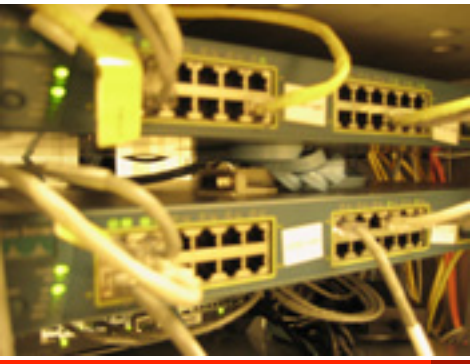


Introduction

Security

Mark Felegyhazi
assistant professor
CrySyS Lab.

BME Department of Telecommunications
(Híradástechnikai Tanszék)
mfelegyhazi(atat)crysys(dot)hu

First look – quick overview

- What is security?
- Prevent or detect/block?
- Security techniques
  - crypto
  - protocols
- Why do we care about economics here?
  - How much is enough to invest in defense?
  - We work together, or not?
- Who is responsible?

- Concepts and definitions
- Attacks
- Cryptography
- Security defense mechanisms
- Security economics

Concepts

Concepts

biztonság

Concepts

biztonság

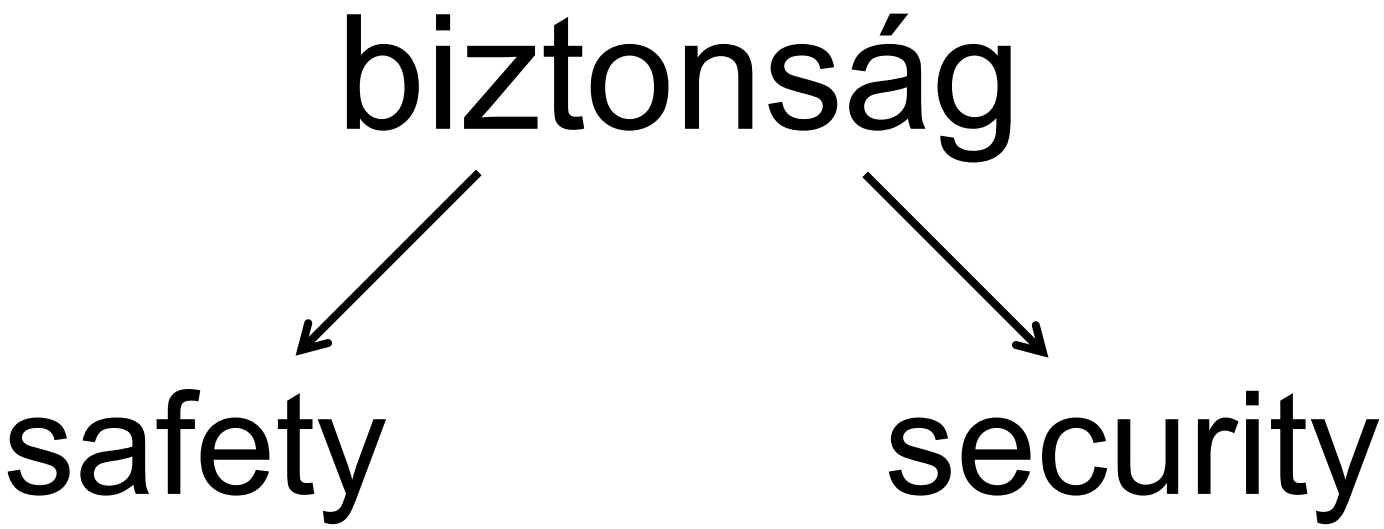
safety

the condition of being protected against the consequences of failure, damage, error, accidents, harm or any other event, which could be considered non-desirable

security

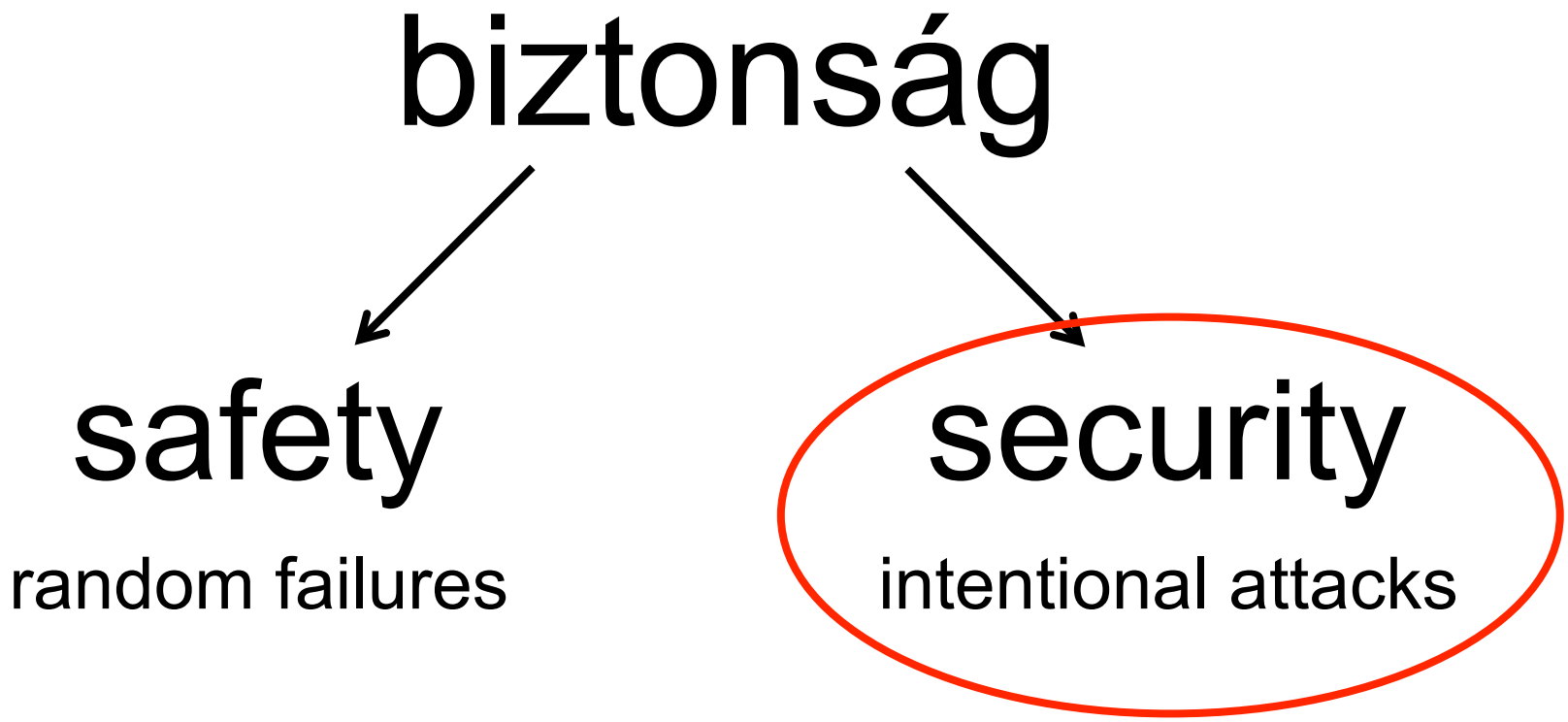
the **process** of delaying, preventing, and otherwise protecting against external or internal defects, dangers, loss, criminals, and other individuals or actions that threaten the steady state of a system

Concepts



achieve an acceptable level of risk

Concepts



Concepts

megbízhatóság

Concepts

megbízható

reliable

able to perform and maintain its functions in routine, as well as in unexpected circumstances

trustworthy

does what people expect it to do – and not something else – despite environmental disruption, human user and operator errors, and attacks by hostile parties

Concepts

megbízható

reliable

random failures

trustworthy

+ intentional attacks

Concepts

adatbiztonság

vs.

adatvédelem

Concepts

adatbiztonság

↓

data **security**

the practice of **protecting** information from unauthorized access, use, disclosure, disruption, modification, or destruction

adatvédelem

↓

data **privacy**

the ability to **control** what information one reveals about oneself, and who can access that information

control can be preserved by protection against disclosure

↓

data security mechanisms can be used to achieve data privacy

but, in general, privacy is a broader (social) concept

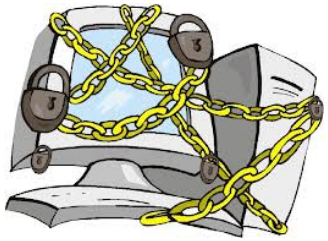
Concepts

information security?

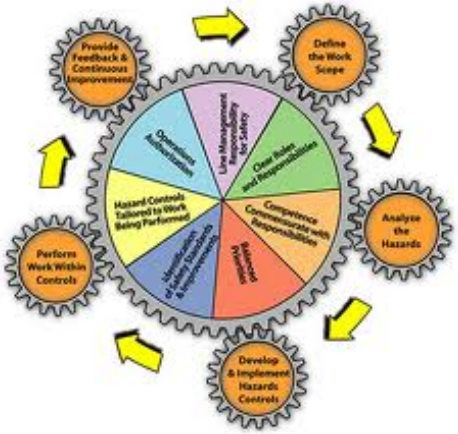


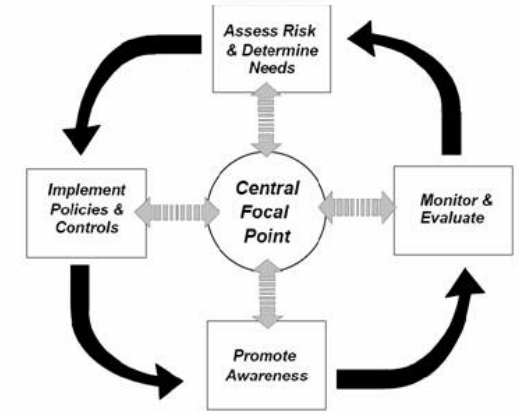

... is about protecting data (transmitted and stored)






... is protecting data processing systems (computers and networks)





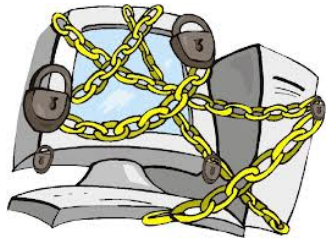
... is a process (aiming at reducing risk)




= cryptography

κρυπτός = "hidden, secret";
γράφειν = "writing"






= computer and network security

user authentication (e.g., passwords)
protection against malware (e.g., virus scanners)
vulnerablity detection and patching
network perimeter defense (e.g., firewalls)
network intrusion detection systems (IDS)
DoS resistance
...

Security

- Merriam-Webster, [4b, (1)]:
  - measures taken to guard against espionage or sabotage, crime, attack, or escape
- Dictionary.com, [1]:
  - freedom from danger, risk, etc.; safety
- Wikipedia.com:
  - **Security** is the degree of protection against danger, damage, loss, and crime.
  - **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
  - **Communications security** is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients.
  - **Computer security** can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Our definition

- **security**: prevention or detection of an attack on the computer system
  - attack: deliberate attempt to compromise the intended use of a computer system

- a few important points
  - attacker: a malicious entity whose aim is to prevent the users of the computing system from achieving their goal (primarily privacy, integrity, and availability of data)
  - **security vs. safety**
- Why economics of computer security?
  - strategic adversary: rational, profit-seeking
  - in general: see “Security Protocols” course from Prof. Levente Buttyan (Hírközlõ rendszerek biztonsága szakirány)

Secure protocols

- in a very general sense, secure protocols are distributed algorithms – involving message passing between participants – that try to reach a certain goal, even in the presence of attackers
- examples:
  - secure communication protocols (for wired and wireless networks)
  - secure key exchange protocols
  - secure routing protocols
  - secure neighbor discovery protocols (in wireless networks)
  - …
- security of a protocol is always evaluated w.r.t. an attacker model
- different types of protocols call for different attacker models

More definitions

- vulnerability
  - attacks usually exploit vulnerabilities
  - a vulnerability is a flaw or weakness in the system's design, implementation, or operation and management
  - most systems have vulnerabilities, but not every vulnerability is exploited
  - whether a vulnerability is likely to be exploited depends on the difficulty of the attack and the perceived benefit of the attacker

- threat
  - a possible way to exploit vulnerabilities
  - a potential attack

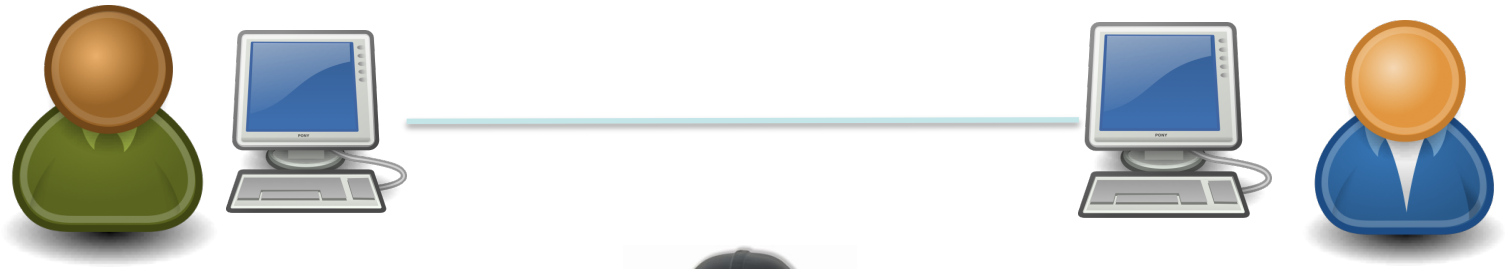
More on attacks

- passive attack
  - requires no intervention into the operation of the system
  - typically consists in the passive acquisition of some information that should not be available to the attacker
  - typical examples:
    - eavesdropping message contents
    - traffic analysis
      - gaining knowledge of data by observing the characteristics of communications that carry the data
      - even if message content is encrypted, an attacker can still
        - » determine the identity and the location of the communicating parties
        - » observe the frequency and length of the messages being exchanged
        - » guess the nature of the communication
  - difficult to detect, should be prevented

More on attacks

- active attack
  - requires an active intervention into the operation of the system
  - typical examples:
    - masquerade (spoofing)
      - an entity pretends to be a different entity
    - replay
      - capture and subsequent retransmission of data
    - modification (substitution, insertion, destruction)
      - (some parts of the) legitimate messages are altered or deleted, or fake messages are generated
      - if done in real time, then it needs a “man in the middle”
    - denial of service
      - normal use or management of the system is prevented or inhibited
      - e.g., a server is flooded by fake requests so that it cannot reply normal requests
  - difficult to prevent, should be detected

Communication security – a simple view



Alice

Malice

Bob

(Bob is not) living next door to Alice

- the motivation, operation, and analysis of security protocols are often presented as tales about two strange characters, Alice and Bob, and their “friends”
- Alice and Bob
  - they live far from each other and communicate only via Internet, e-mail, or telephone
  - they have actually never met, but for some reason, they frequently need to conduct all sorts of business with each other
  - they rarely trust anyone else, sometimes not even each other
  - their history of interactions include exchanging secret e-mails, playing poker over the phone, using electronic coins to buy digital content from each other, remotely signing contracts, running auctions and elections over the Internet, …

Friends

- Carol / Carlos / Charlie is a third participant in communications
- **Eve** is an eavesdropper (a passive attacker)
- Gordon is a government agent
- Isaac is an Internet Service Provider (ISP)
- Justin / Julian is from the justice system
- **Mallory** is a malicious attacker; unlike Eve, Mallory can modify messages, substitute her own messages, replay old messages, and so on (active attacker)
- Oscar is an opponent, usually taken as equivalent to Mallory
- Pat / Peggy is a prover and Victor is a verifier; in their interactions, Peggy always tries to convince Victor that she knows some information without actually revealing that information (zero-knowledge protocols)
- Trent is a trusted arbitrator, some kind of neutral third party, whose exact role varies with the protocol under discussion
- Trudy, is an intruder; another alternative to Mallory
- Zoe, often the last party to be involved in a cryptographic protocol

Communication security services

CIA principles

- confidentiality
  - protection of information from unauthorized disclosure
  - information can be
    - content of communications → (content) confidentiality
    - meta-information (derived from observation of traffic flows) → traffic flow confidentiality
- integrity protection
  - aims to detect message modification and replay
  - provides assurance that data received are exactly as sent by the sender
    - in case of a stream of messages (connection oriented model), integrity means that messages are received as sent, with no duplication, modification, insertion, deletion, reordering, or replays
- availability
  - the service is reachable for the users

Communication security services

- authentication
  - aims to detect masquerade (spoofing)
  - provides assurance that a communicating entity is the one that it claims to be
    - peer entity authentication
    - data/message origin authentication
- non-repudiation
  - provides protection against denial by one entity involved in a communication of having participated in all or part of the communication
    - non-repudiation of message origin
    - non-repudiation of message delivery

Placement of security services

- some services can more naturally be implemented at the application layer (e.g., non-repudiation)
- some services better fit in the link layer (e.g., traffic flow confidentiality)
- but many services can be provided at any layer (e.g., authentication, confidentiality, integrity)
  - lower layer (e.g., link-by-link encryption):
    - services are generic, can be used by many applications
    - protection mechanisms are transparent to the user
  - higher layer (e.g., end-to-end authentication):
    - services are more application specific
    - more user awareness

Attacks

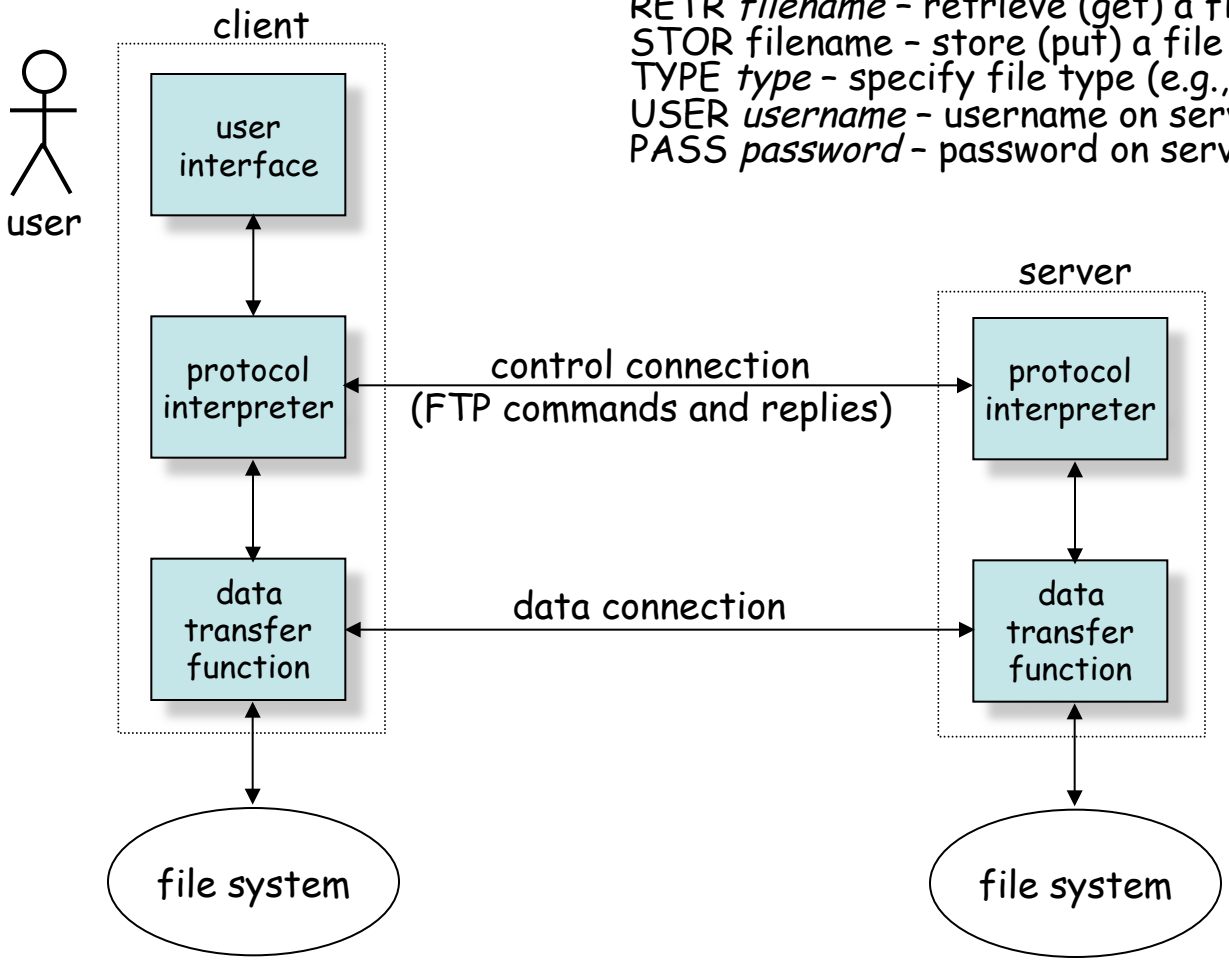
Examples of attacks

- password sniffing in FTP
- password sniffing in TELNET
- mail forging with SMTP
- ARP spoofing
- DoS against a web server
- spam

FTP – File Transfer Protocol

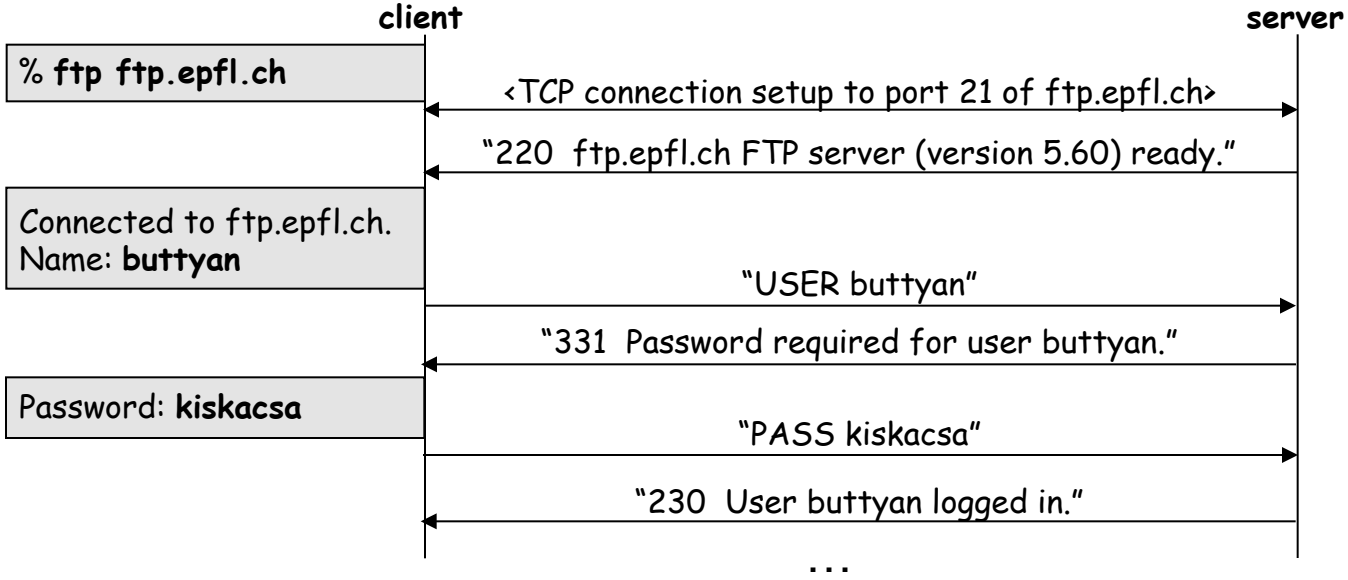
typical FTP commands:

RETR *filename* – retrieve (get) a file from the server
STOR filename – store (put) a file on the server
TYPE *type* – specify file type (e.g., A for ASCII)
USER *username* – username on server
PASS *password* – password on server



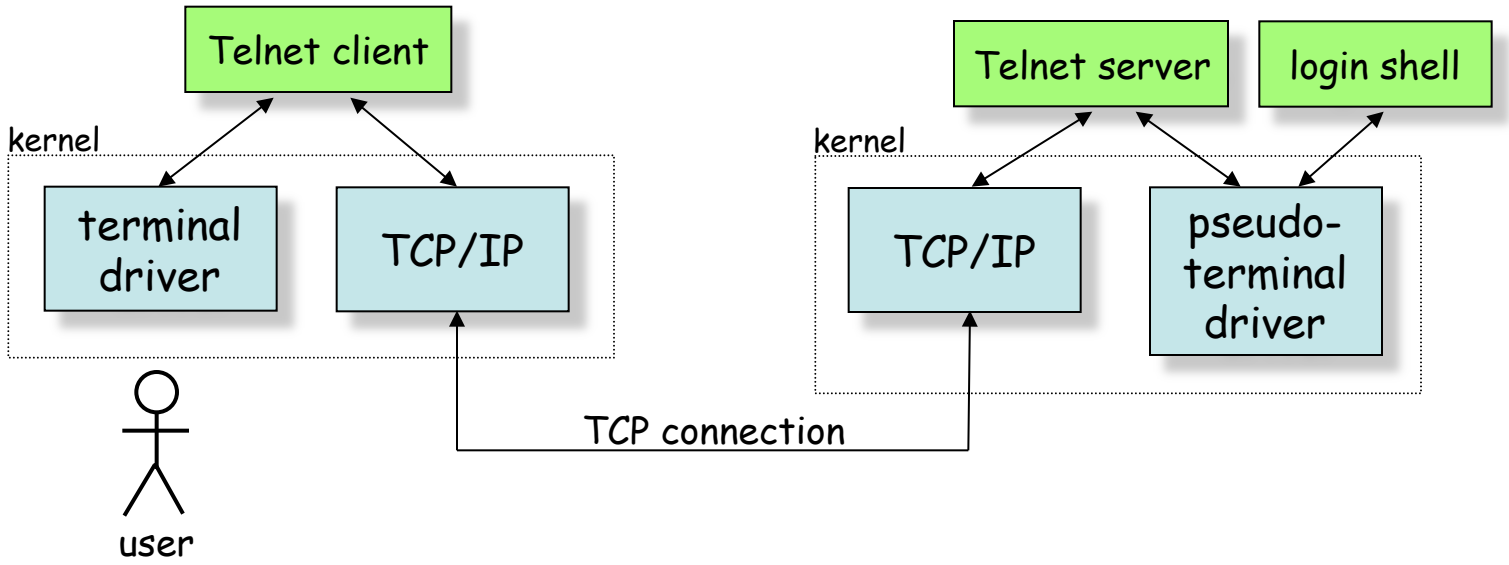
FTP security problems

- neither the control nor the data connection is protected
  - passwords can be eavesdropped
    - FTP is a text(ASCII) based protocol, which makes password sniffing even easier
  - files transmitted over the data connection can be intercepted and modified



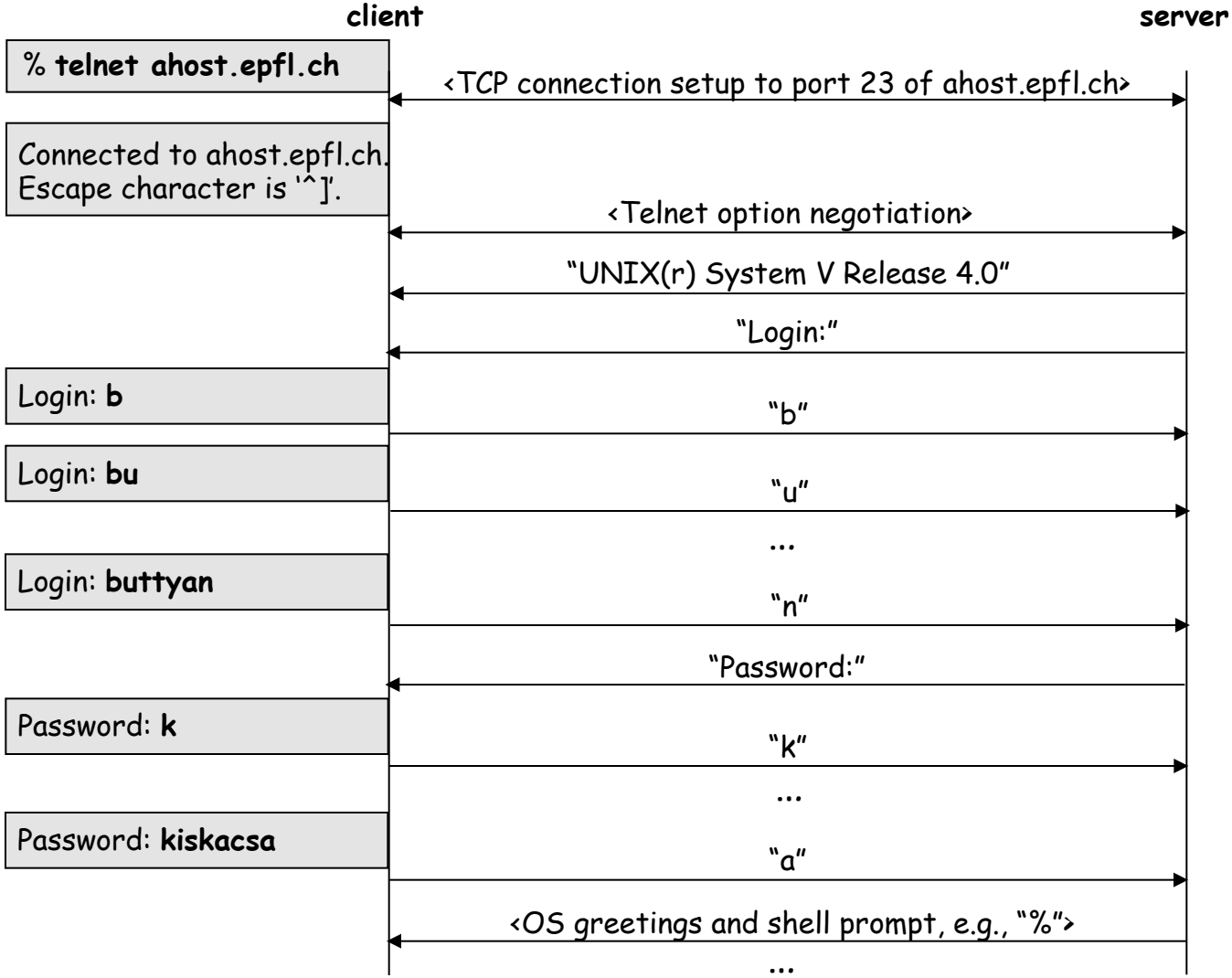
Telnet

- provides *remote login* service to users
- text (ASCII) based protocol

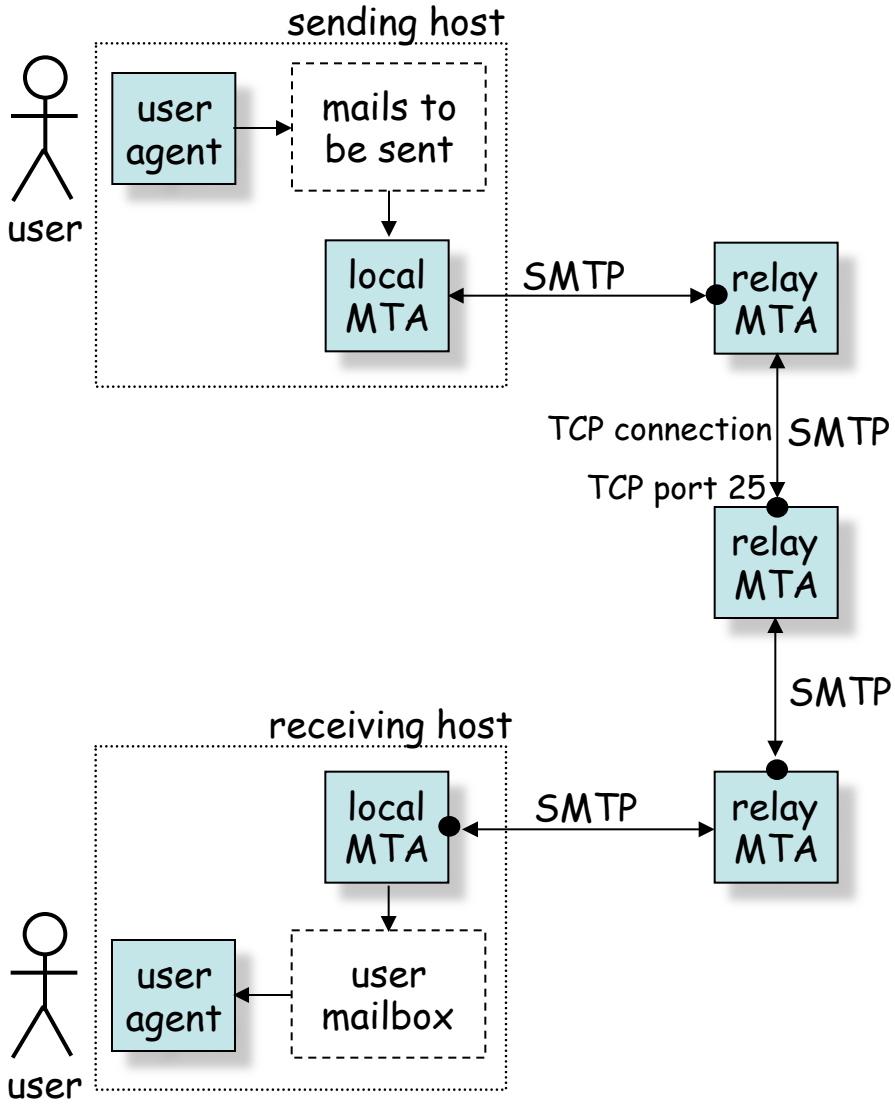


Telnet security problems

- passwords are sent in clear

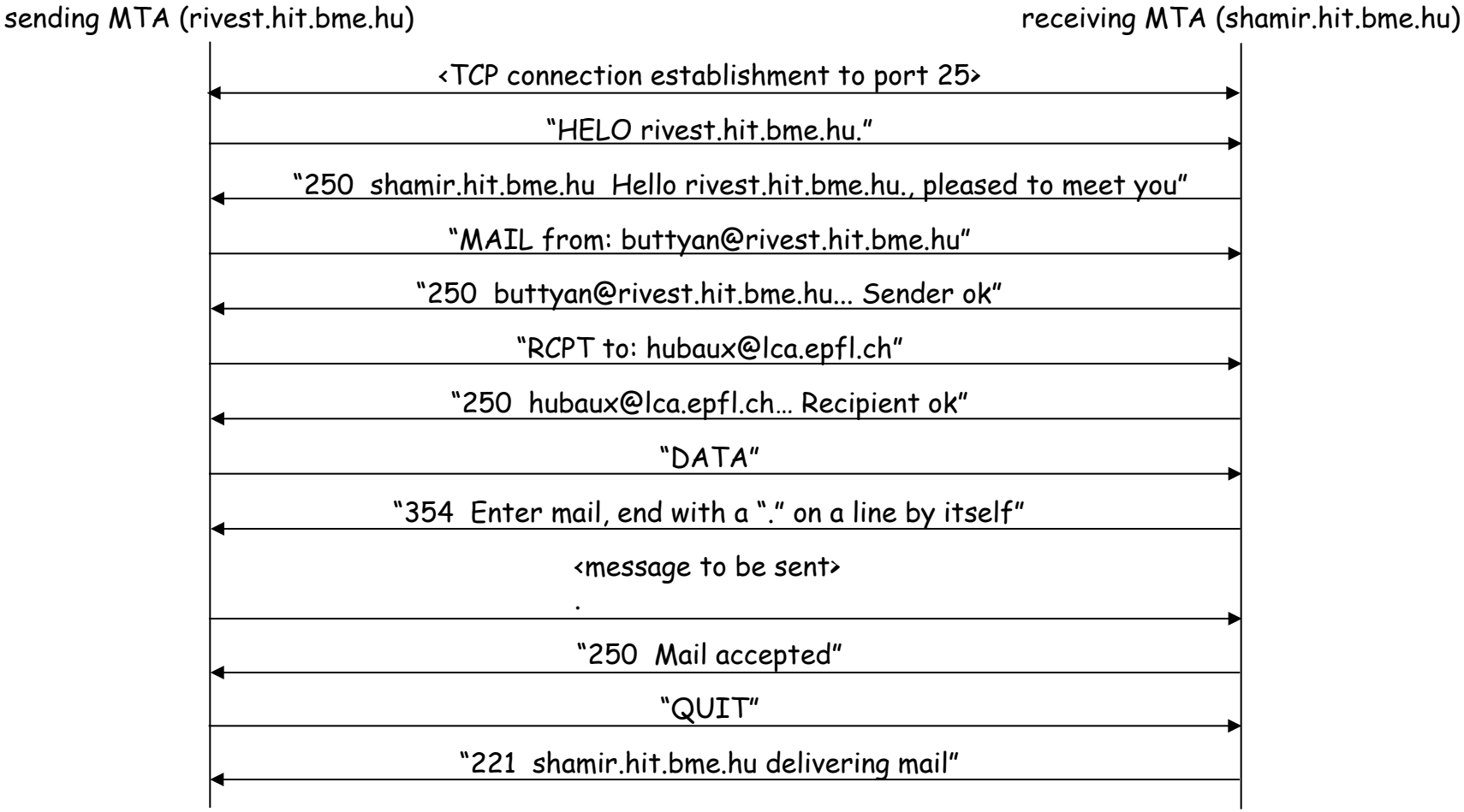


SMTP – Simple Mail Transfer Protocol



SMTP cont'd

- SMTP is used by MTAs to talk to each other
- SMTP is a text (ASCII) based protocol



SMTP security problems

- SMTP does not provide any protection of e-mail messages
  - messages can be read and modified by any of the MTAs involved
  - fake messages can easily be generated (e-mail forgery)
- Example:

```
% telnet frogstar.hit.bme.hu 25
Trying...
Connected to frogstar.hit.bme.hu.
Escape character is '^['.
220 frogstar.hit.bme.hu ESMTP Sendmail 8.11.6/8.11.6;
Mon, 10 Feb 2003 14:23:21 +0100
helo abcd.bme.hu
250 frogstar.hit.bme.hu Hello [152.66.249.32], pleased to meet you
mail from: bill.gates@microsoft.com
250 2.1.0 bill.gates@microsoft.com... Sender ok
rcpt to: buttyan@ebizlab.hit.bme.hu
250 2.1.5 buttyan@ebizlab.hit.bme.hu... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Your fake message goes here.
.
250 2.0.0 h1ADO5e21330 Message accepted for delivery
quit
221 frogstar.hit.bme.hu closing connection
Connection closed by foreign host.
%
```

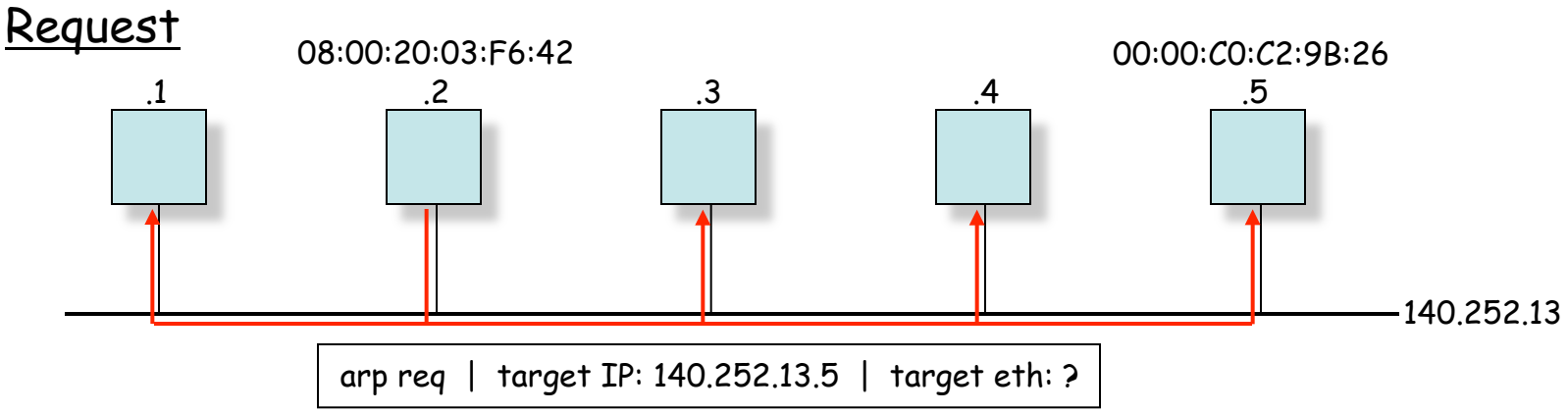
Be careful, though!

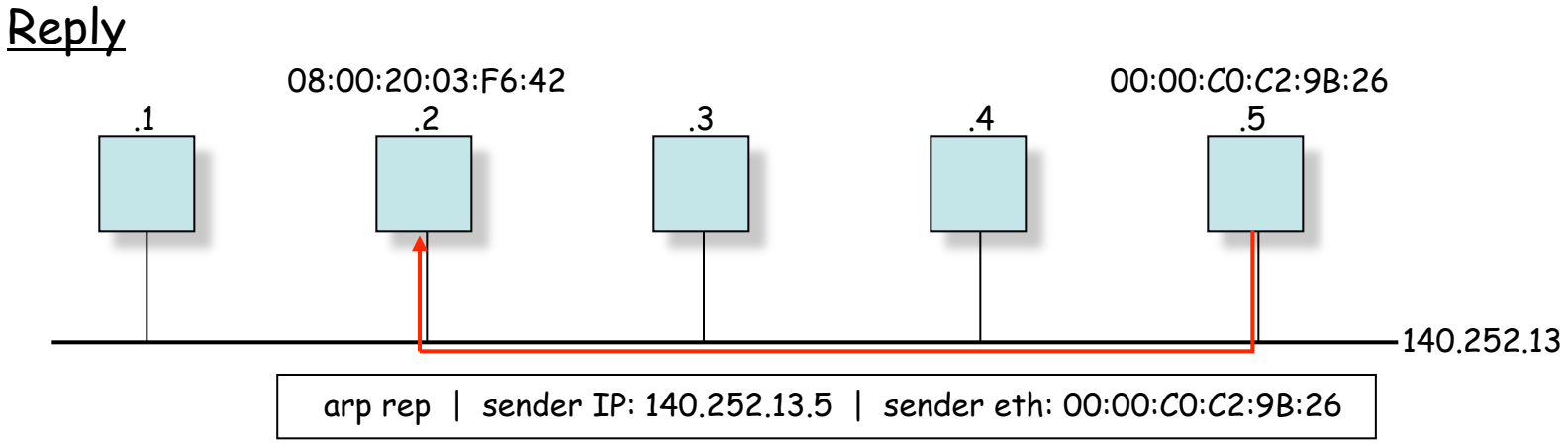
```
Return-Path: <bill.gates@microsoft.com>
Received: from frogstar.hit.bme.hu (root@frogstar.hit.bme.hu [152.66.248.44])
          by shamir.ebizlab.hit.bme.hu (8.12.7/8.12.7/Debian-2)
          with ESMTP id h1ADSsxG022719
          for <buttyan@ebizlab.hit.bme.hu>; Mon, 10 Feb 2003 14:28:54 +0100
Received: from abcd.bme.hu ([152.66.249.32])
          by frogstar.hit.bme.hu (8.11.6/8.11.6) with SMTP id h1ADO5e21330
          for buttyan@ebizlab.hit.bme.hu; Mon, 10 Feb 2003 14:25:41 +0100
Date: Mon, 10 Feb 2003 14:25:41 +0100
From: bill.gates@microsoft.com
Message-Id: <200302101325.h1ADO5e21330@frogstar.hit.bme.hu>
To: undisclosed-recipients:;
X-Virus-Scanned: by amavis-dc
Status:

Your fake message goes here.
```

ARP

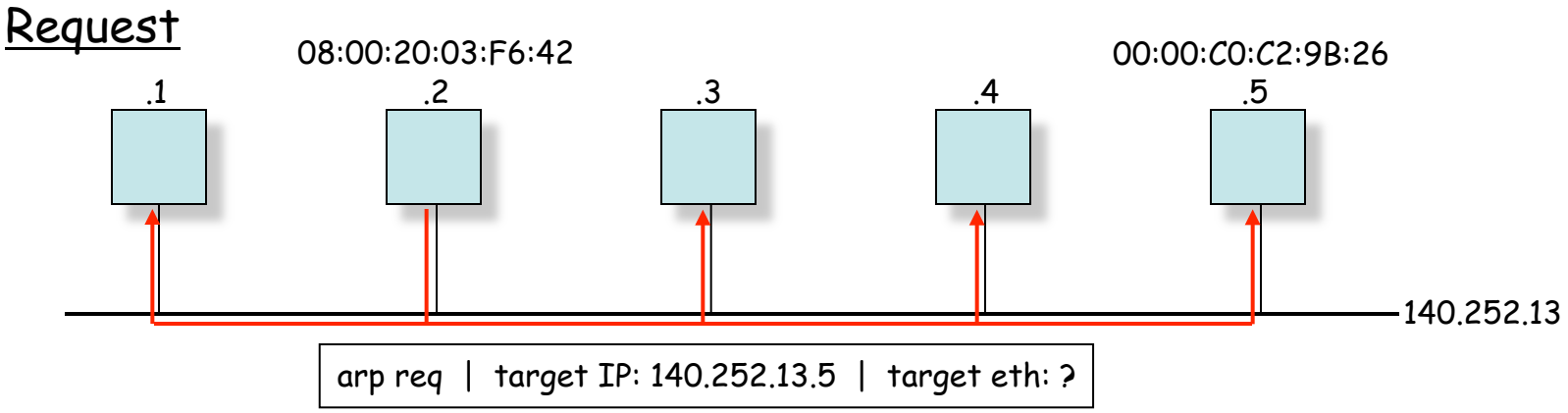
- mapping from IP addresses to MAC addresses

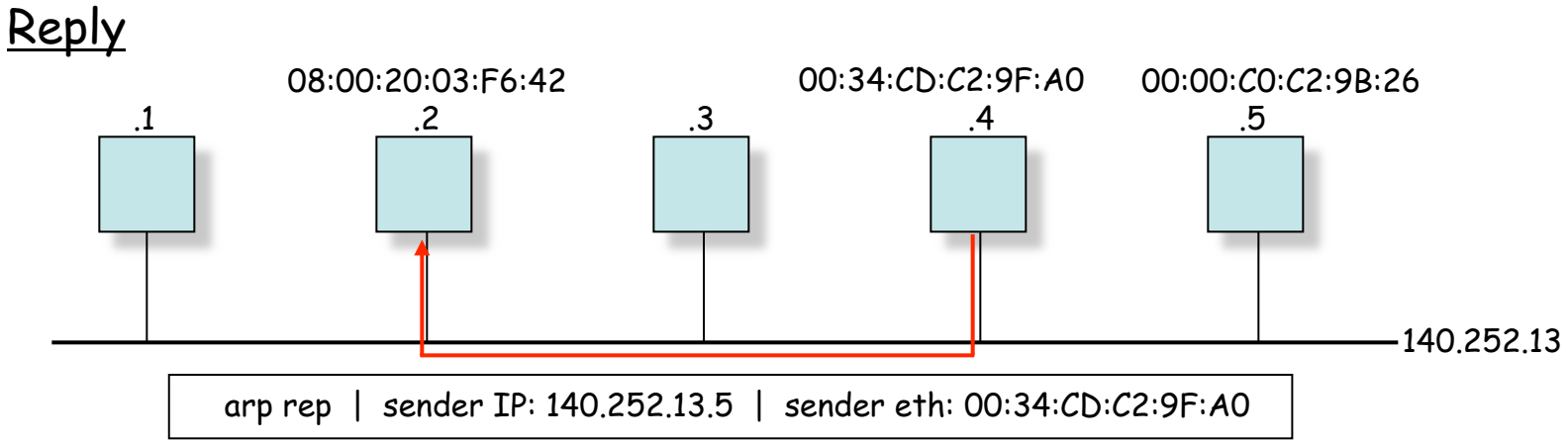




ARP spoofing

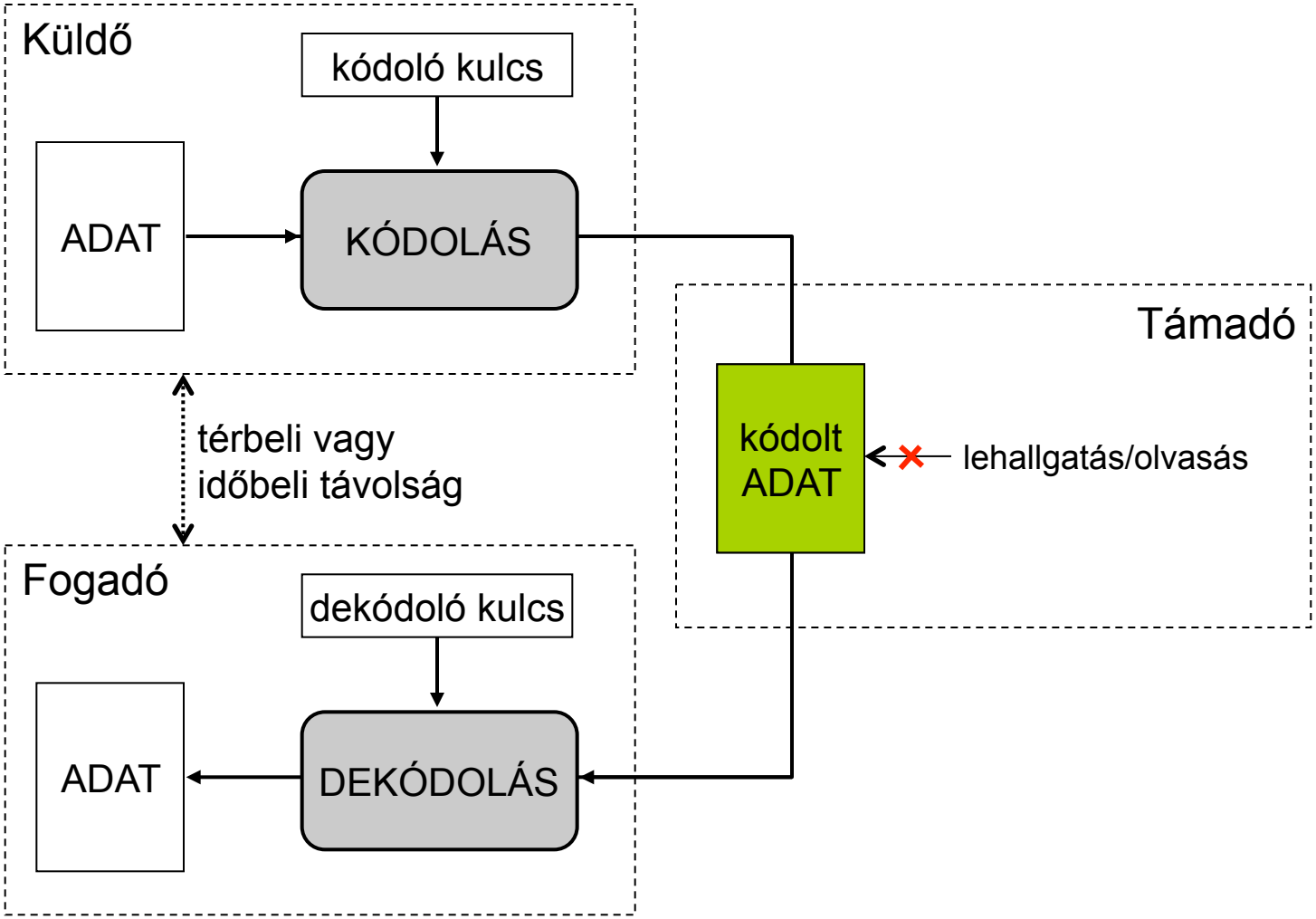
- an ARP request can be responded by another host





Crypto

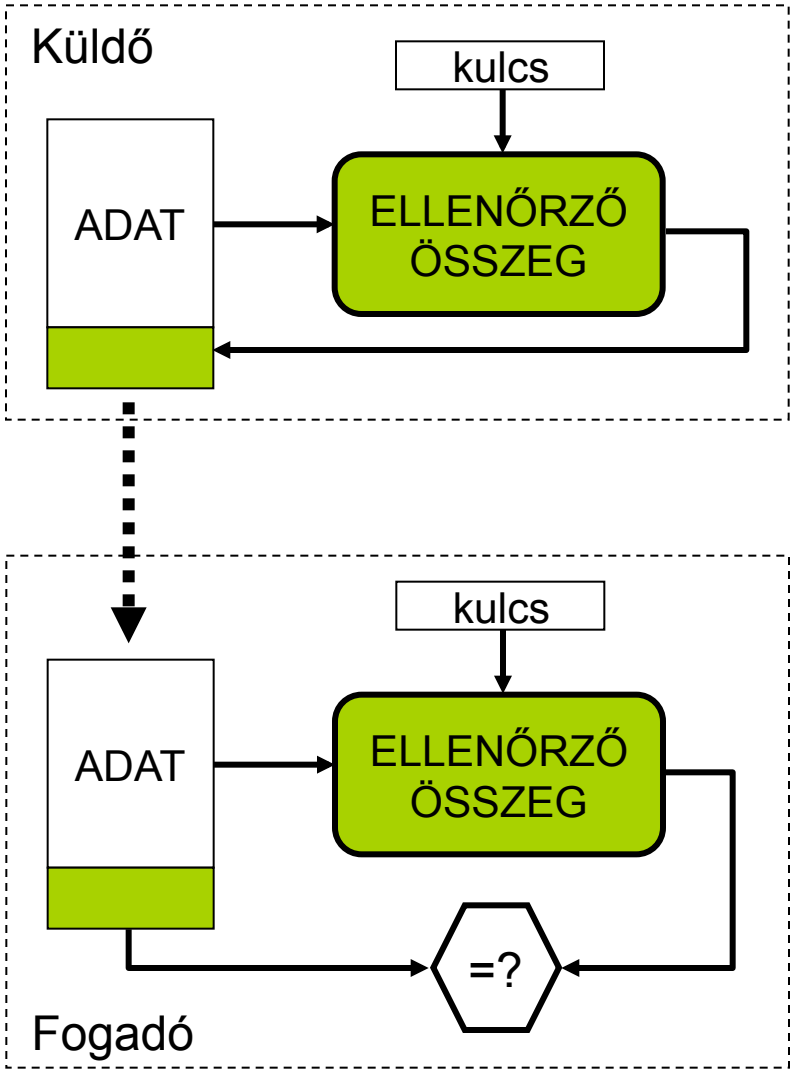
Encryption model



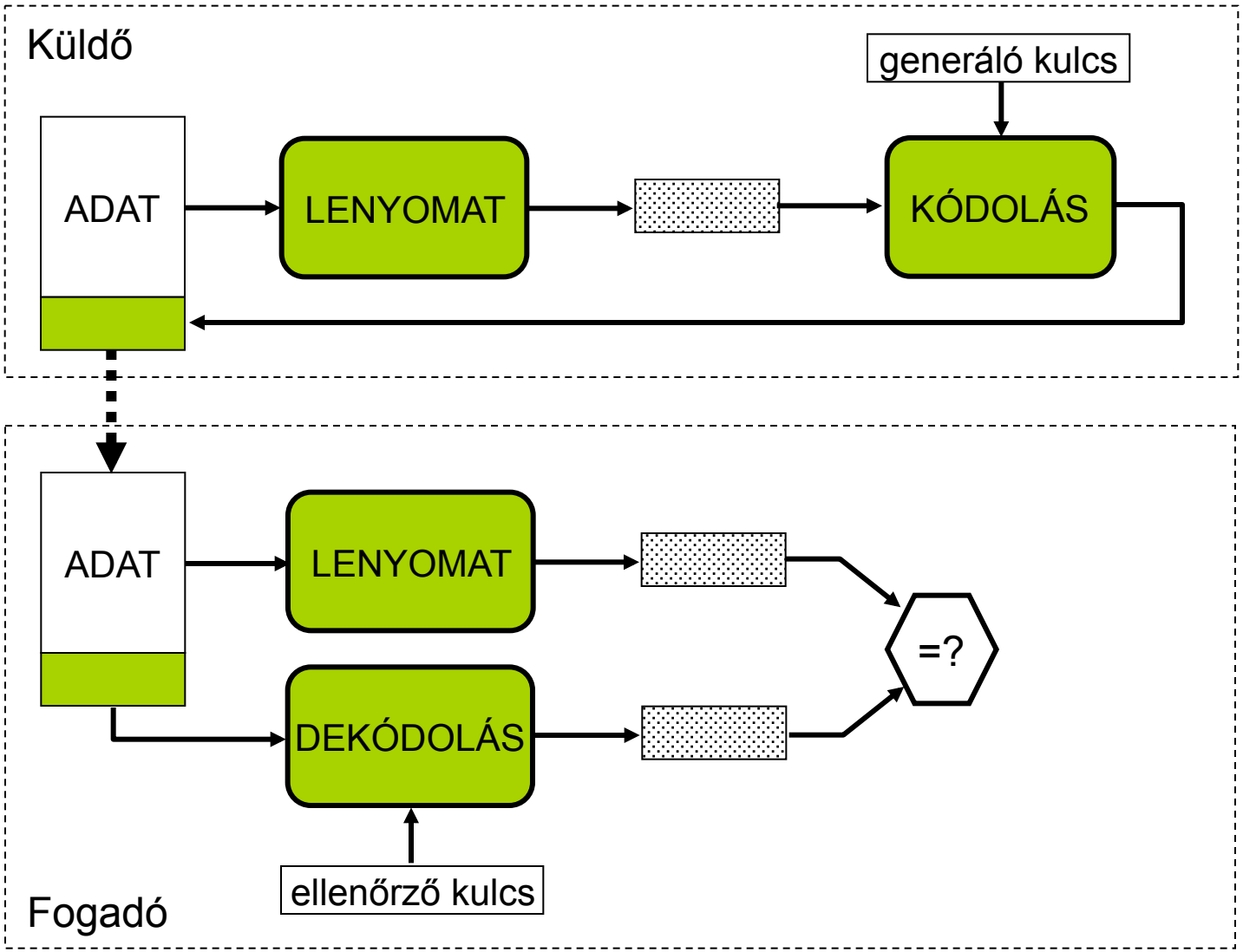
Algorithms for symmetric and asymmetric crypto

- symmetric key
  - DES
  - 3DES
  - AES
  - RC4
- asymmentric (public) key
  - RSA (factorization)
  - elliptic curve
- key agreement
  - Diffie-Hellman
  - PKI and CAs

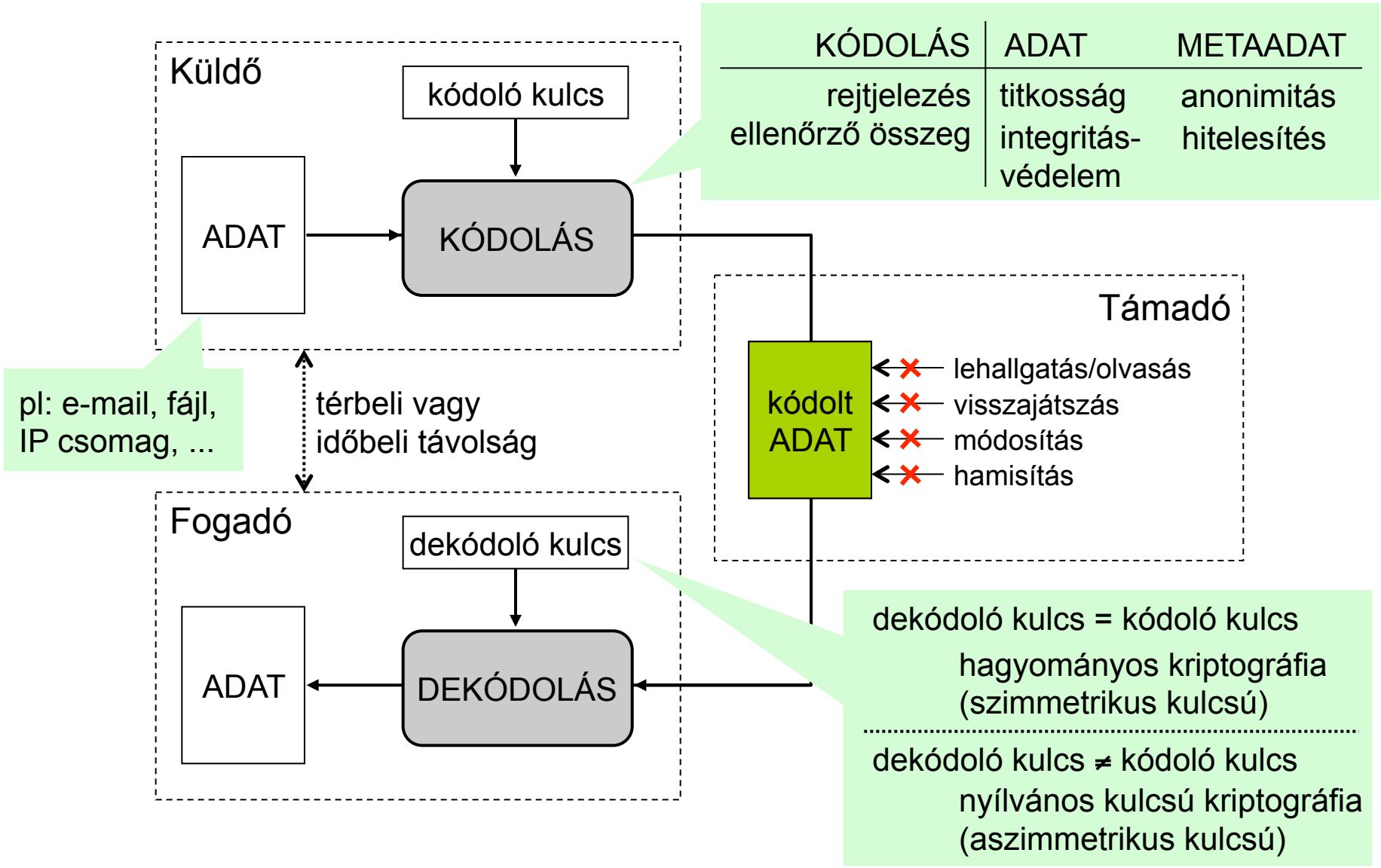
Authentication and integrity protection



Digital signature



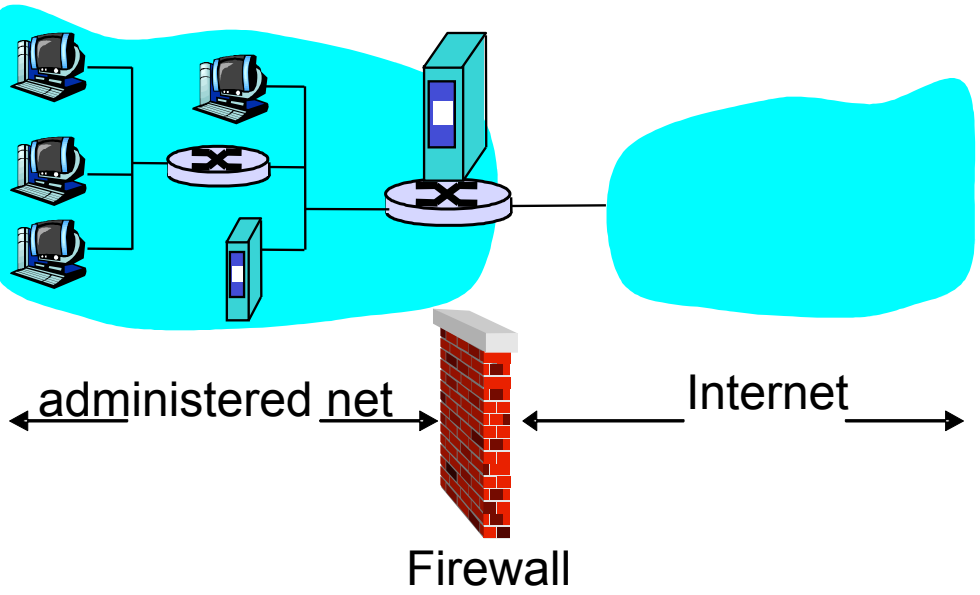
Crypto summary



Network defenses

Firewalls

- separates the internal network from the Internet
- some packets can pass, other are dropped



Firewalls: Why?

Denial-of-Service attack defense:

- SYN-Flooding: attacker initiated several useless TCP connections, not enough resources for legit connections

illegal access or manipulation if internal data:

- website defacement

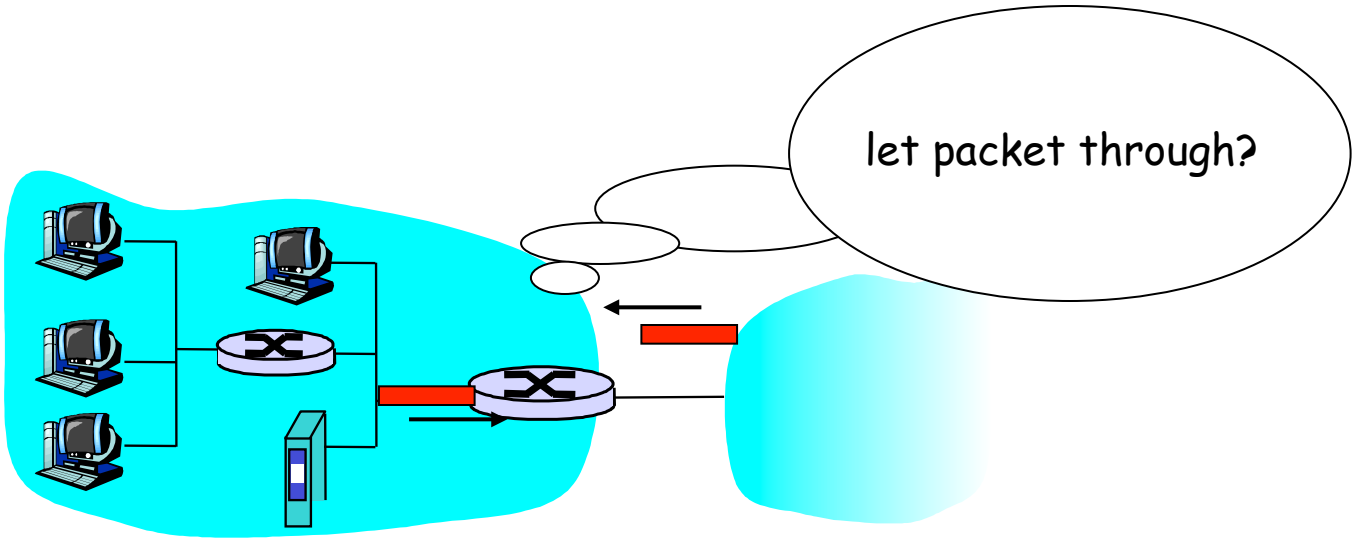
unauthorized access to the internal network

- passing through access control, privilege escalation

3 firewall types (depending on the filtering layer)

- stateless packet filter (L3)
- stateful packet filter (L4)
- application gateway (L7)

Stateless packet filter



- Router-Firewall separates the internal network and the public Internet
- the router processes each packet, and decides to let it through based on:
  - source and dest IP
  - TCP/UDP source and dest port
  - ICMP data type
  - TCP-SYN- and ACK-Bits

Stateless packet filter - examples

goal	Firewall rule
no web access to the outside	drop all incoming packets to all IP addresses to port 80
no incoming TCP connections unless they go to the own webserver	drop all incoming TCP-SYN packets, except if they go to the IP address 130.207.244.203, Port 80.
aviod that a web radio consumes all bandwidth	drop all UDP packets, except for DNS and Router-Broadcasts.
protect network from Smurf-DoS attacks	drop all incoming ICMP broadcast packets (ex. 130.207.255.255)
block net discovery by traceroute	drop outgoing ICMP-TTL-Expired packets

Access Control Lists

- *ACL:* list of rules aplied to all packets on an interface
- in or out
- criterium - action

action	source IP	dest IP	protocoll	source port	dest port	Flags
allow	222.22/16	nicht in 222.22/16	TCP	> 1023	80	egal
allow	nicht in 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	nicht in 222.22/16	UDP	> 1023	53	---
allow	nicht in 222.22/16	222.22/16	UDP	53	> 1023	----
drop	alle	alle	alle	alle	alle	alle

Stateful packet filter

- stateless packet filters often let useless traffic pass:
  - ex. packets with port 80, ACK flag set, but no TCP connection exists

action	source IP	dest IP	protocoll	source port	dest port	Flags
allow	not in 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* follow TCP connections
  - read SYN and FIN packets
  - timeout for inactive connections on the firewall

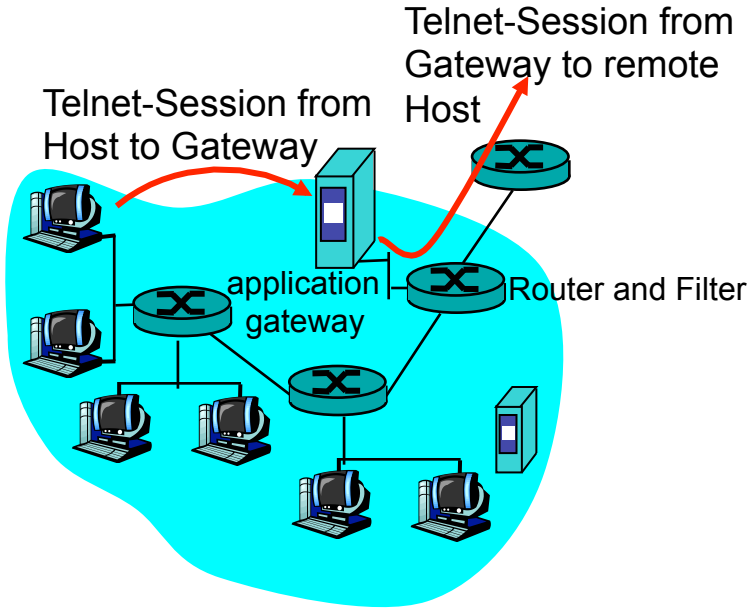
Stateful packet filter

- ACL is extended to check the connection status

action	source address	dest address	proto	source port	dest port	flag bit	check conn
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Application gateway

- filtering packets based on application info and TCP/ UDP/IP fields
- example: only some users can Telnet to the outside



1. require each Telnet connection to pass the gateway
2. establish a Telnet session for authorized users with the remote host; Gateway used as a proxy to relay data
3. router firewall blocks all Telnet connection not originating from the gateway

Limits of firewalls and gateways

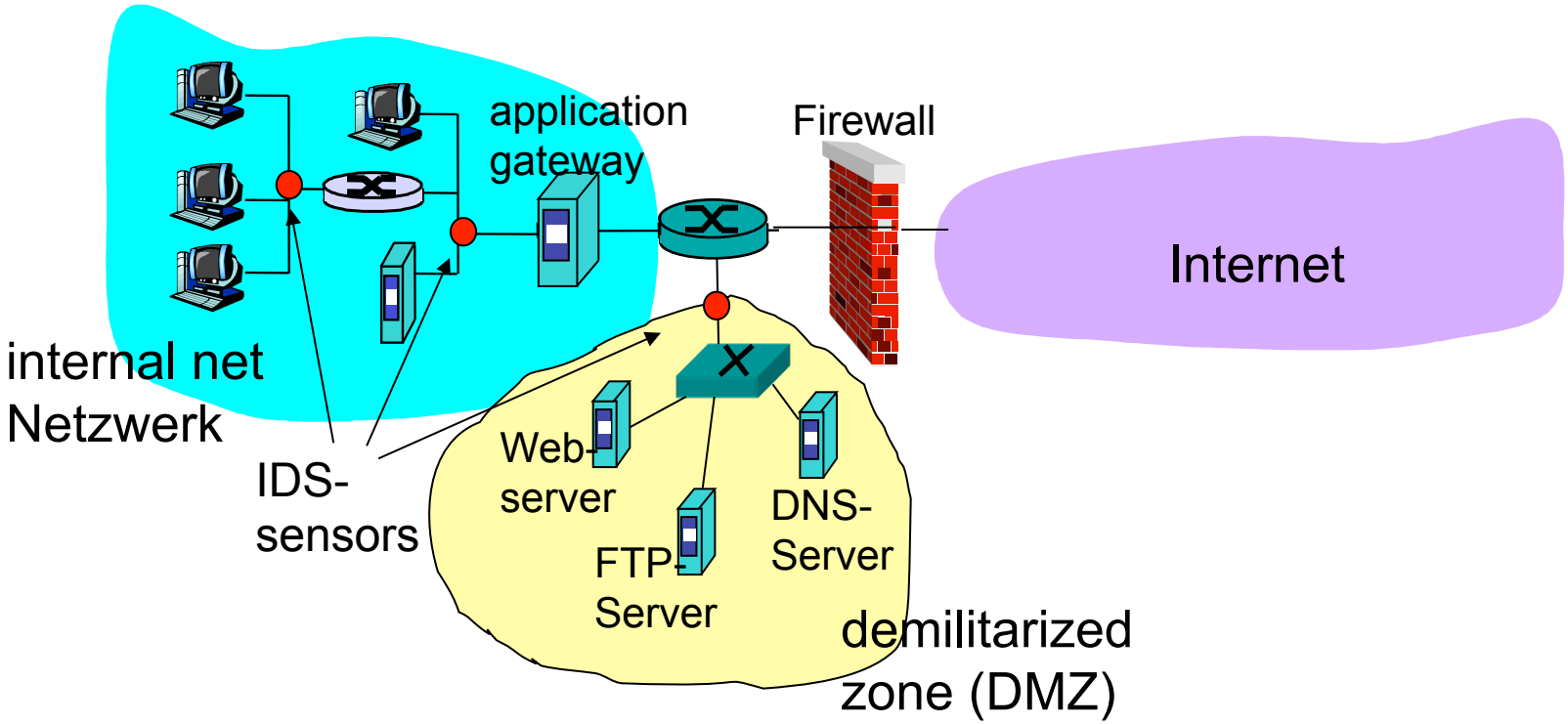
- IP-Spoofing: a router cannot know if the data comes from the source IP
- we need an application gateway for each special application
- Client software has to know which gateway to access:
  - need to set an address of the web proxy
- "all or nothing" rules for UDP
- communication possibilities vs. security level
- even well protected networks are targeted by attacks

Intrusion detection systems (IDS)

- packet filters:
  - applied only on TCP/IP headers
  - data from different sessions cannot be correlated
- Intrusion detection systems (IDS)
  - *Deep Packet Inspection:* analyze the content of packets (ex. for patterns signalling a well-known attack)
  - correlation of multiple packets
    - Port-Scanning
    - network mapping
    - DoS attacks

Intrusion detection systems

- multiple IDS: various tests at different locations



Security concepts summary

- basic concepts
  - security, attack, vulnerability, threat
  - passive vs. active attacks
  - eavesdropping, traffic analysis, masquerade (spoofing), modification, replay, denial of service
  - main communication security services: confidentiality, integrity, availability, authentication, non-repudiation
- some real world attacks
  - ARP spoofing, e-mail forgery, eavesdropping Telnet and FTP passwords, DDoS attacks
- network defenses