Introduction

Security Protocols (bmevihim132)

Dr. Levente Buttyán

associate professor

BME Hálózati Rendszerek és Szolgáltatások Tanszék

Lab of Cryptography and System Security (CrySyS)

buttyan@hit.bme.hu, buttyan@crysys.hu

Outline

- some basic concepts and terminology
- examples for attacks on protocols
- main communication security services

Protocol

- Merriam-Webster:
  - *3b* **:** a set of conventions governing the treatment and especially the formatting of data in an electronic communications system <network *protocols*>

- Wikipedia:
  - A communications protocol is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications.

Security

- Merriam-Webster:

  4b (1) **:** measures taken to guard against espionage or sabotage, crime, attack, or escape

- Wikipedia:
  - Security is the degree of protection against danger, damage, loss, and criminal activity… The key difference between security and reliability is that security must take into account the actions of people attempting to cause destruction.
  - **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
  - The term **computer system security** means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

My definitions

- protocol
  - a distributed algorithm that involves message passing between participants aiming at accomplishing a certain goal cooperatively

- security
  - prevention or – if that is not possible – detection of attacks
  - an attack is a deliberate attempt to compromise a system
  - system compromise means
    - incorrect status of some system resources (e.g., lost password, inappropriately set file access rights, …)
    - incorrect behavior of some system components (e.g., malfunctioning devices, programs, services, ...)
    - decreased overall system dependability (e.g., the system works but the quality of service provided is not acceptable)

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 that we will discuss in details or touch upon in this course:
  - 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 definitions

- 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 definitions

- 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

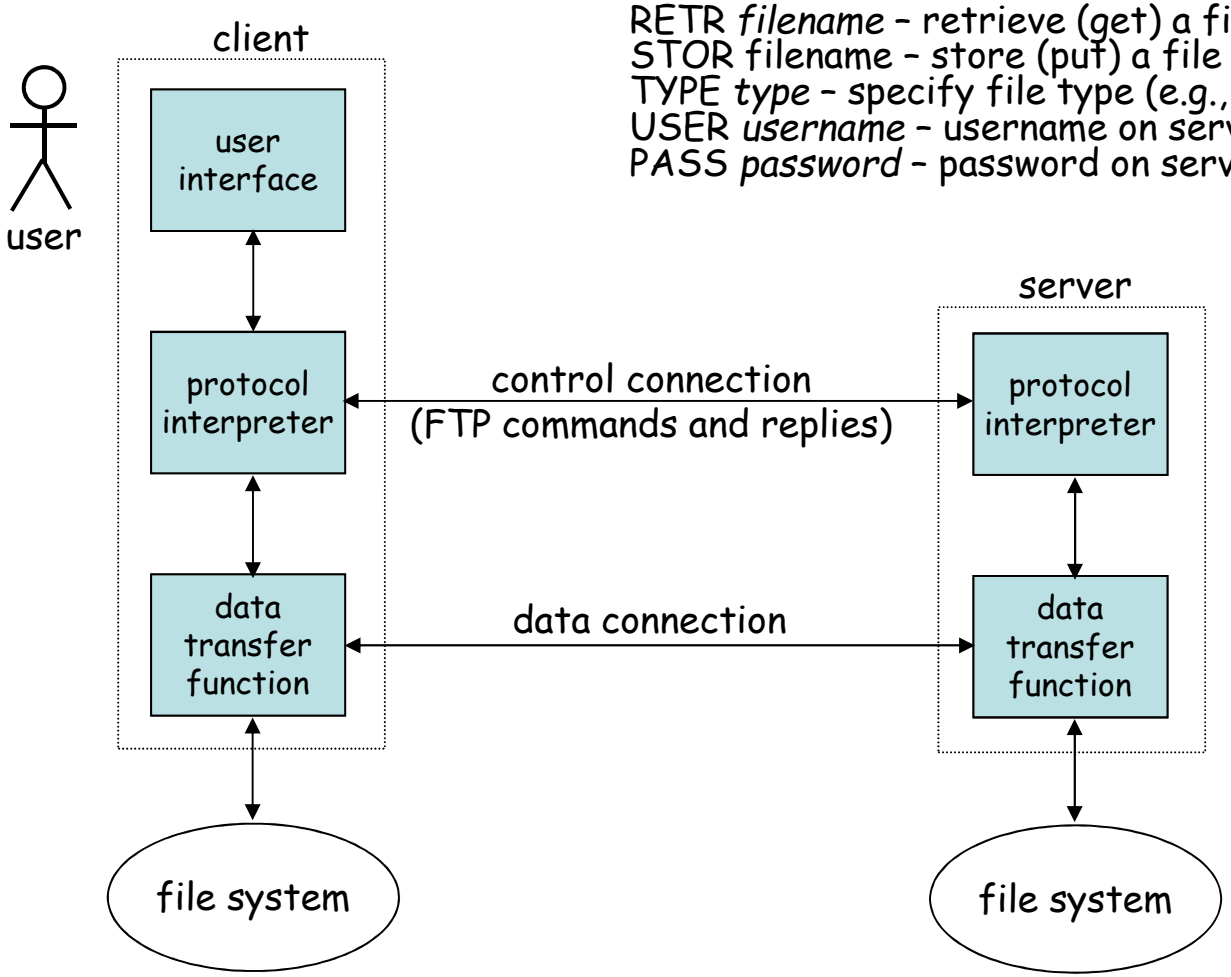
Examples for attacks

- password sniffing in FTP
- password sniffing in TELNET
- mail forging with SMTP
- ARP spoofing

FTP – File Transfer Protocol

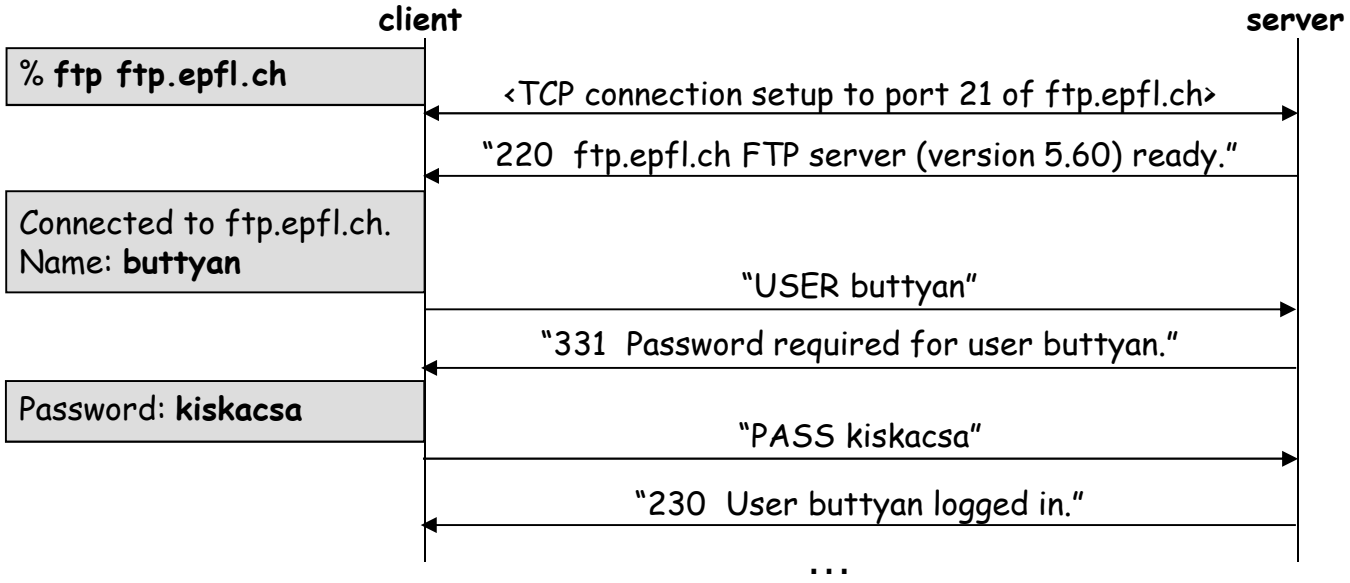
typical FTP commands:

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



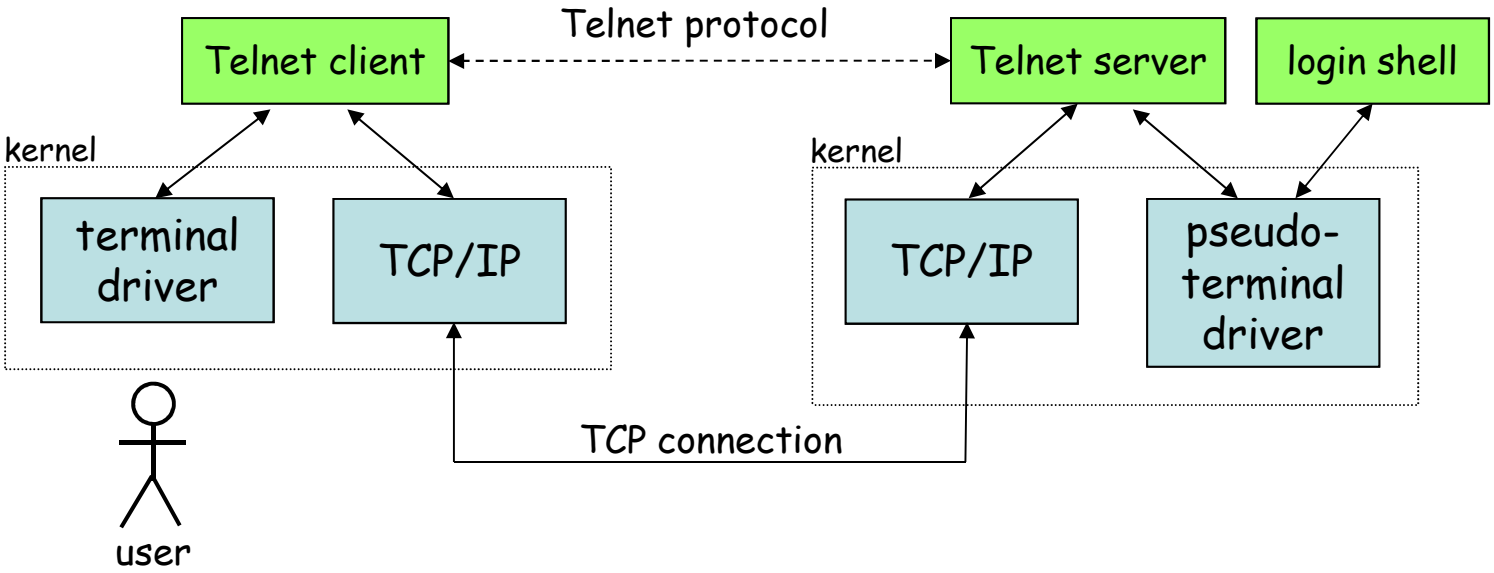
FTP security problems

- 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



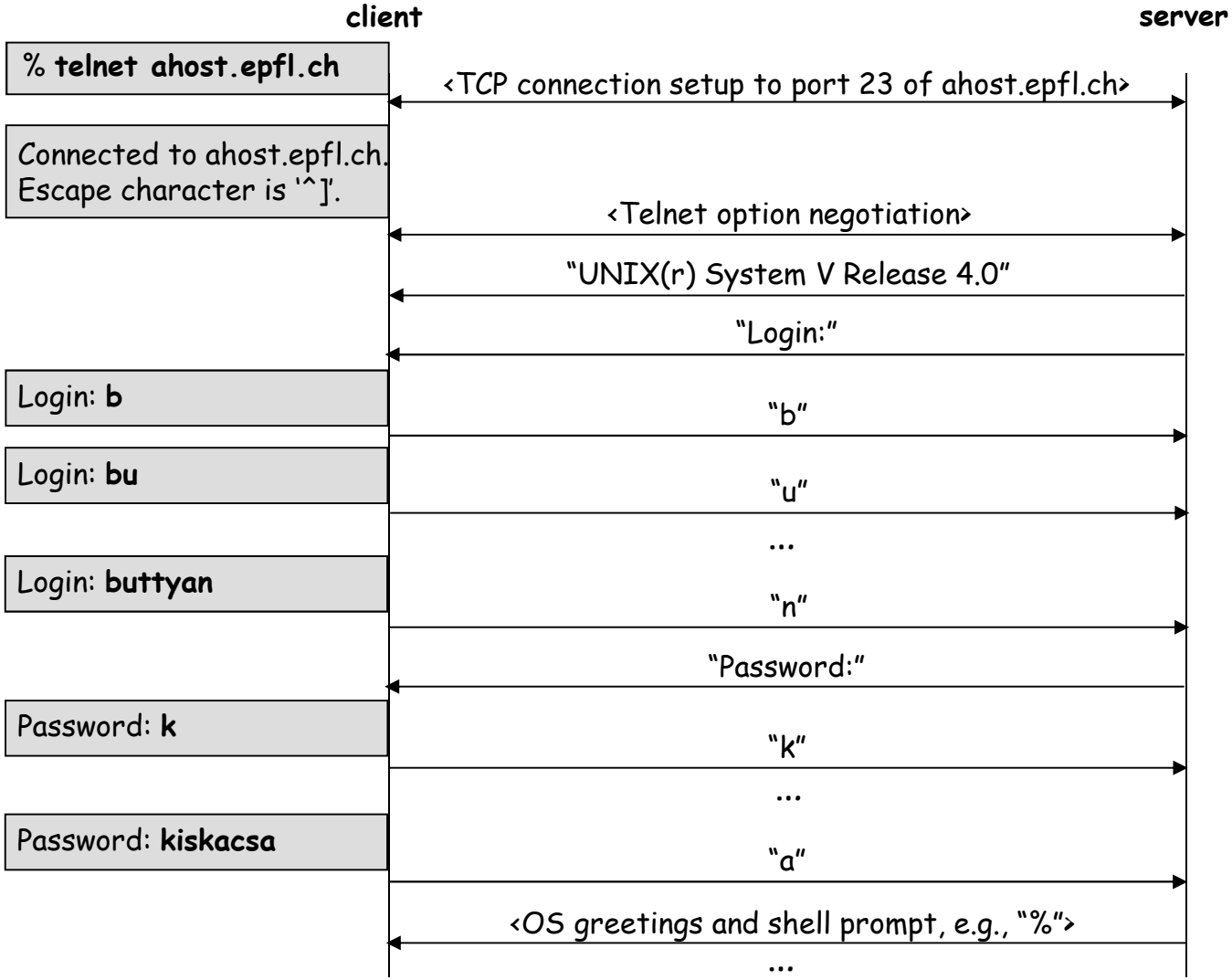
Telnet

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

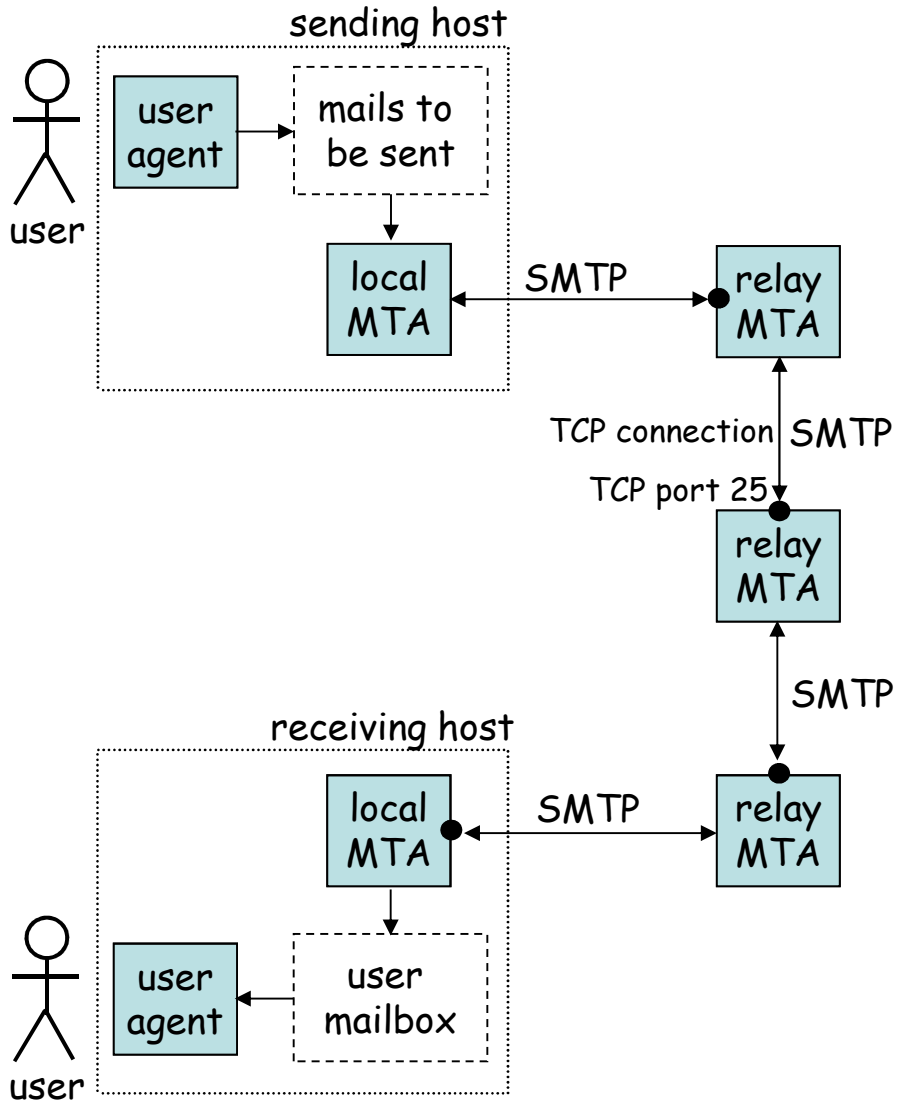


Telnet security problems

- passwords are sent in clear

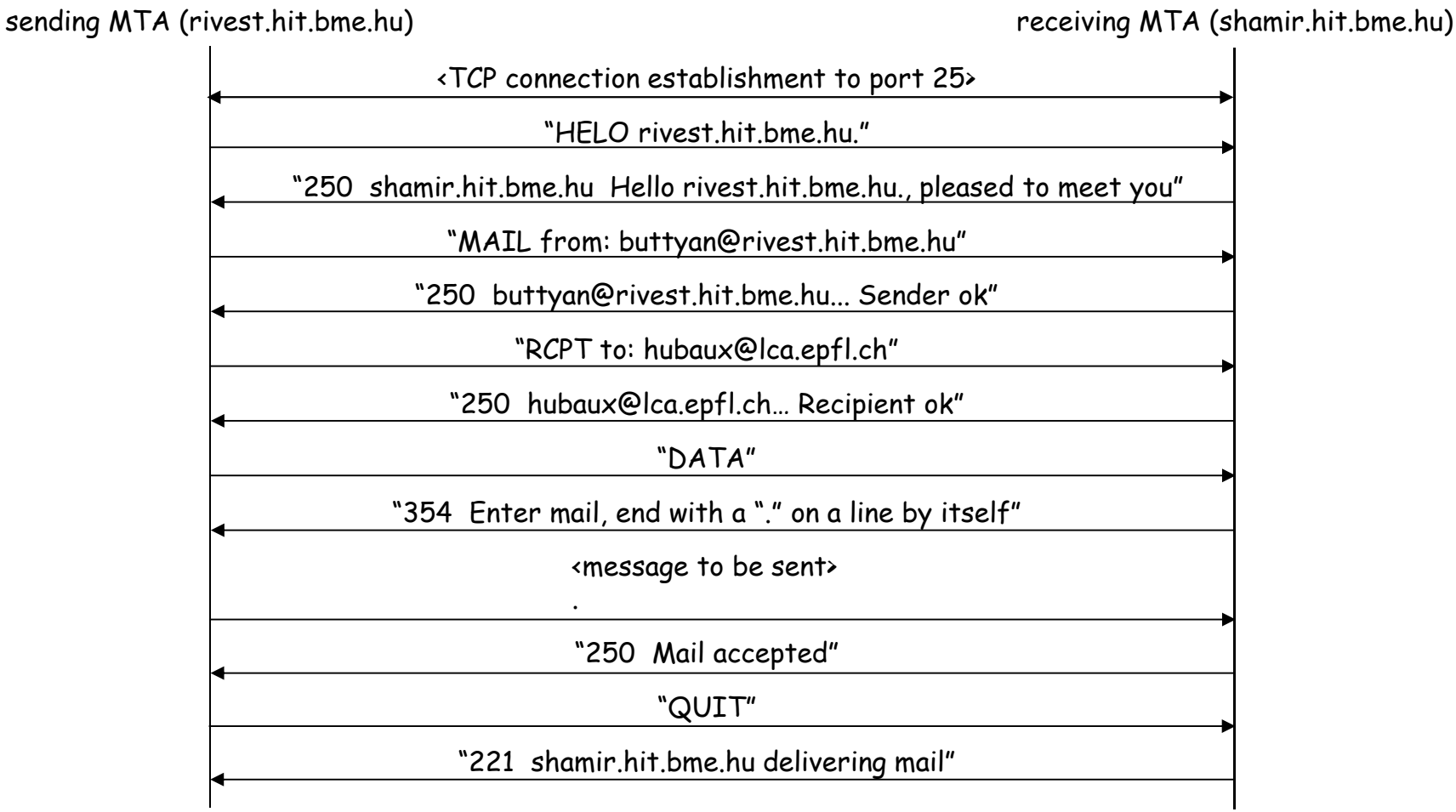


SMTP – Simple Mail Transfer Protocol



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.
%
```

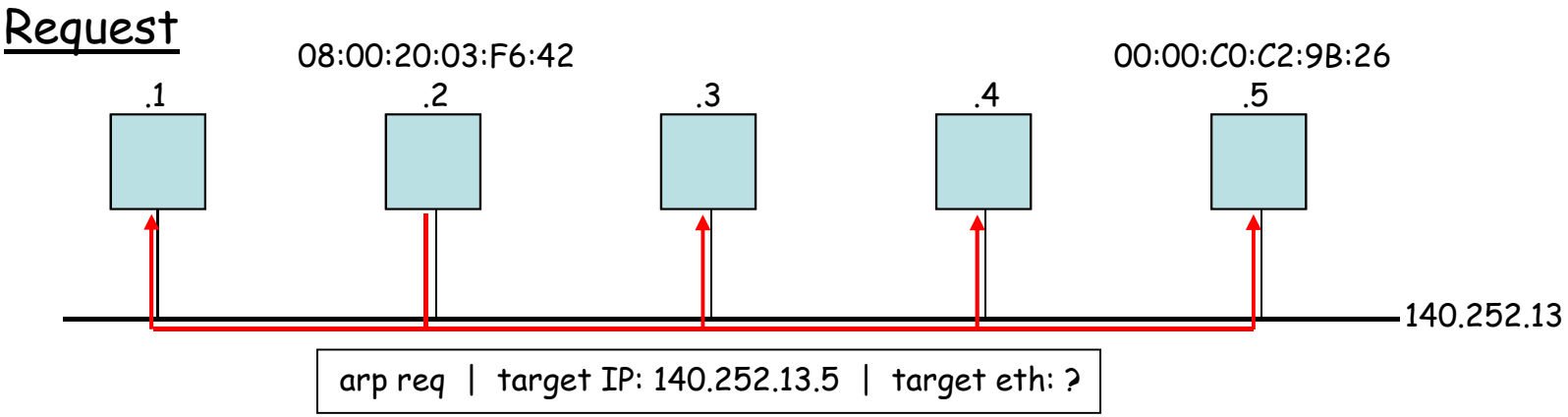
Be careful, though!

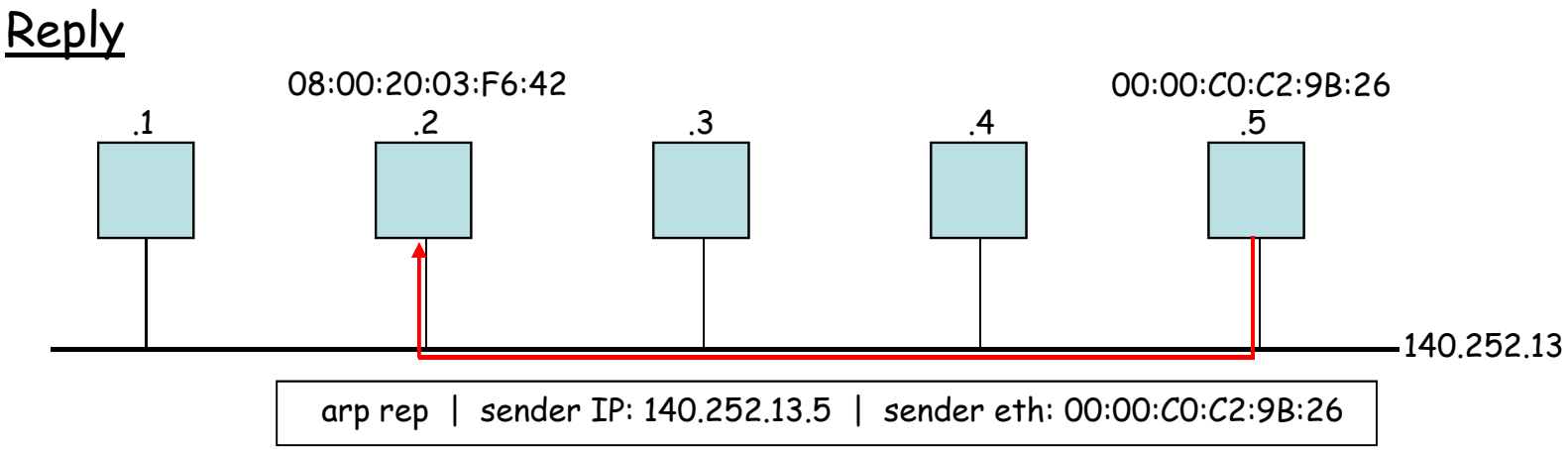
Return-Path: <bill.gates@microsoft.com>
Received: from frogstar.hit.bme.hu (root@frogstar.hit.bme.hu [152.66.248.44])
by shamir.ebizlab.hit.bme.hu (8.12.7/8.12.7/Debian-2)
with ESMTP id h1ADSsxG022719
for <buttyan@ebizlab.hit.bme.hu>; Mon, 10 Feb 2003 14:28:54 +0100
Received: from abcd.bme.hu ([152.66.249.32])
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

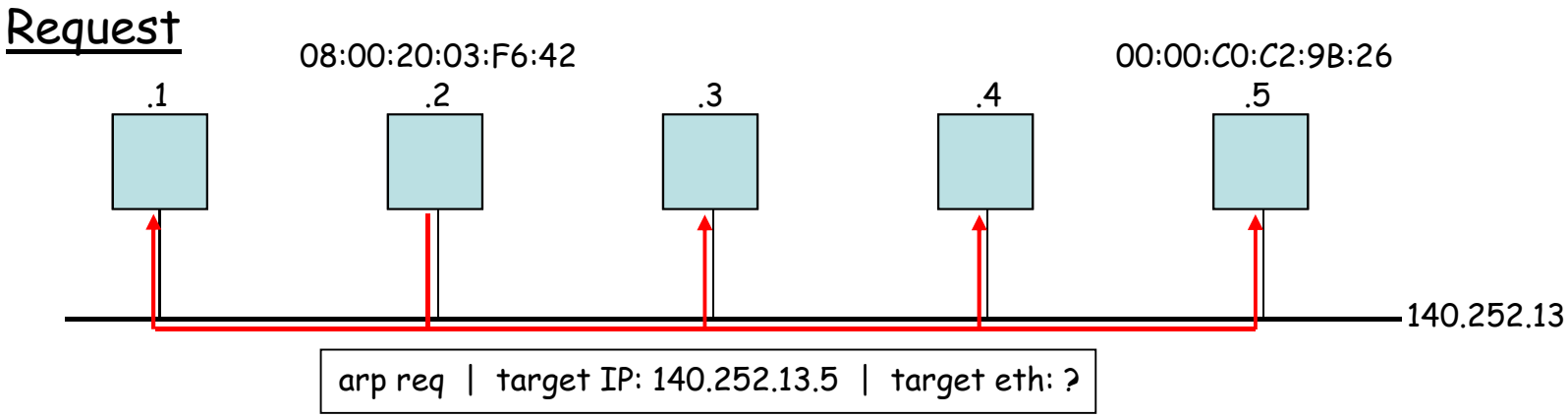
- mapping from IP addresses to MAC addresses

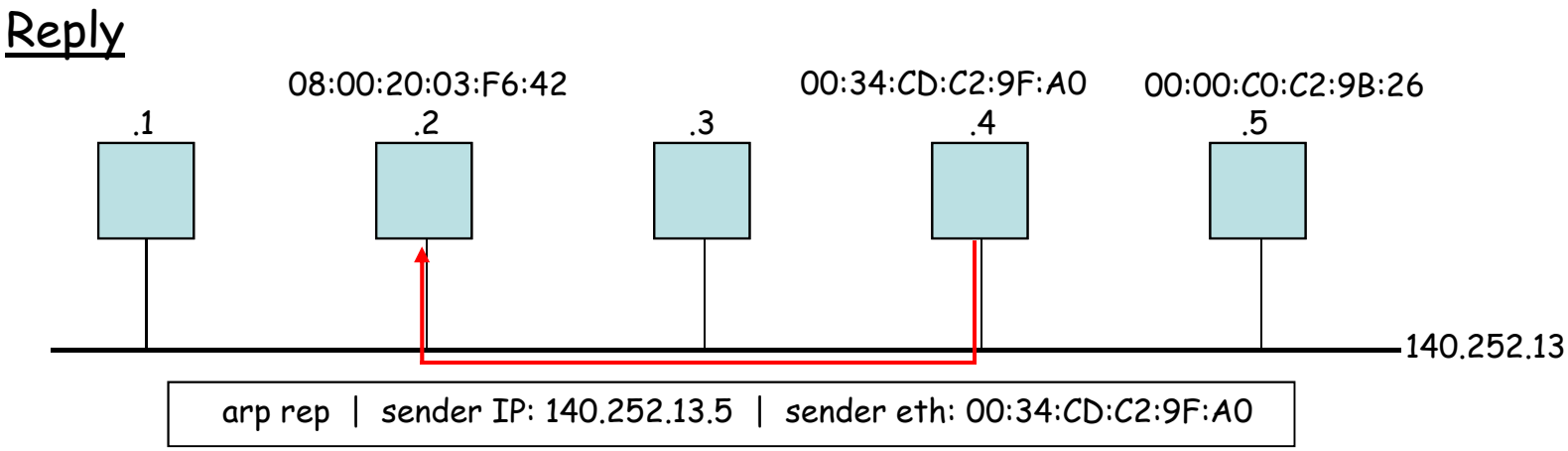




ARP spoofing

- an ARP request can be responded by another host





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

- 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

Communication security services

- 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

- 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

Summary

- basic concepts
  - protocol, security, attack, vulnerability, threat
  - passive vs. active attacks
  - eavesdropping, traffic analysis, masquerade (spoofing), modification, replay, denial of service
  - main communication security services: authentication, confidentiality, integrity, non-repudiation

- some real world examples
  - ARP spoofing, e-mail forgery, eavesdropping Telnet and FTP passwords

The world of Alice and Bob

- the motivation, operation, and analysis of security protocols are often presented as tales about two strange characters, Alice and Bob, and their “friends”

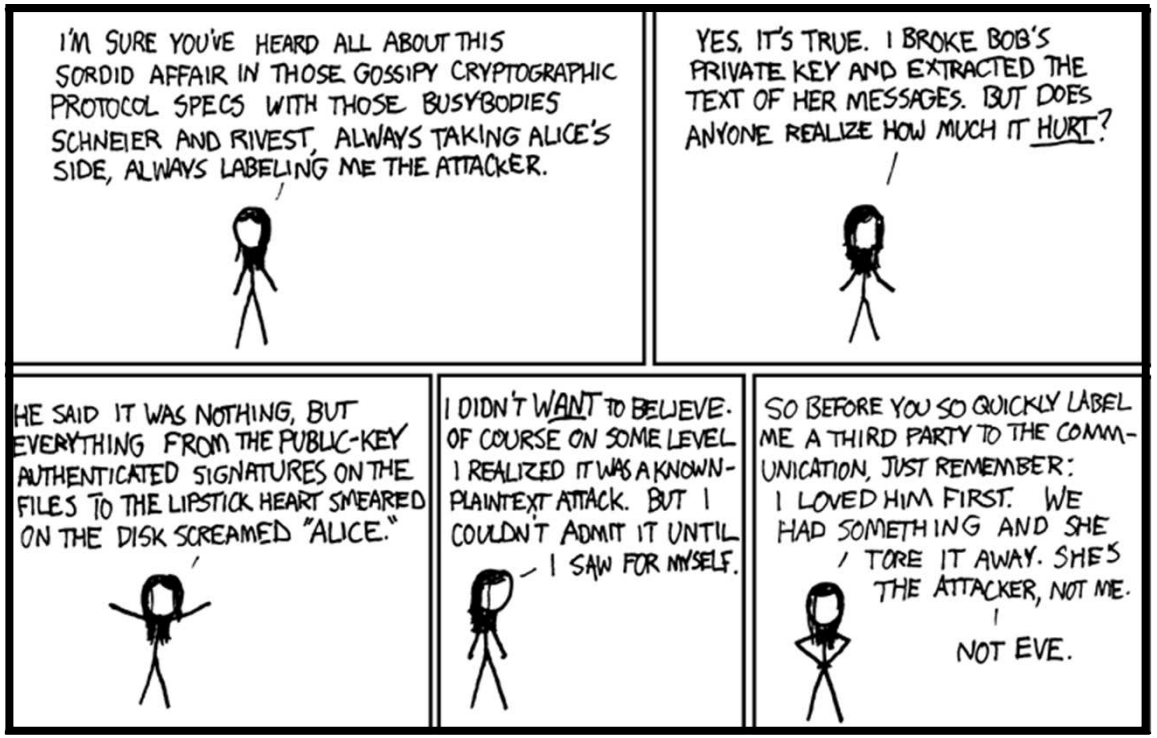
- Alice and Bob
  - they live far from each other and communicate only via Internet, e-mail, or telephone
  - they have actually never met, but for some reason, they frequently need to conduct all sorts of business with each other
  - they rarely trust anyone else, sometimes not even each other
  - their 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

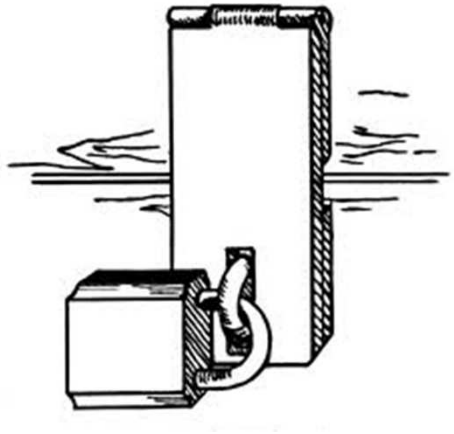
Fame

- Alice and Bob has web site (http://www.aliceandbob.net)
- they are on facebook
- they are in Wikipedia (http://en.wikipedia.org/wiki/Alice_and_Bob)
- there is even a song about them (MC Plus+)
- and many comics…



Exercise

- Design a protocol that allows Alice to send a secret message on a postcard to Bob using Trent/Eve/Trudy as the courier! If needed, they can use a metal box that can be locked with a padlock:



- Try to “implement” your protocol by replacing the postcard with a binary bit string, the metal box with a simple encryption scheme, and the courier with an untrusted network! Does your implementation preserve the security properties of the metaphore?