Security and Networking Basics

Internet Security [1] VU

Engin Kirda engin@infosys.tuwien.ac.at
Christopher Kruegel chris@auto.tuwien.ac.at

Outline

- Introduction and Motivation
- Security Threats
- Open Systems Interconnection (OSI)-Reference Model
  - comparison with TCP/IP protocol suite
- Internet Protocol
  - structure, attributes
  - IP on local networks
  - LAN and fragmentation attacks

Basic terminology

- Who is a “hacker“ and who is a “cracker“?
- What is a script kiddie?
- Why do people hack into systems?
  - Recognition
  - Admiration
  - Curiosity
  - Power & Gain
  - Revenge

One big problem

- System and network administrators are not prepared
  - Insufficient resources
  - Lack of training
- Intruders are now leveraging the availability of broadband connections
  - Many connected home computers are vulnerable
  - Collections of compromised home computers are “good“ weapons (e.g., for distributed denial of service attacks).

Number of Reported Incidents

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

www.cert.org

Vulnerabilities Reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2003

Year	2000	2001	2002	2003
Vulnerabilities	1,090	2,437	4,129	3,784

www.cert.org

A little bit of history

- “Hacking”, actually, has been around for centuries.
  - 1870s: teenagers were playing around with the “new” phone system
  - 1960s: mainframe computers like the MIT’s Artificial Intelligence Lab became staging ground for hackers. Hacker was a positive term
  - 1970s: hackers start tampering with phones (the largest network back then). “phreaks” emerge (phone hackers)
  - Early 1980s: The term “cyberspace” is coined in film *Neuromancer.* First hacker arrests are made. Two hacker groups form: Legion of Doom (US) and Chaos Computer Club (DE)

A little bit of history…

- Late 1980s: Computer Fraud and Abuse Act, CERT (Computer Emergency Response Team) is formed, Kevin Mitnick is arrested
- Early 1990s: AT&T long distance service crashes, crackdown on hackers in the US, hackers break into Griffith Air Force Base, NASA, etc.
- Late 1990s: Hackers deface many government web sites, Defense Department computers receive 250,000 attacks in one year
- 2000s: Number of attacks keep rising, “new” attacks emerge (e.g., phishing)

Changing Nature of the Threat

- Intruders are more prepared and organized
- Internet attacks are easy, low-threat and difficult to trace
- Intruder tools are increasingly sophisticated and easy to use (e.g., by kiddies)
- Source code is not required to find vulnerabilities
- The complexity of Internet-related applications and protocols are increasing – and so is our dependency on them

Security Threats

Information Domain

- Leakage
  - acquisition of information by unauthorized recipients. e.g. Password sniffing
- Tampering:
  - unauthorized alteration/creation of information (including programs)
  - e.g. change of electronic money order, installation of a rootkit

Security Threats

Operation Domain:

- Resource stealing
  - (ab)use of facilities without authorization
- Vandalism
  - interference with proper operation of a system without gain

Methods of attacking

- Eavesdropping
  - getting copies of information without authorization
- Masquerading
  - sending messages with other‘s identity
- Message tampering
  - change content of message

Methods of attacking

- Replaying
  - store a message and send it again later, e.g. resend a payment message
- Exploiting
  - using bugs in software to get access to a host
- Combinations
  - Man in the middle attack
    - emulate communication of both attacked partners (e.g., cause havoc and confusion)

Social Engineering

- Before we get into technical stuff – let's look at a popular non-technical attack method
  - Remember the film "Sneakers"?
  - "The art and science of getting someone to comply to your wishes"
  - Security is all about trust. Unfortunately, the weakest link, the user, is often the target (i.e., "Hit any user to continue" ☺)
  - Social engineering by phone
  - Dumpster Diving
  - Reverse social engineering
- According to report, secret services often use social engineering techniques for intrusion

Choosing a good password

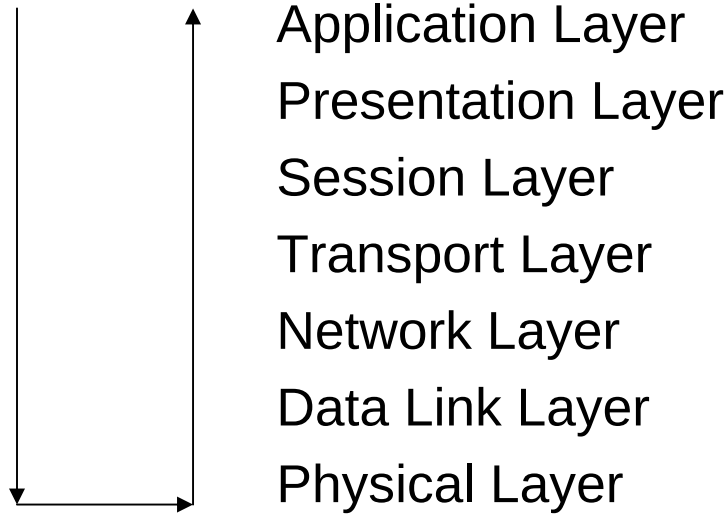
- Retina checks are currently not possible, so guard your password ;-)
  - ***NEVER give your password to anyone***
  - ***Make your password something you can remember***
  - ***Make your password difficult for others to guess***
  - ***DO NOT Change your password because of e-mail***
- Crackers used might crack following passwords:
  - Words in *any* dictionary, Your user name, Your name, Names of people you know, substituting some characters (a 0 (zero) for an o, or a 1 for an l)
  - http://www.openwall.com/john/ (John, passwd cracker)

Choosing a good password 2

- Guidelines…
  - a password that is at least six characters long
  - a good password will have a mix of lower- and upper-case characters, numbers, and punctuation marks, and should be at least 6 characters long
  - take a phrase and try to squeeze it into eight characters (e.g., this is an interesting lecture == ***tiail***), Throw in a capital letter and a punctuation mark or a number or two (== ***0Tiail4***)
  - Something that no one but you would ever think of. The best password is one that is totally random to anyone else except you. It is difficult to tell you how to come up with these, but people are able to do it. Use your imagination!

OSI Reference Model

- Developed by the ISO to support open systems interconnection
  - layered architecture, level n uses service of (n-1)



OSI Reference Model

- Physical Layer
  - connect to channel / used to transmit bytes (= network cable)
- Data Link Layer
  - error control between adjacent nodes
- Network Layer
  - transmission and routing across subnets
- Transport Layer
  - Ordering
  - Multiplexing
  - correctness

OSI Reference Model

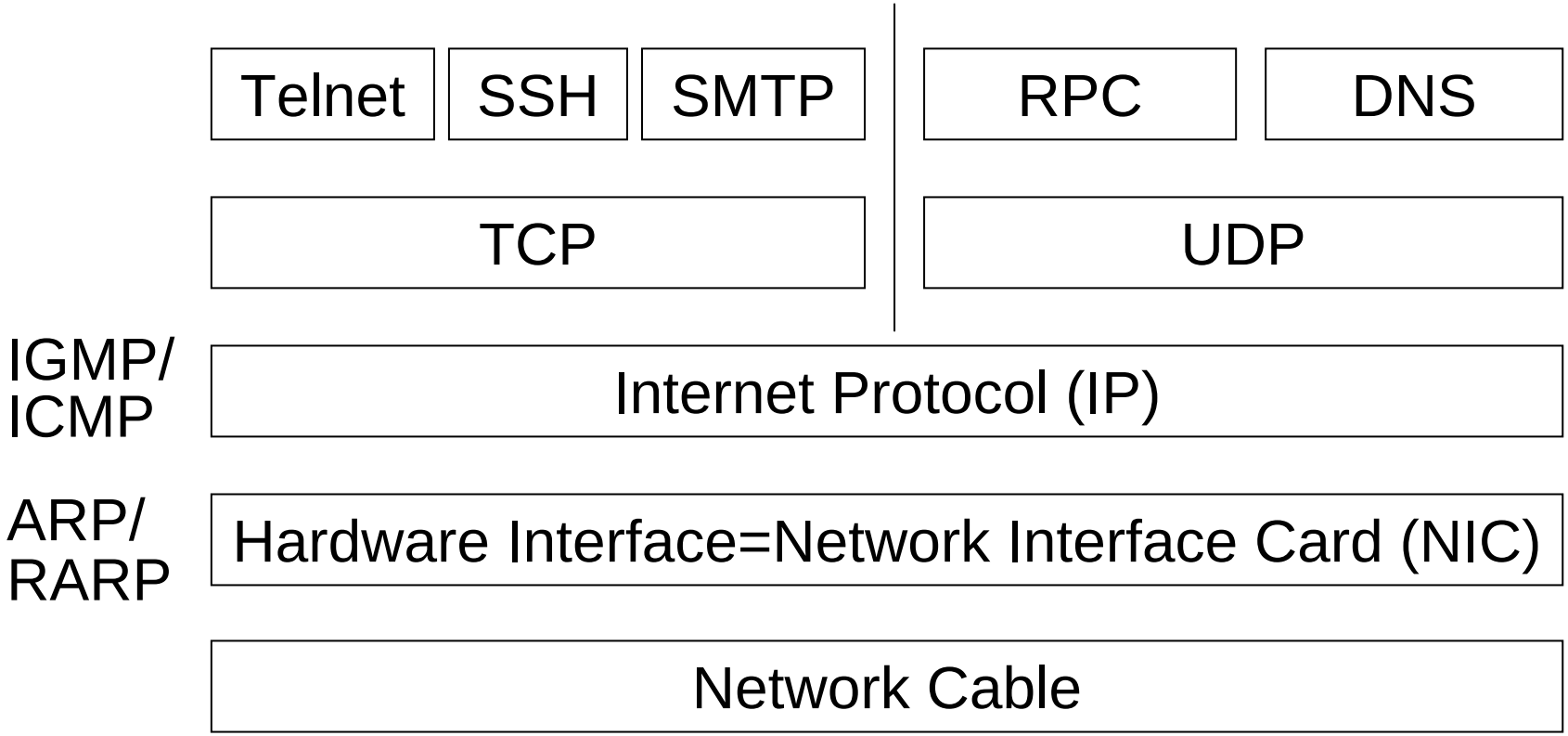
- Session Layer
  - support for session based interaction
  - e.g. communication parameters/communication state
- Presentation Layer
  - standard data representation
- Application Layer
  - application specific protocols

Why layering?

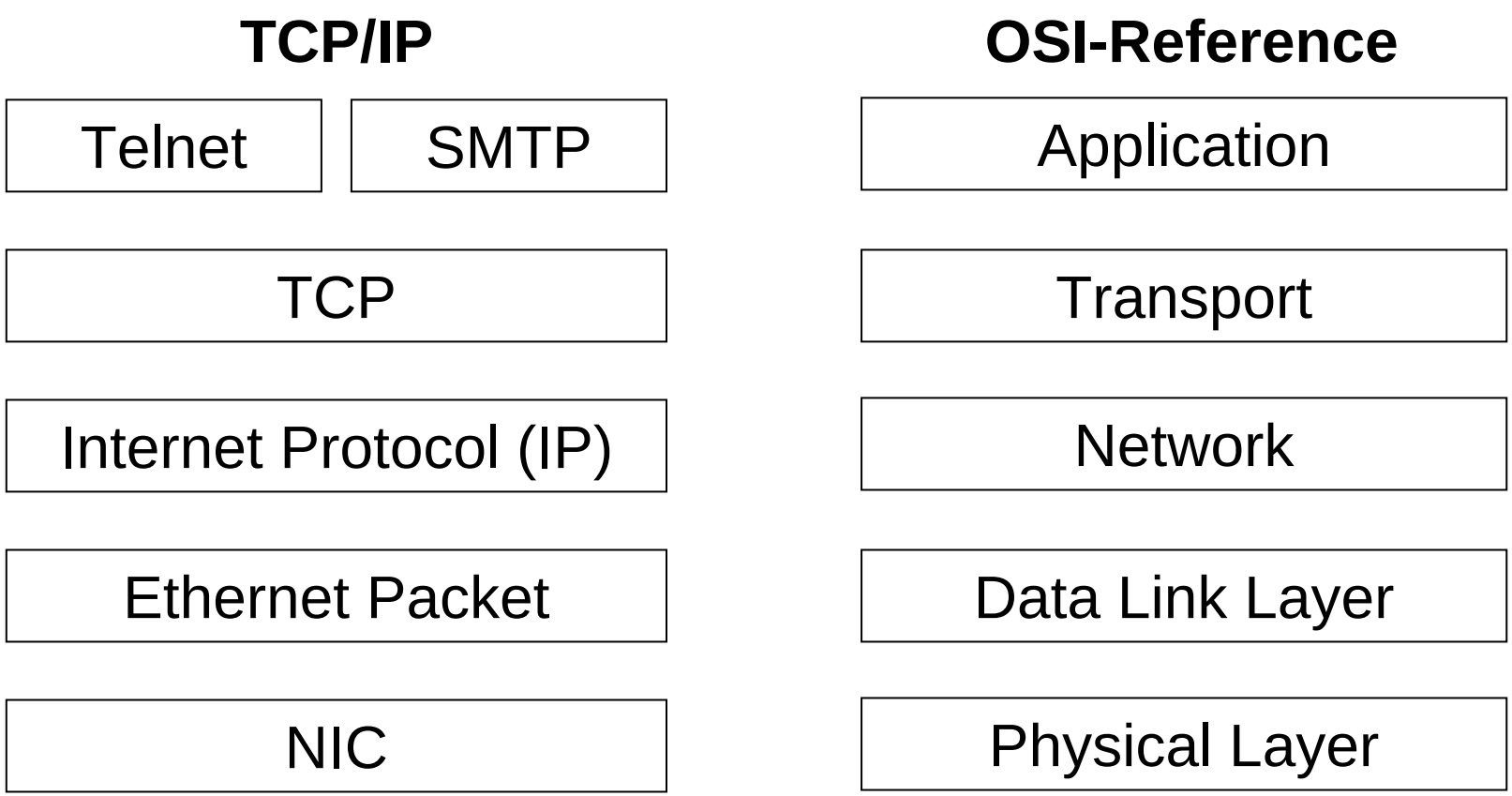
- openness
  - as long as upper layers are the same heterogenous networks can interact
- fertilizes compatibility of systems
- allows vendor specific devices
- allows vendor specific protocols
- provides independence from one manufacturer

- OSI Implementation: MAP (Manufacturing Automation Protocol –GM, Token Ring)

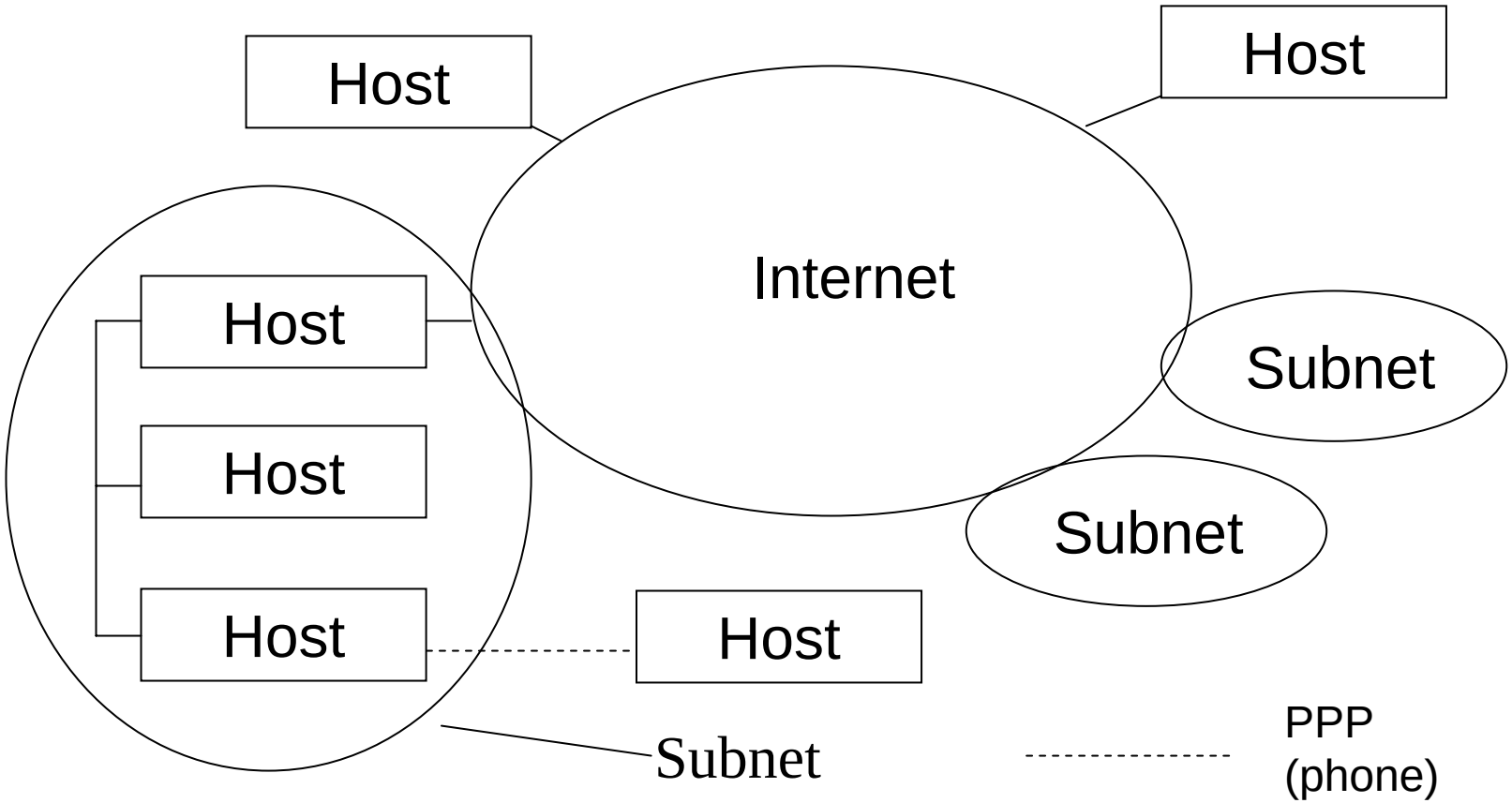
TCP-IP Layering



Mapping


TCP/IP
OSI-Reference
Telnet
SMTP
Application
TCP
Transport
Internet Protocol (IP)
Network
Ethernet Packet
Data Link Layer
NIC
Physical Layer

The Internet



IP Addresses

- IP addresses in IPv4 are 32 bit numbers
  - (class+net+host id)
- each host has a unique IP address for each NIC
- Represented as dotted-decimal notation:
  - 10000000 10000011 10101100 00000001 =128.131.172.1

- Classes: <starts with> <netbits> <hostbits> <#of possible hosts>
- Class A: 0 7 24 16777216
- Class B: 10 14 16 65536
- Class C: 110 21 8 256
- Class D: 1110 special meaning: 28 bit multicast address
- Class E: 1111 reserved for future use

IP Subnetting

- it is unrealistic to have networks with so many hosts
  - divide the hostbits into subnet ID and host ID
  - saves address space
- Example: Class C normally has 24 netbits

  Class C network with subnet mask 255.255.255.240

  240=1111 0000

  | host ID => 16 hosts within every subnet

  subnet ID => 16 subnets within this network

Special IP Addresses

- as source and destination address
  - loopback interface
- as destination address
  - all bits set to 1: local broadcast
  - netid <> only 1s, hostid only 1s: net directed broadcast to netid
- reserved addresses (RFC 1597) - non routable
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.131.255.255
  - 192.168.0.0 - 192.168.255.255

Internet Protocol (IP) 1/2

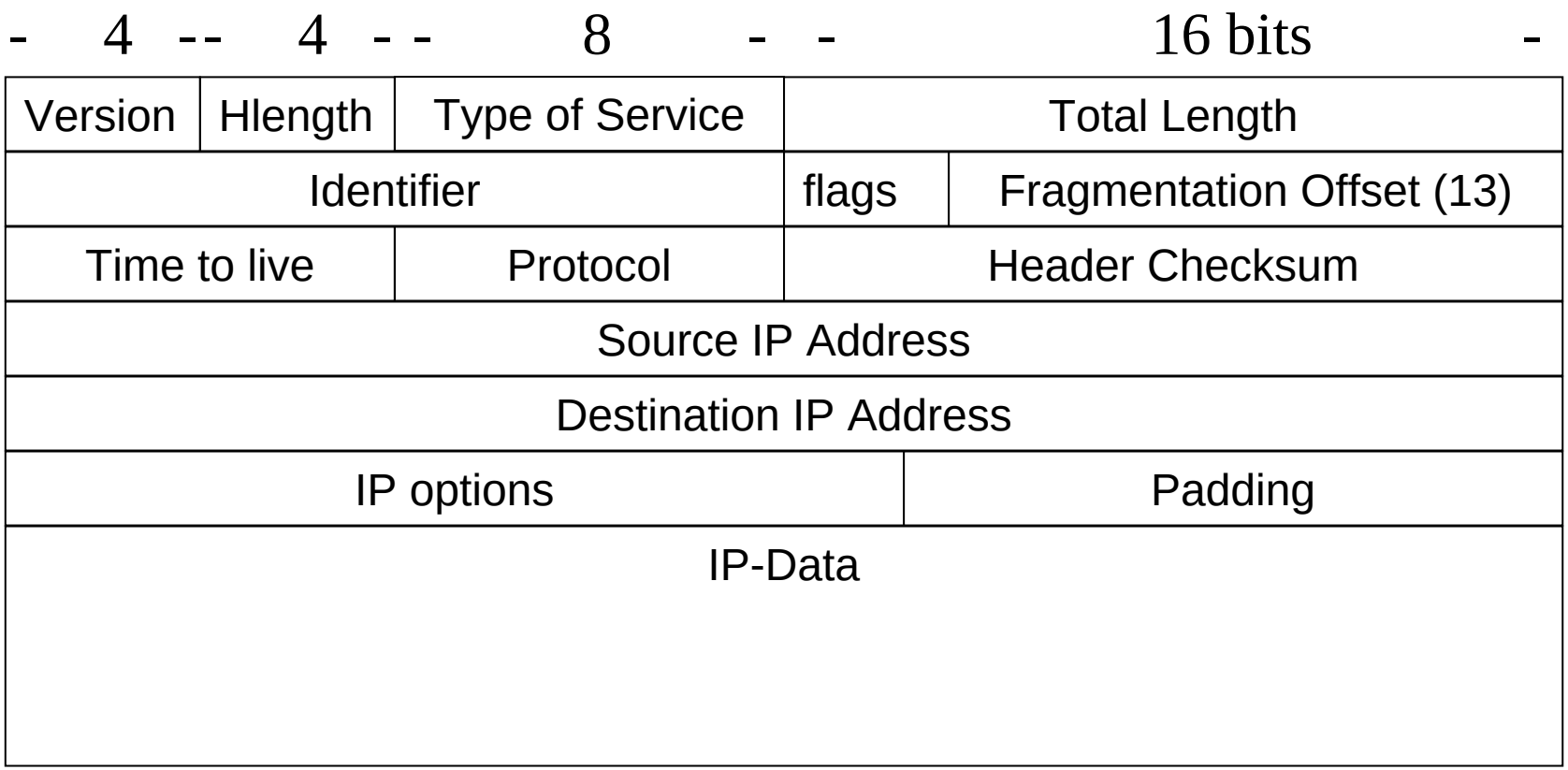
- is the glue between hosts of the Internet
- standardized in RFC 791
- Attributes of delivery
  - Connectionless
  - unreliable best-effort datagram
    - delivery, integrity, ordering, non-duplication are NOT guaranteed
- IP packets (datagrams) can be exchanged by any two nodes that are set up as IP nodes

Internet Protocol (IP) 2/2

- for direct communication IP is tunneled through
  - lower level protocols
    - Ethernet
    - Token Ring
    - FDDI
    - PPP, etc.

- standardized data ordering (network ordering) in the
  - header
  - network ordering = big endian (Linux 0x86: little endian)
    - Least significant byte is stored at the highest byte address memory

IP Datagram


- 4 -- 4 - - 8 - - 16 bits -
Version
Hlength
Type of Service
Total Length
Identifier
flags
Fragmentation Offset (13)
Time to live
Protocol
Header Checksum
Source IP Address
Destination IP Address
IP options
Padding
IP-Data

IP Header

- Normal size: 20 bytes
- Version (4 bits):
  - current value = 4 (IPv4)
- Header length (4 bits):
  - number of 32 bit words in the header, including IP options
- Type of service
  - priority (3 bits), QOS(4), unused bit
- Total length: total size of the IP header and data
- Identifier (16): datagram identification
  - +1 incremented

IP Header

- Flags (3) and offset (13 bits)
  - used for fragmentation of datagram
- Time To Live (8 bits):
  - Allowed number of hops in the delivery process
- Protocol (8bits):
  - specifies the type of protocol which is encapsulated in the datagram (TCP, UDP)
- Header checksum (16):
  - checksum calculated over the IP header.
- Addresses (32+32 bits)
  - specify source and destination

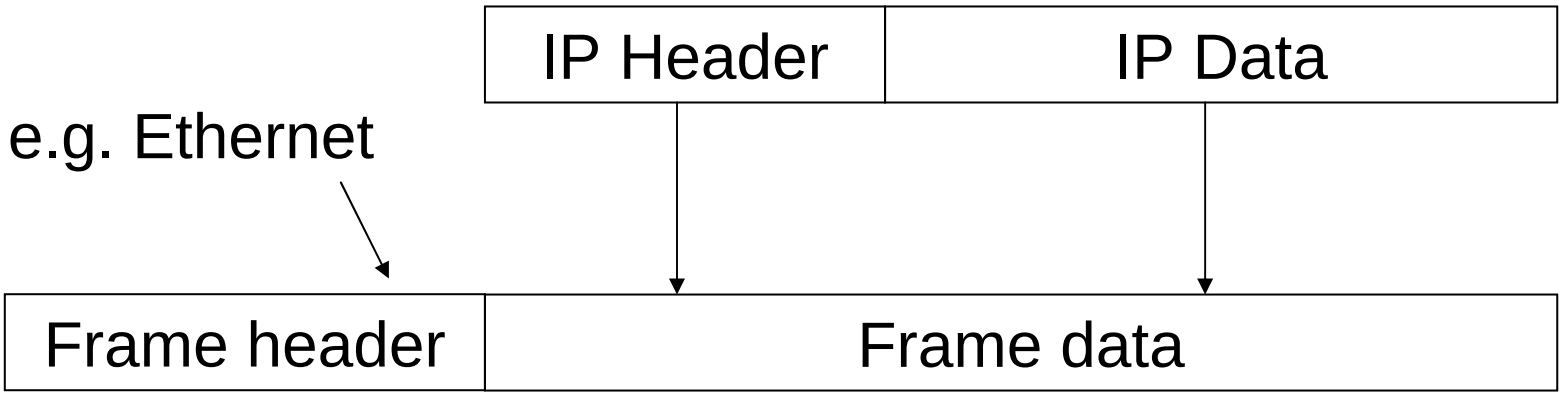
IP Options

- Variable length
- identified by first byte
  - security and handling restrictions:
  - Record route: ip addresses of routers are stored
  - Time stamp: each router records its timestamp
  - Source route:
    - specifies a list of IP addresses that the datagram has to traverse
      - loose: prefer these hosts
      - strict: only use the specified hosts (route)

IP Encapsulation

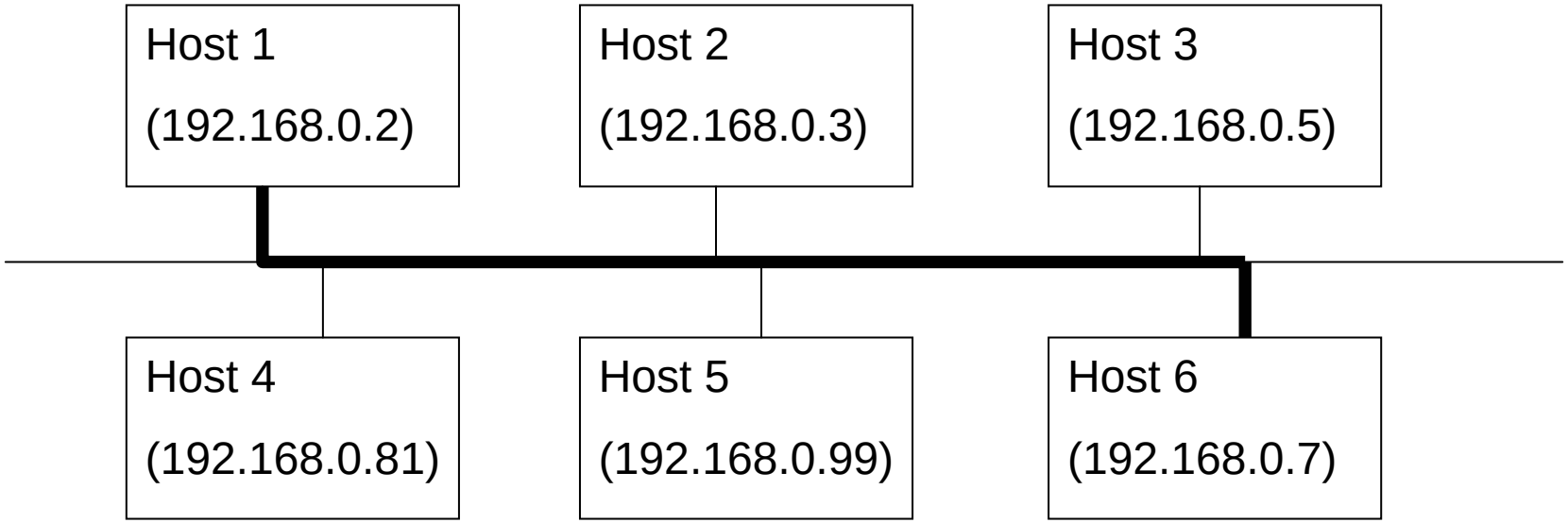
- How are IP datagrams transferred over a LAN?
  Can‘t be done directly because of different formats
  RFC 894, 826 explain IP over Ethernet

Solution: Encapsulation + direct delivery



Direct IP delivery

- If two hosts are in the same physical network the IP datagram is encapsulated and delivered directly



Fragmentation

- Used if encapsulation in lower level protocol demands to split the datagram into smaller portions
  - when datagram size is larger than data link layer MTU
  - (=Maximum Transmission Unit)
- performed at
  - the source host
  - or in an intermediate step
- reassembling
  - = rebuilding the IP packet
  - is ONLY performed at the destination
- each fragment is delivered as a separate datagram

Fragmentation

- adapted IP header is sent in every fragment
- Controlled using 3 bits IP-flags + 13 bits offset
  - Reserved
  - don‘t fragment bit: set if datagram shouldn‘t be fragmented
  - more fragments bit: set if this is not the last fragment
    - of an IP datagram
- if fragmentation would be necessary, but don‘t fragment bit is set -> Error message (ICMP) is sent to sender
- if one fragment is distorted or lost, the entire datagram is discarded

Fragmentation-Attacks

Old trick: Ping of death: violate maximum IP datagram size

- ping is an IP based service: are hosts up and reachable?
- Normally uses 64 bytes payload.
- With fragmentation an IP packet with size > 65535 could be sent

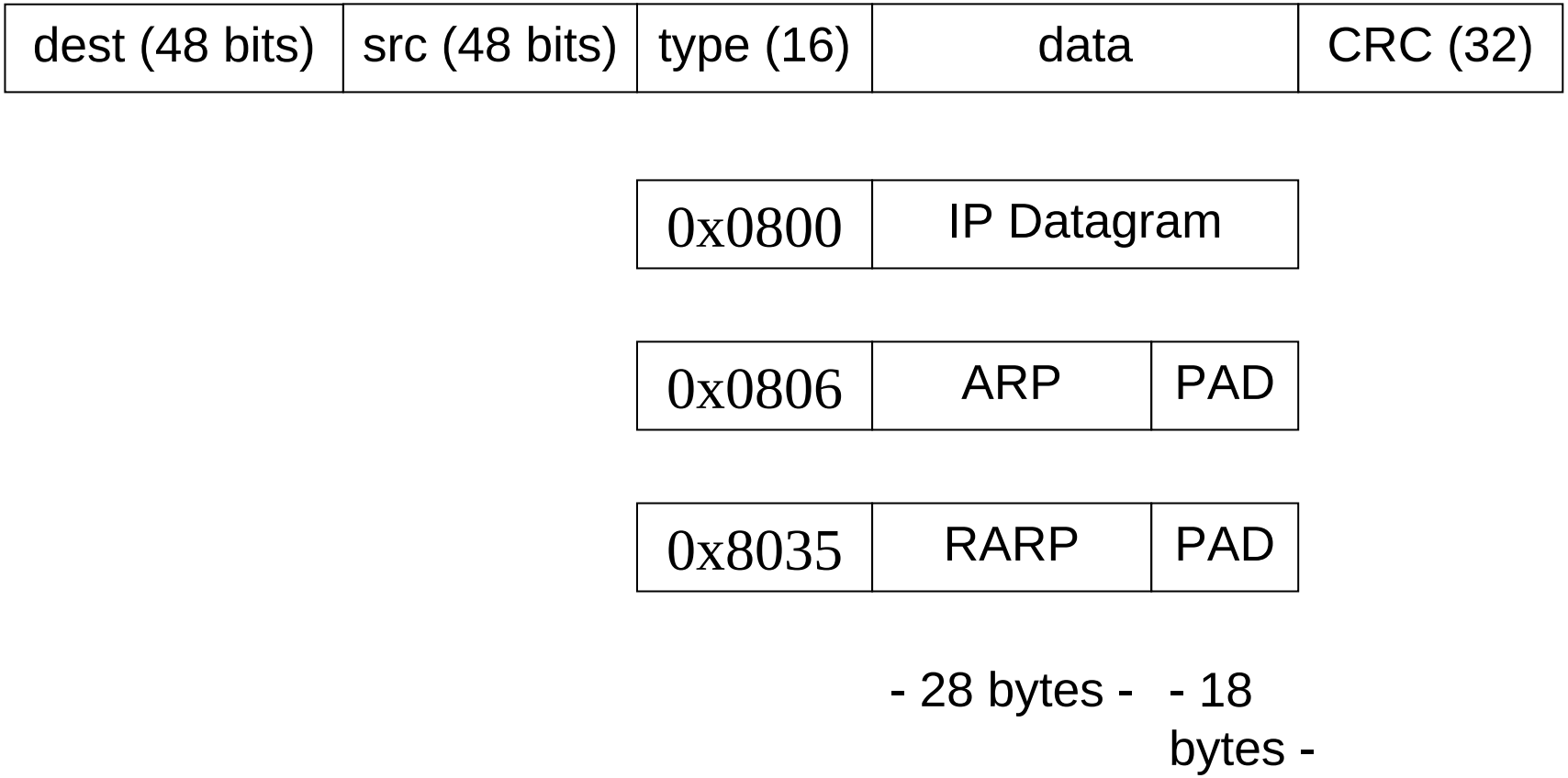
Offset of the last segment is such that the total size of the reassembled datagram is bigger than the maximum allowed size: a static kernel buffer is overflowed causing a kernel panic (worked with Windows, Mac, Linux 2.0.x)

Fragmentation-Attacks

Old trick: TCP overwrite: fool the firewall

- IP datagram containing TCP traffic is fragmented
- TCP header contains allowed port (e.g. 80)
- => firewall lets this packet pass
- data is sent fragmented
- one packet contains frag-offset=1: ports will be over-
    - written (e.g. new port = 23).
- after packet has been reassembled completely, it will be delivered to the new port

Ethernet


dest (48 bits)
src (48 bits)
type (16)
data
CRC (32)
0x0800
IP Datagram
0x0806
ARP
PAD
0x8035
RARP
PAD
- 28 bytes -
- 18 bytes -

Ethernet

- Widely used link layer protocol
- Carrier Sense, Multiple Access, Collision Detection
- Addresses: 48 bits (e.g. 00:38:af:23:34:0f), mostly
  - hardwired by the manufacturer
- Type (2 bytes): specifies encapsulated protocol
  - IP, ARP, RARP
- Data:
  - min 46 bytes payload (padding may be needed), max 1500 bytes
- CRC (4 bytes)

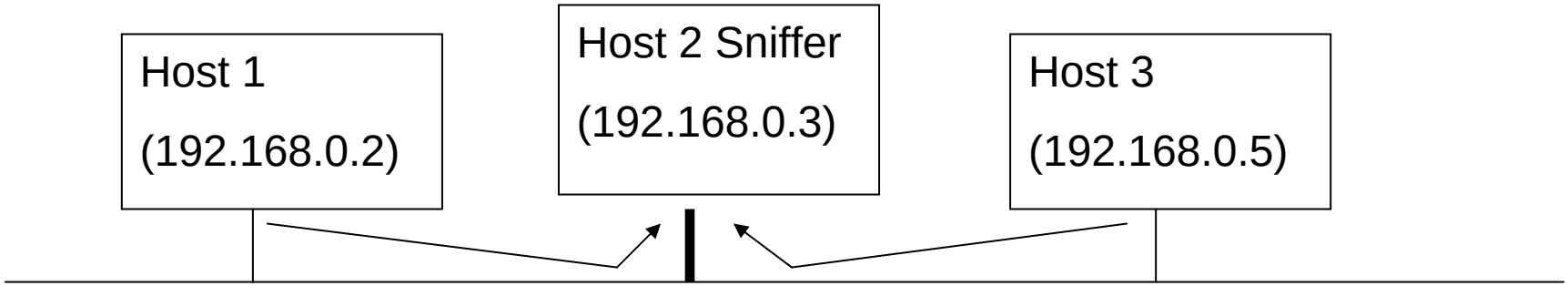
LAN Attacks

- Goals:
  - Information Recovery
  - Impersonate Host
  - Tamper with delivery mechanisms

- Methods:
  - Sniffing
  - IP Spoofing (next lectures)
  - ARP attacks (next lectures)

Network Sniffing

- Is the base for many attacks
  - attacker sets computer‘s NIC into **promiscuous mode**
  - NIC delivers all arriving packets to IP layer
  - can access all the traffic on the segment
- many protocols transfer authentication information in cleartext => collect username/password etc.
- many tools available: tcpdump -x, dsniff etc.



Network Sniffing

Is Sniffing also possible at switched Ethernet, where the switch only forwards the right packets to your host? YES!

- MAC flooding
  - Switch maintains table with MAC address/port mappings
  - flooding switch with bogus MAC addresses will overflow table
  - switch will revert to hub mode

- MAC duplicating/cloning
  - you can buy NICs with reconfigurable MAC addresses
  - switch will record this in table and sends traffic to you

Detecting Sniffers 1/2

- interface is in promiscuous mode
  - use programs like /sbin/ifconfig to find out state of NIC
- suspicious DNS lookups
  - sniffer attempts to resolve names associated with IP addresses
  - trap: generate connection from fake IP => detect DNS traffic

Detecting Sniffers 2/2

- sending IP packet to a replying service (DNS, Telnet)
  - set the destination IP Address to that host
  - set the MAC address to a non-existing one
  - host replies => all packets are delivered to the TCP/IP stack

- latency
  - use ping to analyze response time of host A
  - generate huge amount of traffic to other hosts
  - analyze response time of host A
  - if in promiscuous mode: larger response time, because all the packets are analyzed

Conclusion

- In this lecture, we looked at security and networking basics
  - Security threats
  - Social Engineering
  - OSI Reference Model and TCP/IP Protocol Suite
  - Ethernet, IP
  - LAN and Fragmentation attacks
- Next lecture: We starting looking at TCP/IP Protocol Suite and related attacks
- See you after the holidays! Enjoy them ;-)