1. Network Security: Introduction

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

September 20, 2020

Section 1

About Teachers

Teachers

Ing. Tomáš Čejka, Ph.D.

- Scope of interest: network monitoring, anomaly detection, network security
- Studied at CTU in Prague, FEE (Bc.), FIT (Ing., Ph.D.)
- Researcher&Developer in CESNET
  Leader of a research&development team
- Participant on several projects related to network monitoring and network security
- Supervisor of many (successful) bachelor/master thesis
- Leader of a research&development team here at FIT CTU in Prague
  - Network Traffic Monitoring Laboratory
  - `https://netmon.fit.cvut.cz`

Contact

Tomas Cejka

- cejkato2@fit.cvut.cz
- cejkat@cesnet.cz
- @tomcejka
- A-954

PGP (cejkato2):

```
1F46 1E9E 7248 99FB 2666  8E6B 512E 05B5 D9B5 0B1B
```

PGP (cejkat):

```
BB66 06E7 08E9 836D 3936  B5B2 8F63 32E3 D255 DA7A
```

Teachers

Ing. Simona Buchovecká

- Ph.D. candidate
- Studied at CTU in Prague, FEE (Bc.), FIT (Ing.)
- Cyber & Privacy - Threat Management Leader at PwC
- Teacher of English course (MIE-SIB)

Section 2

Course Introduction

“Disclaimer”

- Attacking someone or someone’s device(s) is BAD — don’t do it!!! (without prior written agreement)
- IT Crowd Piracy warning: `https://www.youtube.com/watch?v=ALZZx1xmAzg`
- Defense is very important — we should learn how attacks work in order to prevent them.
- Attacks are very frequent — we must be prepared.

Rules of This Course

- See Course Pages: cs / en
- Homeworks
- Tutorials

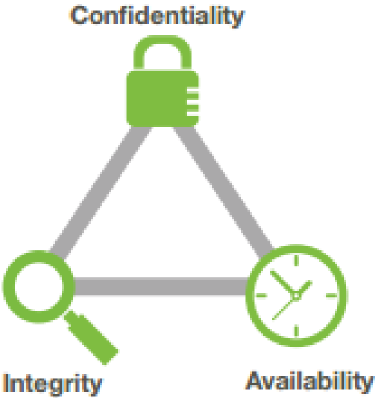
Section 3

Insight to Network Security

Event & Incident (NIST framework)

- **Event** is any observable occurrence in a system or network
- **Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data
- **A computer security incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- Security Incident != Operations incident (different objectives)

(Network) Security Mission



Data:

- At rest
- In transit

Security & Risk Management

- Security is aimed at preventing loss or disclosure of data, while sustaining authorized access
- Risk = threat*vulnerability
- Security aims to remove vulnerabilities and blocking threat agents/events
- Risk management
  - Identifying factors that could damage or disclose data
  - Evaluating those factors – data value vs. countermeasure cost
- Security
  - Implementing cost effective countermeasures

Common Methods to Mitigate Risks

- Compartmentalize
- Secure Fail
- Defense-in-Depth
- Least privilege
- Security-by-Obscurity

The Weakest Link of (Network) Security

- (In)Secure protocols?
- Passwords?
- Client certificates?

NO!

- The **human factor** is the weakest link
- Kevin Mitnick: "... I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and JUST ASK FOR IT"
- Important detail: attacker must pretend to be an insider

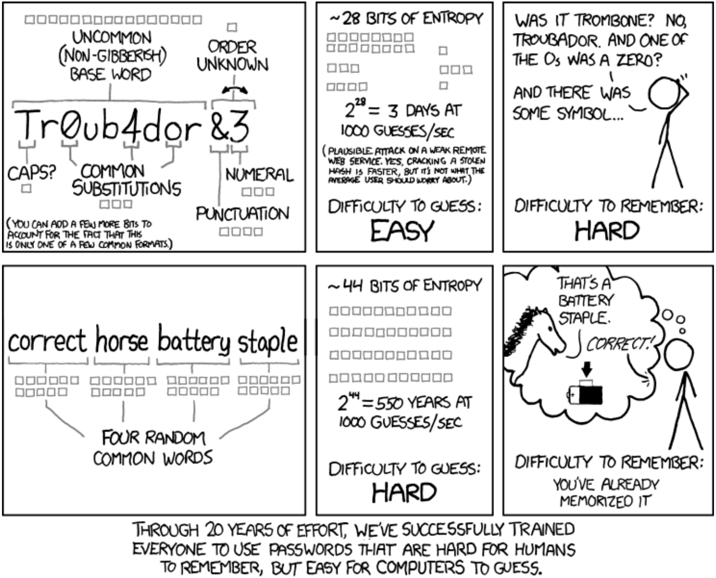
Weakest Links of Network Security

The Human Factor:

- The trust of humans can be manipulated by social engineers
- No matter how advanced technological security measures

Protocol and service related weaknesses:

- Authentication: fake IP or MAC addresses, etc.
- Authorization: fake servers like DHCP, DNS, etc.

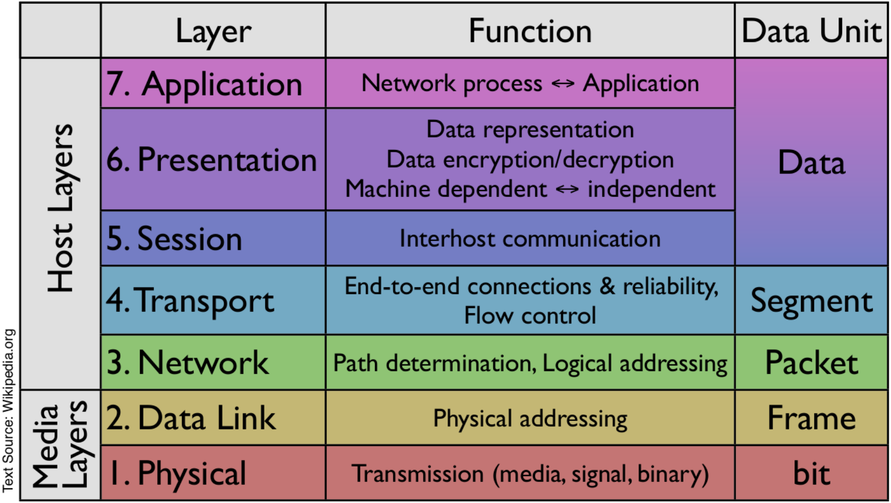

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com/936/

Section 4

Network Models and Protocols

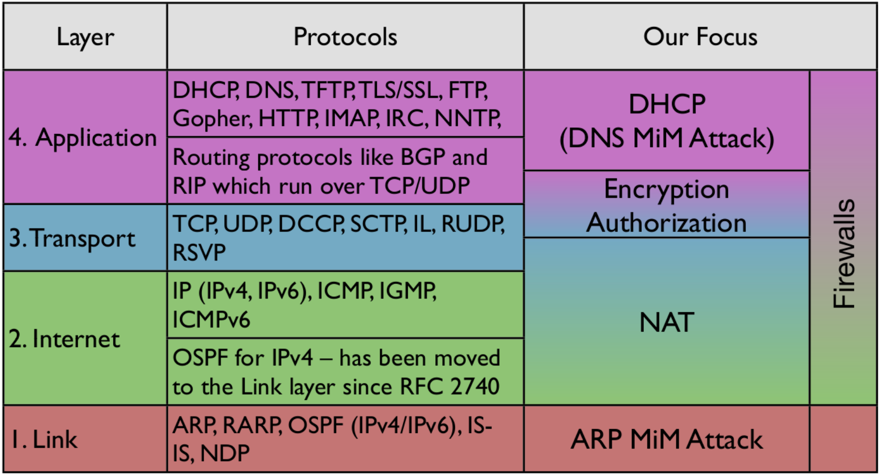
Open Systems Interconnection Model



	Layer	Function	Data Unit
Host Layers	7. Application	Network process ↔ Application	Data
	6. Presentation	Data representation Data encryption/decryption Machine dependent ↔ independent	
	5. Session	Interhost communication	
	4. Transport	End-to-end connections & reliability, Flow control	Segment
	3. Network	Path determination, Logical addressing	Packet
Media Layers	2. Data Link	Physical addressing	Frame
	1. Physical	Transmission (media, signal, binary)	bit

Text Source: Wikipedia.org

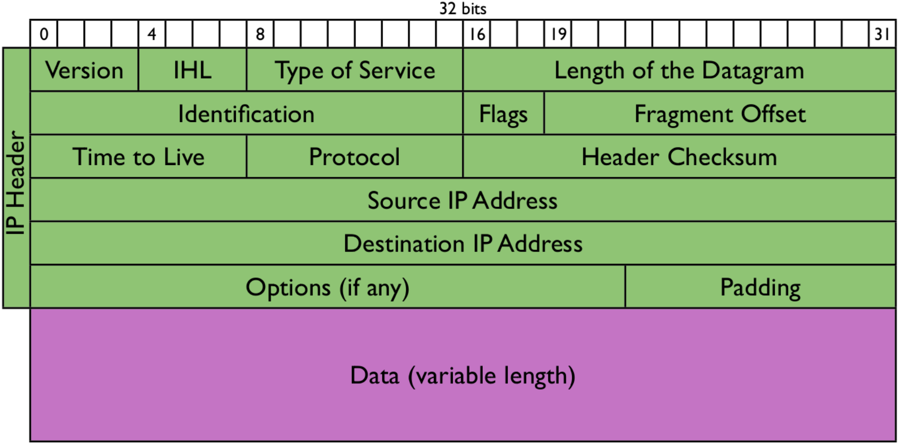
Internet Protocol Suite - RFC 1122



Layer	Protocols	Our Focus	
4. Application	DHCP, DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP,	DHCP (DNS MiM Attack)	Firewalls
	Routing protocols like BGP and RIP which run over TCP/UDP	Encryption Authorization	
3. Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP	NAT	
2. Internet	IP (IPv4, IPv6), ICMP, IGMP, ICMPv6		
	OSPF for IPv4 – has been moved to the Link layer since RFC 2740		
1. Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP	ARP MiM Attack	

Text Source: Wikipedia.org

IPv4 Header Structure



32 bits

0 4 8 16 19 31

IP Header

Version | IHL | Type of Service | Length of the Datagram

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

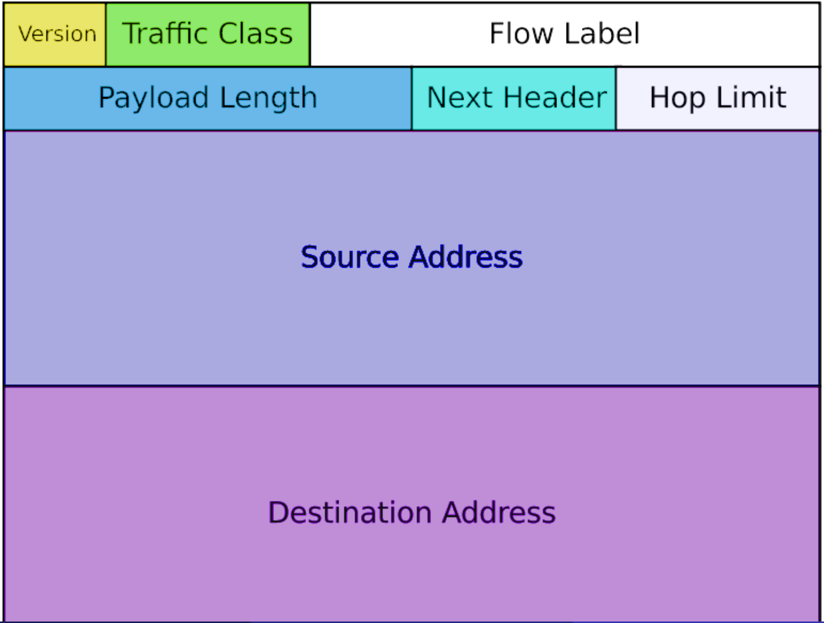
Source IP Address

Destination IP Address

Options (if any) | Padding

Data (variable length)

IPv6 Header Structure



Version

Traffic Class

Flow Label

Payload Length

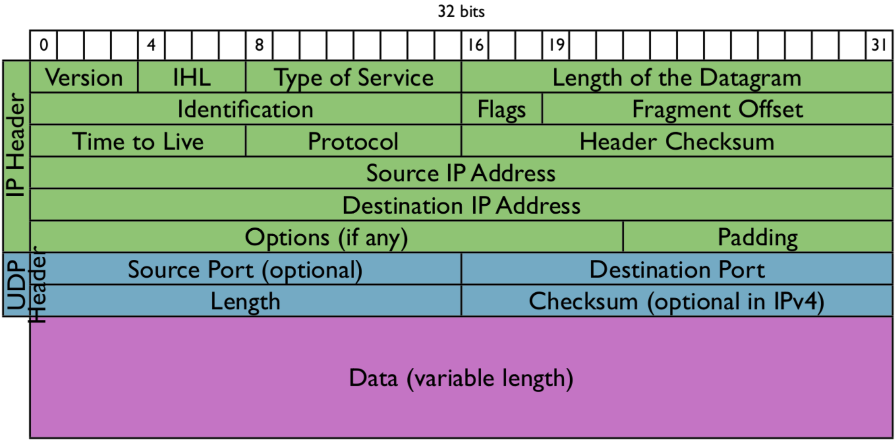
Next Header

Hop Limit

Source Address

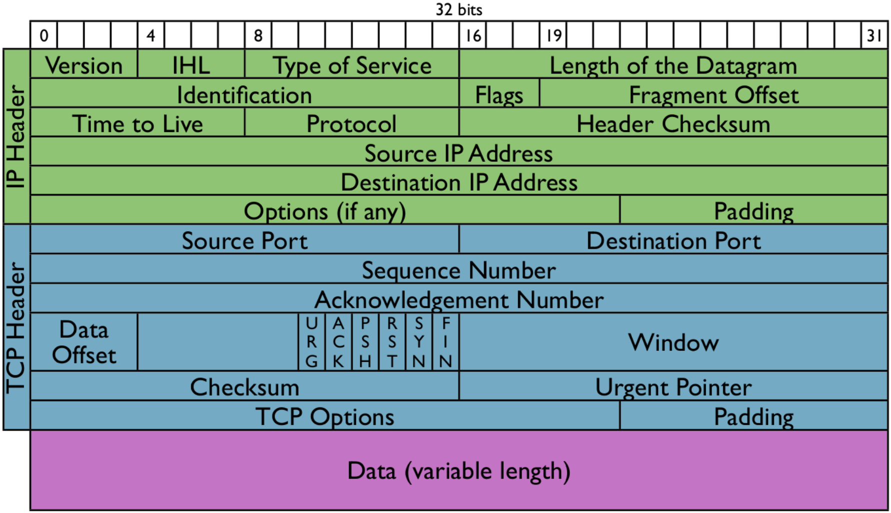
Destination Address

UDP Header Structure



Version	IHL	Type of Service	Length of the Datagram	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options (if any)				Padding
Source Port (optional)			Destination Port	
Length			Checksum (optional in IPv4)	
Data (variable length)				

TCP/IP Packet Structure



32 bits

0 4 8 16 19 31

IP Header

Version | IHL | Type of Service | Length of the Datagram

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options (if any) | Padding

TCP Header

Source Port | Destination Port

Sequence Number

Acknowledgement Number

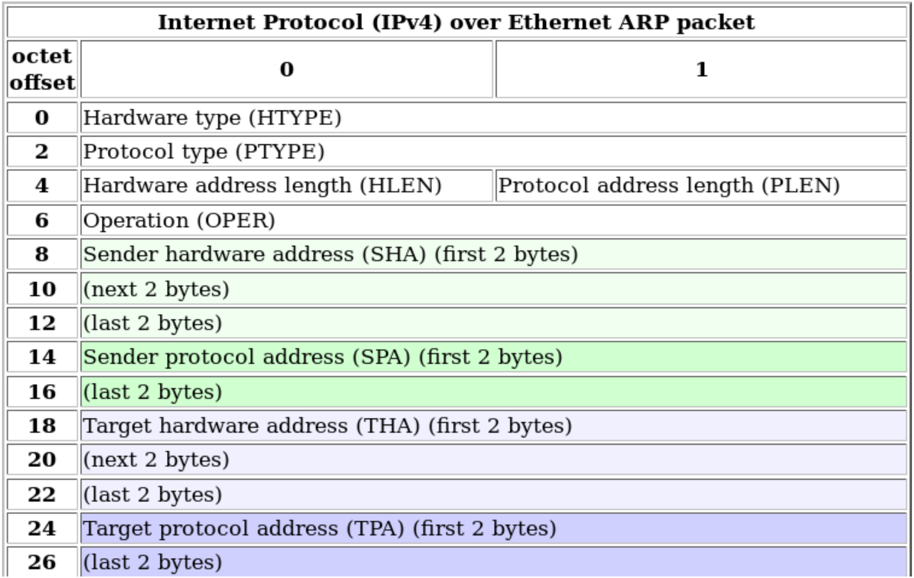
Data Offset | URG | ACK | PSH | RST | SYN | FIN | Window

Checksum | Urgent Pointer

TCP Options | Padding

Data (variable length)

ARP Header Structure



Internet Protocol (IPv4) over Ethernet ARP packet

octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

DHCP

Dynamic Host Configuration Protocol

Allows a computer in a LAN to be configured automatically:

- IP Address
- Gateway
- DNS Servers etc...

Maintains a database for keeping track of connected computers

Operation Phases: DHCP Discovery

- The client broadcasts messages on the physical subnet to
  - discover available DHCP servers
  - User Datagram Protocol (UDP) packet
  - with the broadcast destination 255.255.255.255 (or a specific subnet broadcast address)

Operation Phases: DHCP Offer

- A DHCP server receives an IP lease request
- Reserves an IP address for the client
- Sends a DHCPOFFER message to the client
- The message contains:
  - The client's MAC address
  - the offered IP address
  - a subnet mask
  - the lease duration
  - and the IP address of the DHCP server

Operation Phases: DHCP Acknowledgement

- The server sends the client a DHCPPACK packet with:
  - the lease duration
  - any other configuration information the client requested.
- This completes the IP configuration process

Operation Phases: DHCP Atacks

- Two types of attacks
  - Unauthorized DHCP Servers (Rogue Servers)
  - Falsified DHCP Clients (DHCP Starvation)
- Rogue DHCP Server
  - A trojan installed on an infected machine
  - Serves bogus DHCP packets to other machines
  - If the Trojan is fast it can modify the network configuration of other computers.
- DHCP Starvation
  - Use-up IP Addresses

Section 5

Basic Defense: Packet Filtering

Firewalls

- Block unauthorized access
- Permit authorized communications
- Often provide NAT and DHCP
  - Example: Basic residential routers
- Software firewalls can be installed on a host to protect a single computer

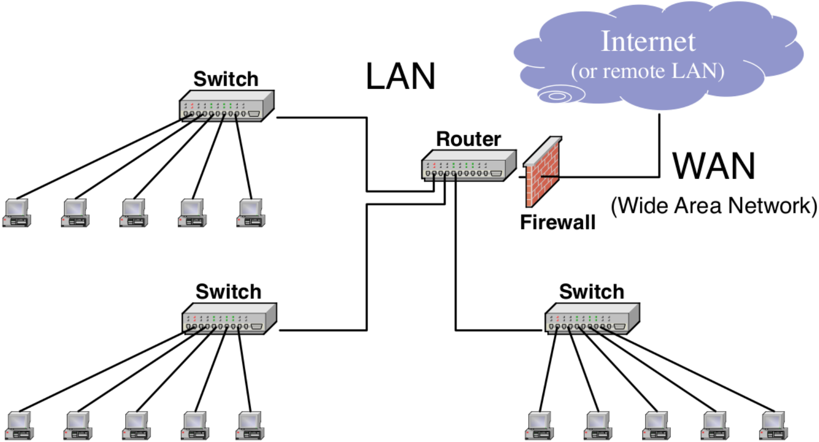
Types of Firewalls

- Packet filter: inspects each packet and apply specified rules
- Application layer: “understand” certain applications and protocols (FTP, DNS, web)
- Stateful filter: maintain sessions or network flows to detect out-of-place packets
- NAT: Provides basic firewalling protection

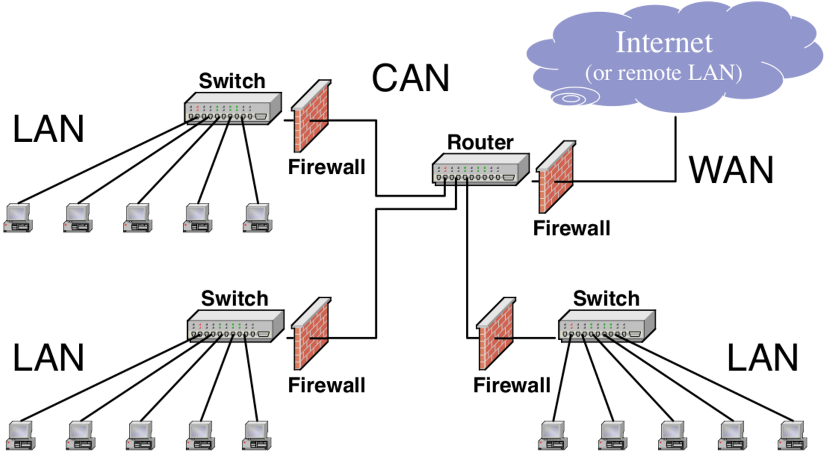
Practical self-study:

investigate *iptable*, *nftables*, *firewalld*

LAN Security #1



LAN Security #2



Questions?