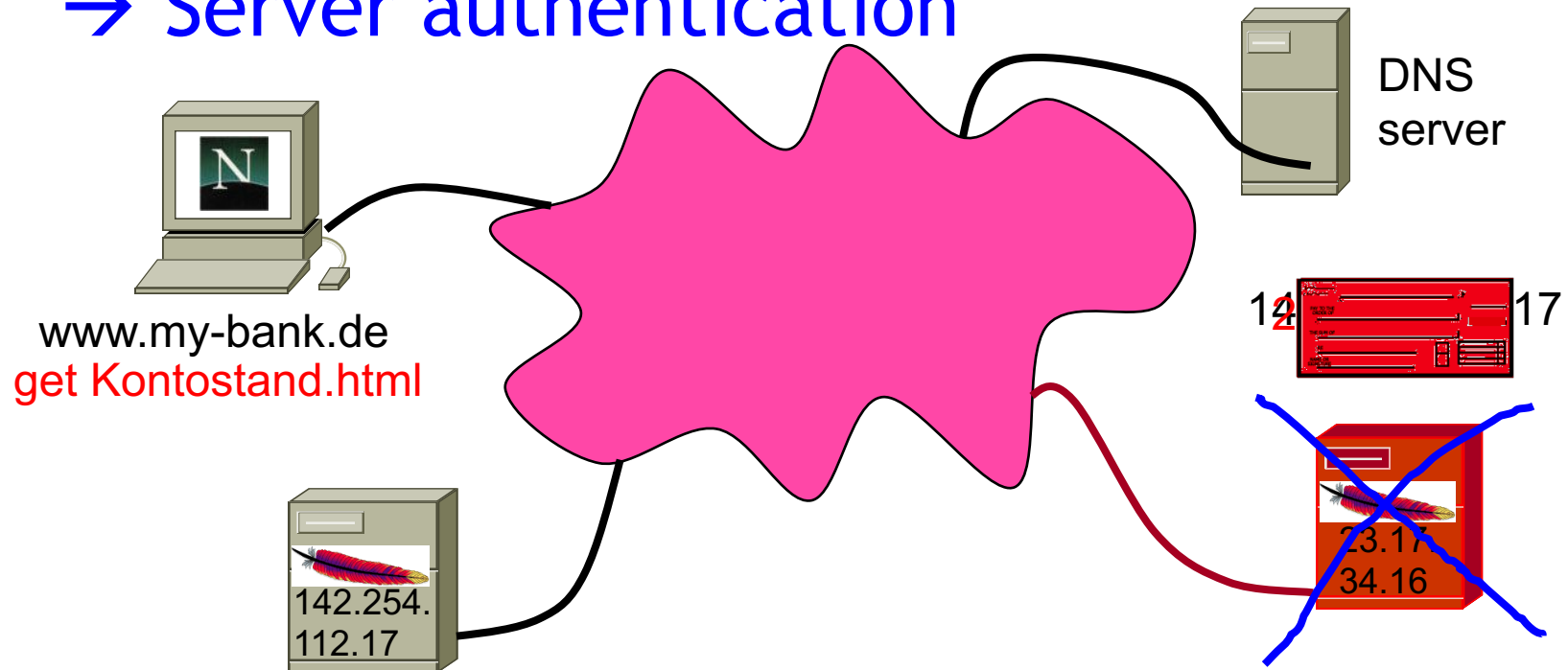
1. DNS-Request
2. http-Request



Possible attacks:

1. Compromise of DNS (DNS spoofing)

→ Server authentication

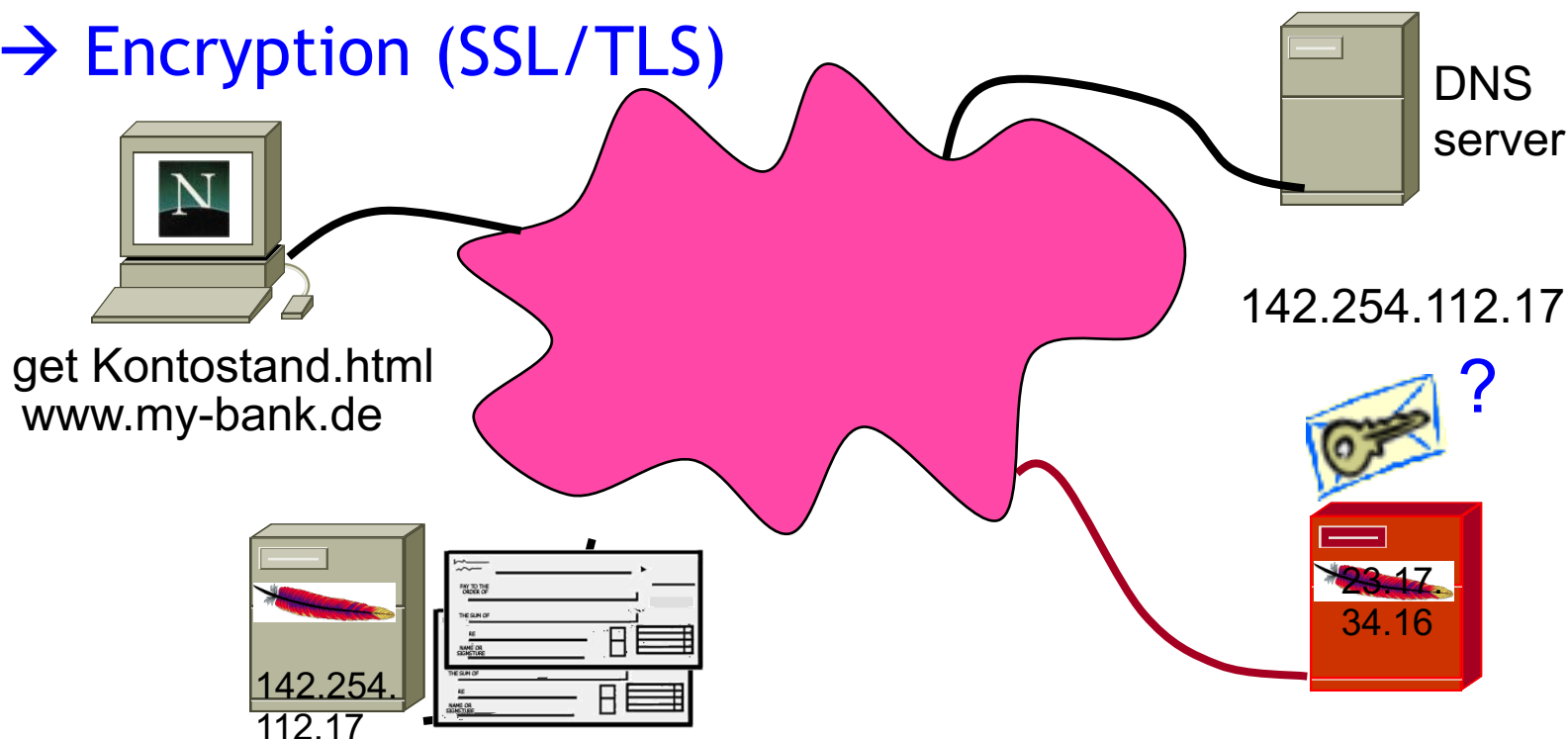


[based on: J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

Possible attacks:

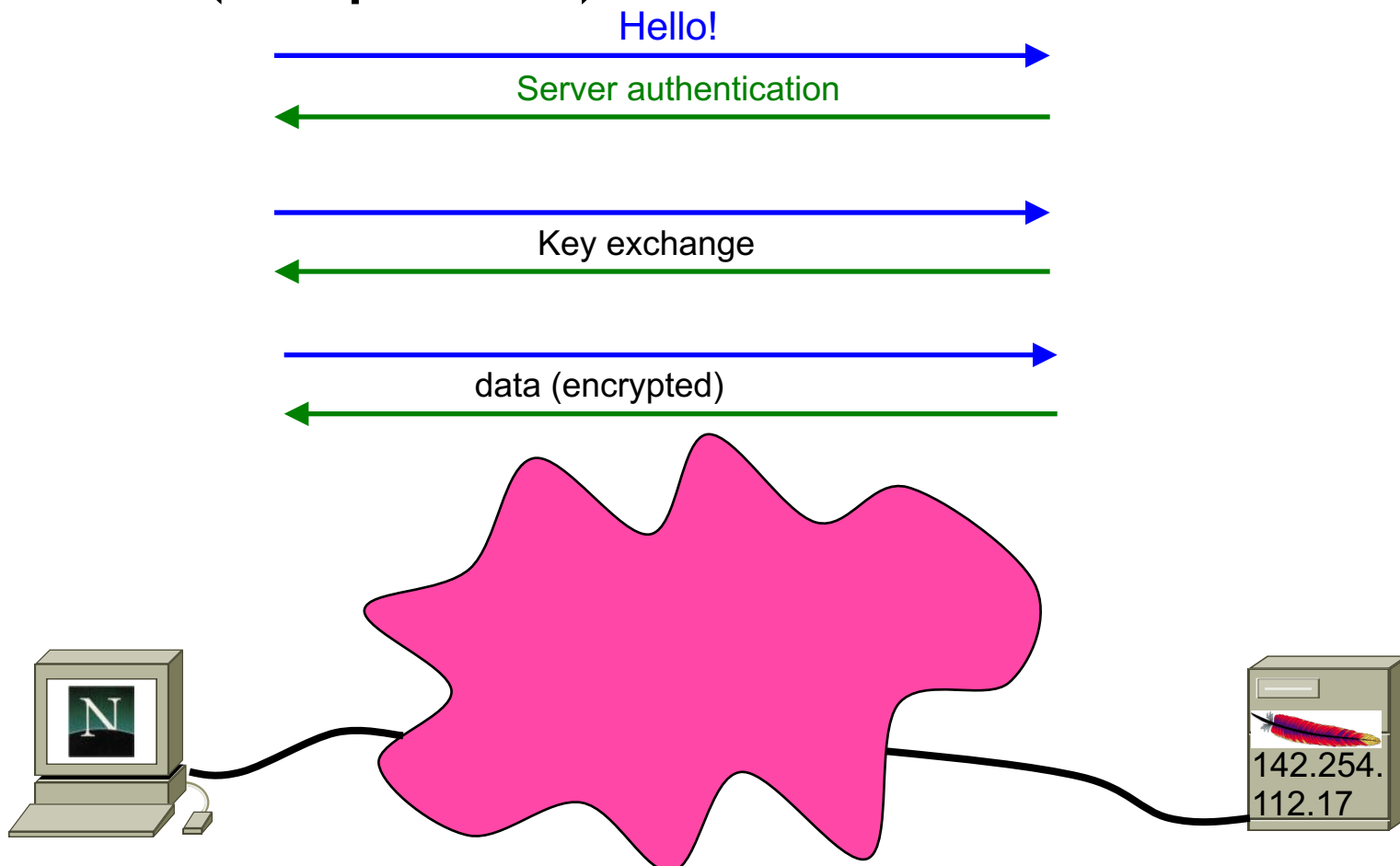
1. Compromise of DNS
2. Eavesdropping

→ Encryption (SSL/TLS)



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

SSL/TLS (simplified):



SSL/TLS:

- Server- and client-authentication
- Key exchange for symmetric encryption
- MACs to secure integrity

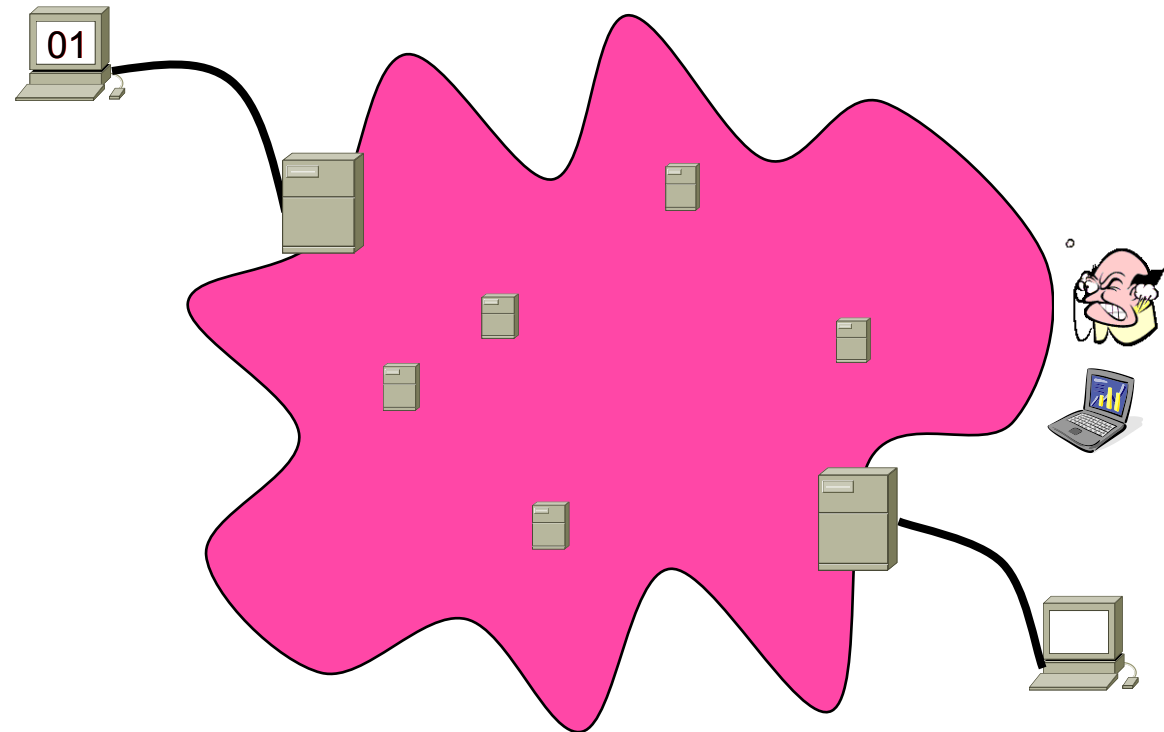
Security Goal	http	https (SSL/TLS)
Authenticity	x	✓ (mostly server only)
Non-Repudiation	x	x
Confidentiality	x	✓
Integrity	x	✓
Date documentation	x	x

- 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).



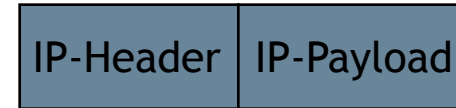
- Introduction
- Infrastructure Security Components
 - Firewalls
 - Demilitarized Zone
 - Intrusion Detection
- Security Protocols
 - Virtual Private Networks
 - Secure Socket Layer
 - IPsec
- Application Layer Security
- Wireless / Mobile Security

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

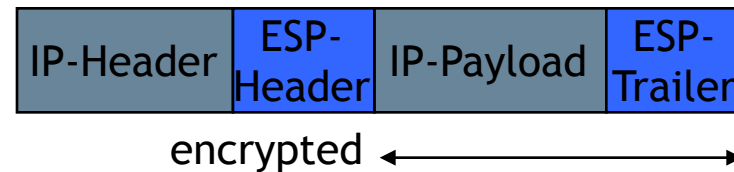


Encapsulating Security Payload (ESP)

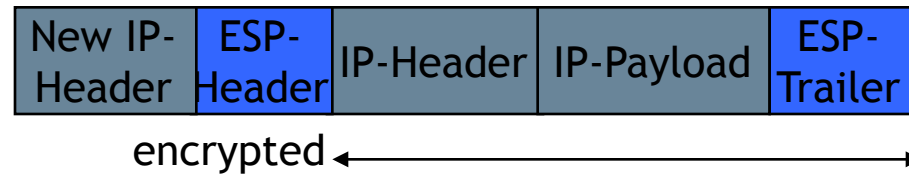
- Data Packet



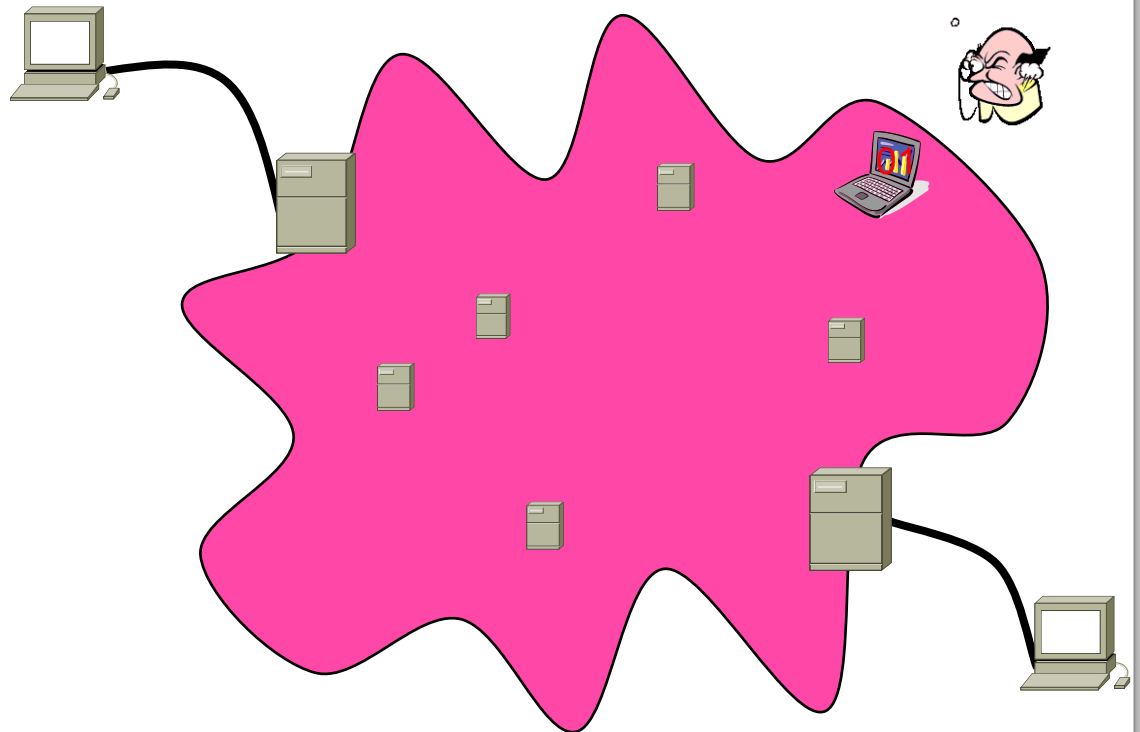
- ESP-Transport-Mode



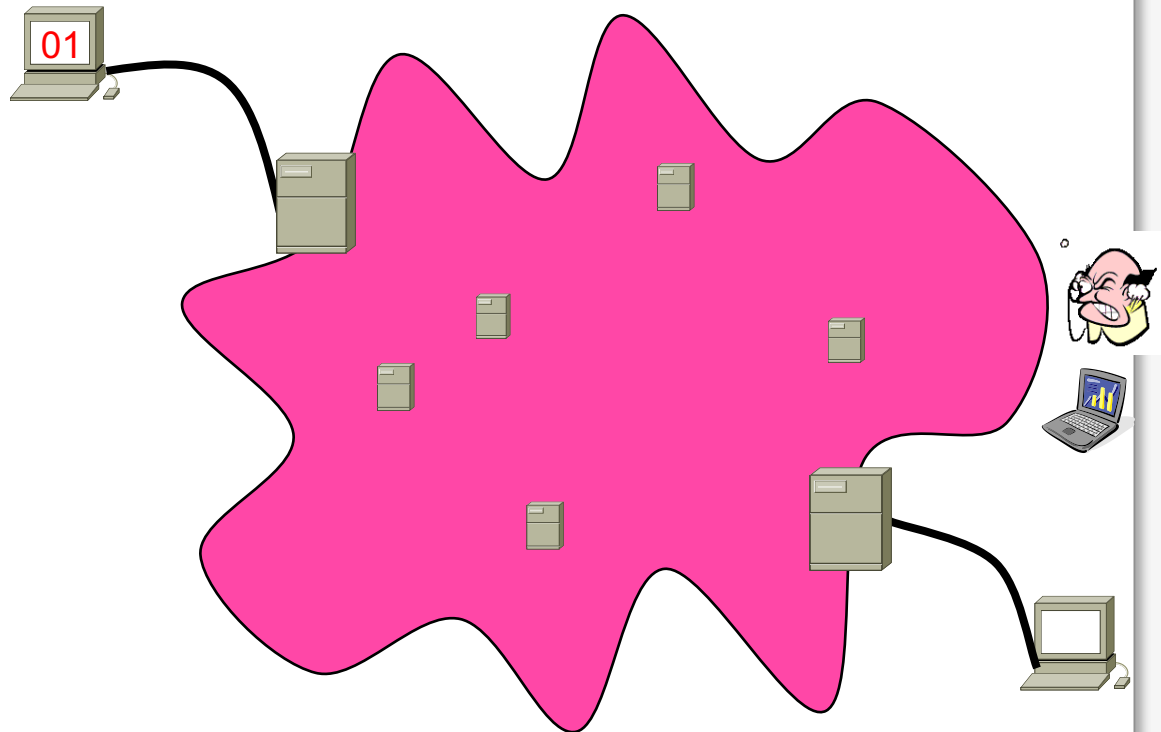
- ESP-Tunnel-Mode



- Attacker sends IP-packets with a faked sender address.

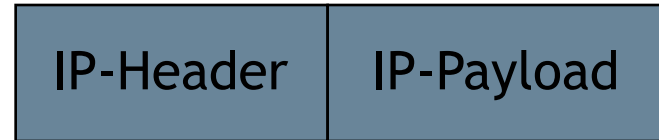


- Attacker impersonates the recipient.

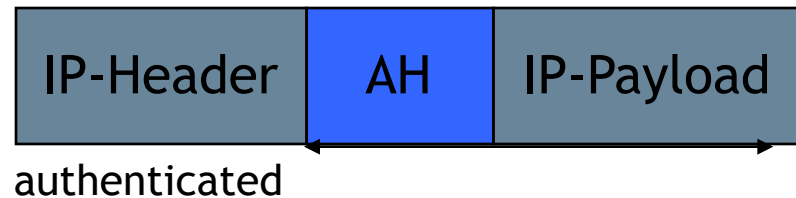


IPsec Authentication Header (AH)

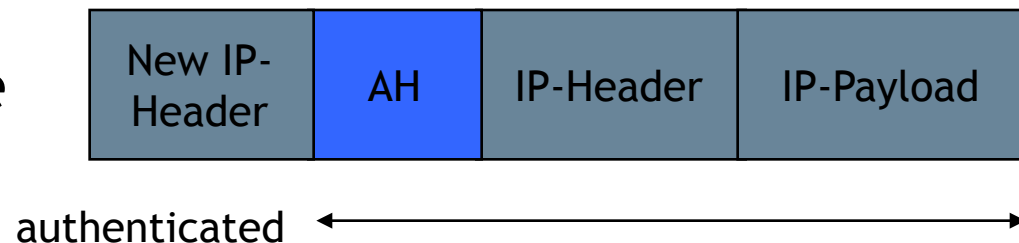
Data Packet



AH-Transport-Mode



AH-Tunneling-Mode



- 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.

User Name:

Password:

Remember me next time.

1=1 always true



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



Commented line, because "-- "

- 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.

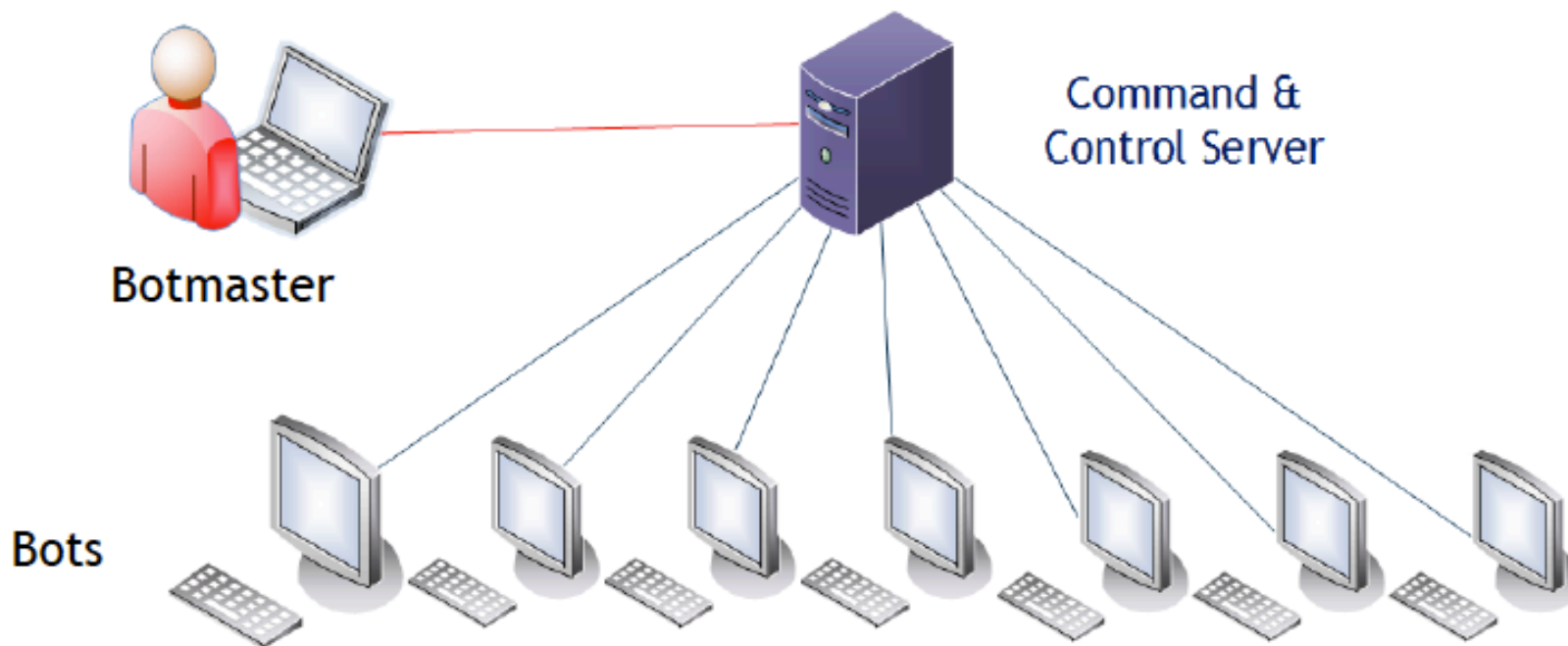
XSS (Cross-site Scripting)

- 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.

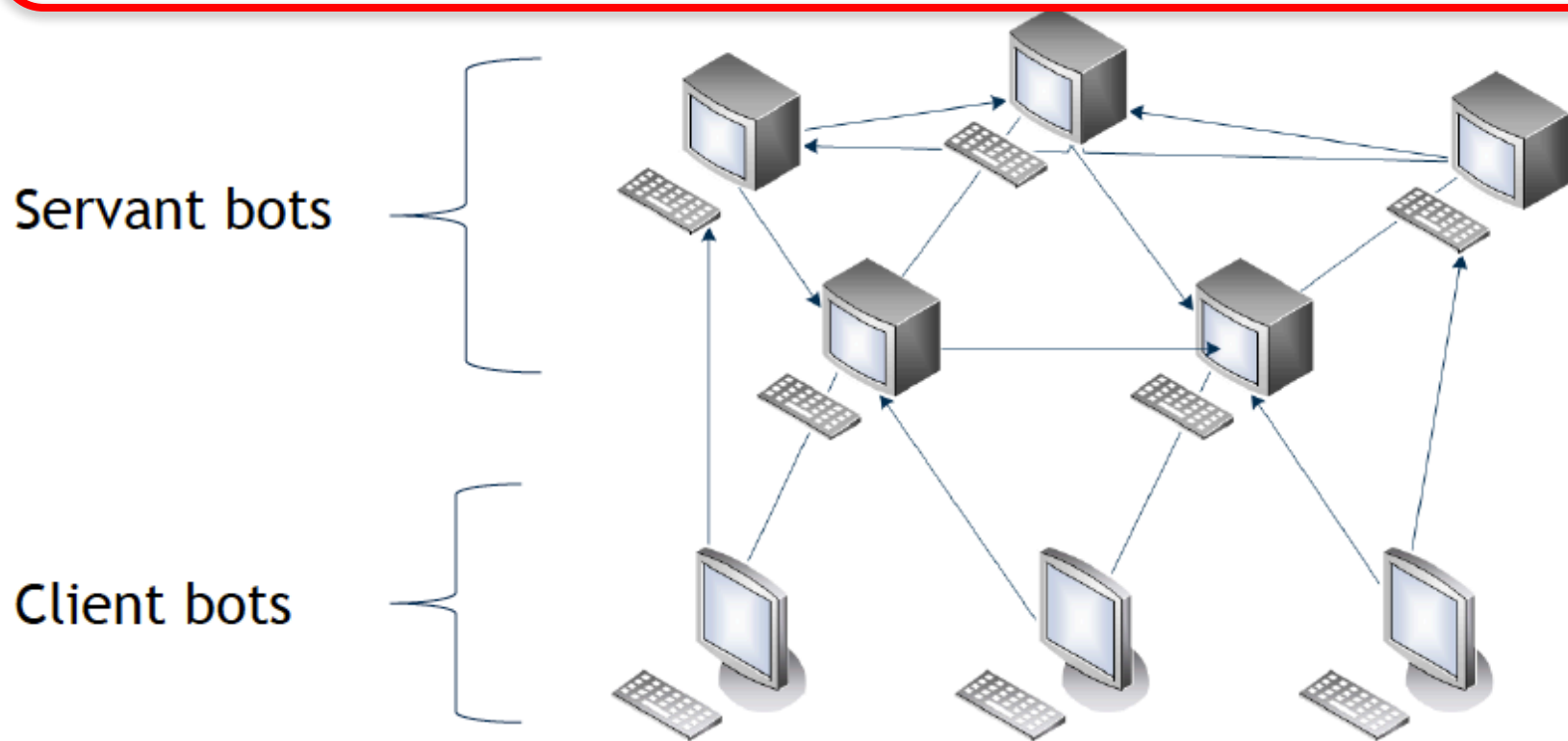
Distributed Denial of Service (DDoS)

- 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.



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

- [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 2017-01-18
- [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>