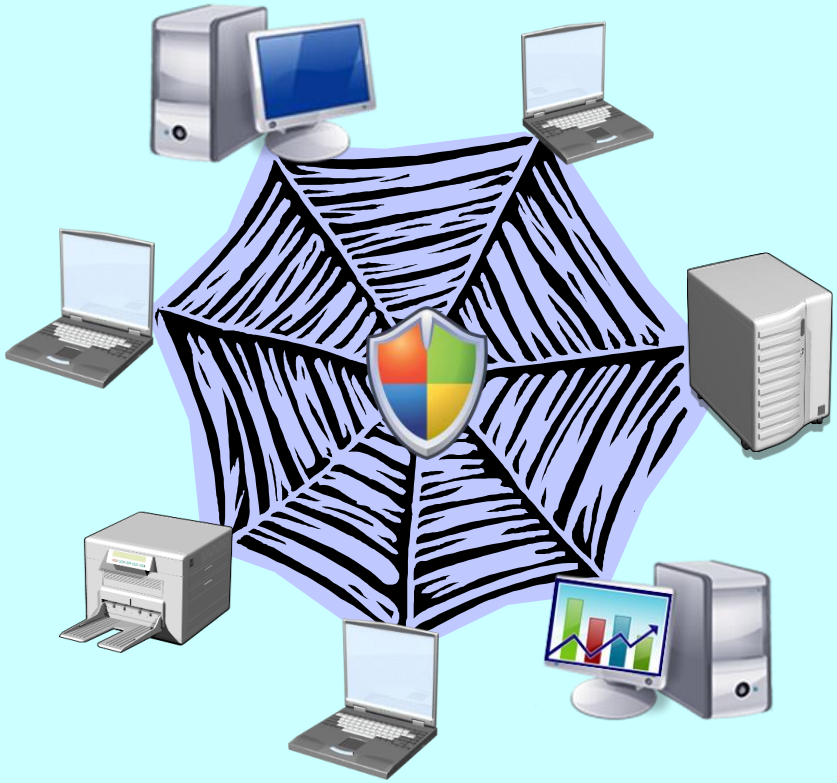
Network Security



Michał Szychowiak, PhD

https://www.cs.put.poznan.pl/mszychowiak/en

3 Tiers Architecture

© Michał Szychowiak, 2022

Agenda

1. **TCP/IP 101**
   - Data-Link, IP, TCP, UDP, DNS, …
2. **Network attacks**
3. **Network protection**
   - Authentication protocols
4. **Mobile networks**
   - WiFi
   - Telecom networks

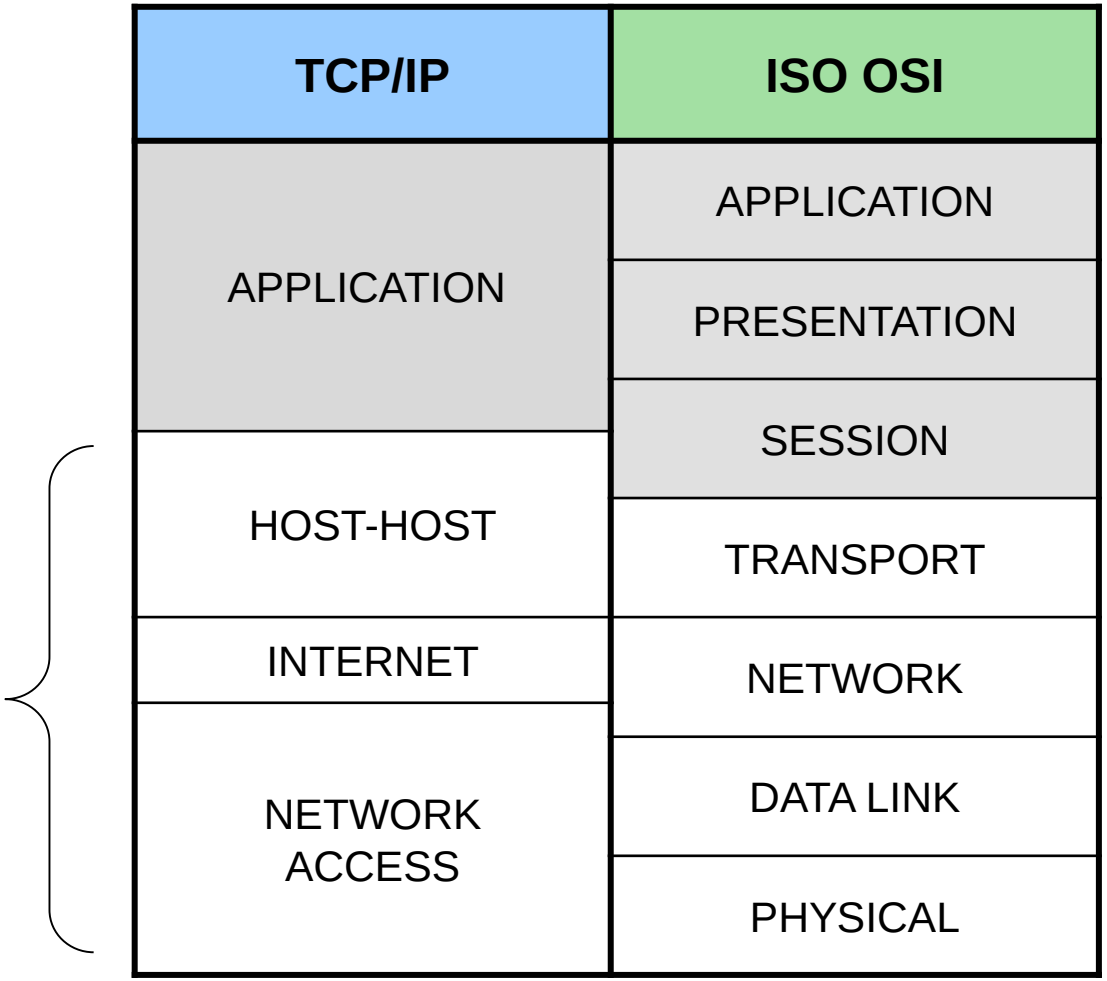
© Michał Szychowiak, 2022

TCP/IP & OSI

no security guarantees

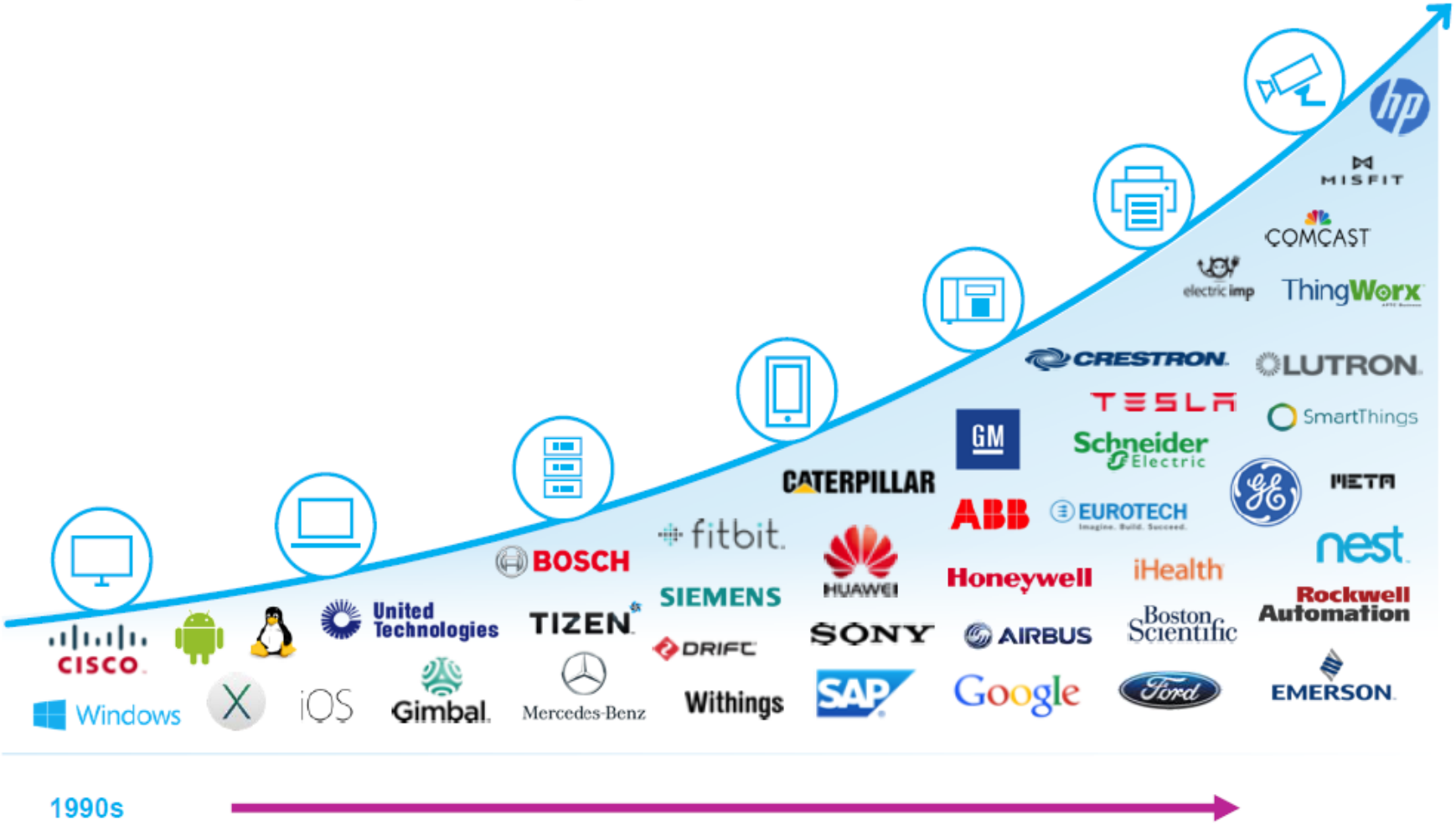
because

no security mechanism implemented



© Michał Szychowiak, 2022

TCP/IP everywhere



Embedded TCP/IP libraries

Microchip TCP/IP	https://www.securityfocus.com/bid/59603/info
uIP, lwIP	https://www.kb.cert.org/vuls/id/210620
RTCS TCP/IP	https://www.us-cert.gov/ics/advisories/ICSMA-17-250-02A
picoTCP	https://nvd.nist.gov/vuln/detail/CVE-2017-1000210
FreeRTOS+TCP	https://blog.zimperium.com/freertos-tcpip-stack-vulnerabilitiesdetails
Nucleus NET	https://us-cert.cisa.gov/ics/advisories/icsa-19-318-01
Interpeak IPnet	https://us-cert.cisa.gov/ics/advisories/icsa-19-274-01
InterNiche NicheStack	https://us-cert.cisa.gov/ics/advisories/icsa-20-105-08
Treck TCP/IP	https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01
. . .	

© Michał Szychowiak, 2022

Data Link Layer

Ethernet

- shared medium
- broadcast, multicast (addresses)
- NIC *promiscuous* mode
- simple CRC code

Network devices

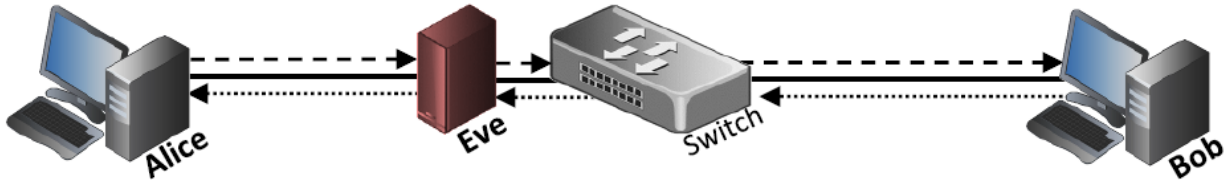
- dynamic switching (transparent)
- static switching (VLAN + DTP=*Dynamic Trunking Protocol*, VxLAN + VTEP=*Virtual Tunnel EndPoint*) → VLAN hopping

© Michał Szychowiak, 2022

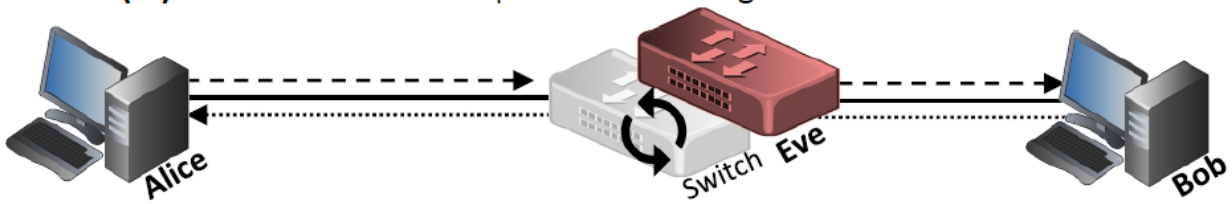
Data Link Layer

MitM attacks

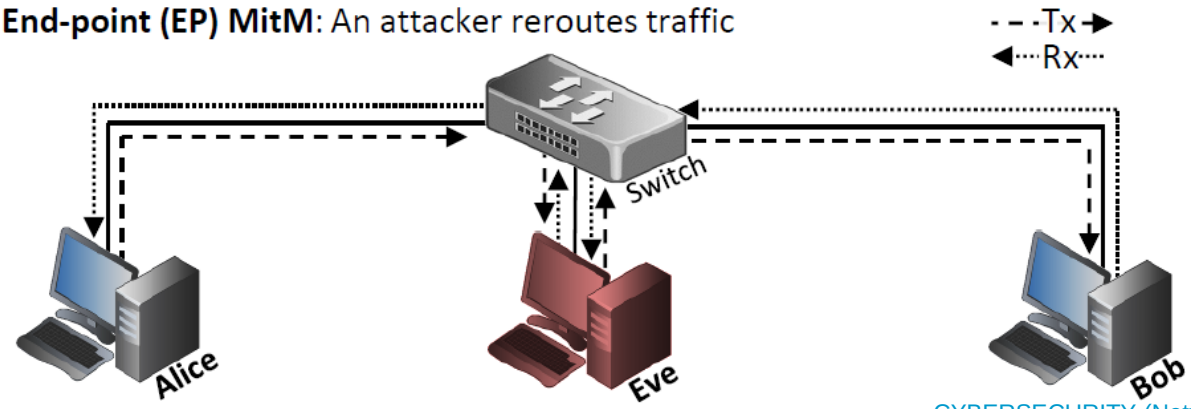
In-line (IL) MitM: An attacker physically intercepts traffic



In-Point (IP) MitM: An attacker replaces an existing network switch



End-point (EP) MitM: An attacker reroutes traffic



© Michał Szychowiak, 2022

Data Link Layer

Ethernet

- shared medium
- broadcast, multicast (addresses)
- NIC *promiscuous* mode
- simple CRC code

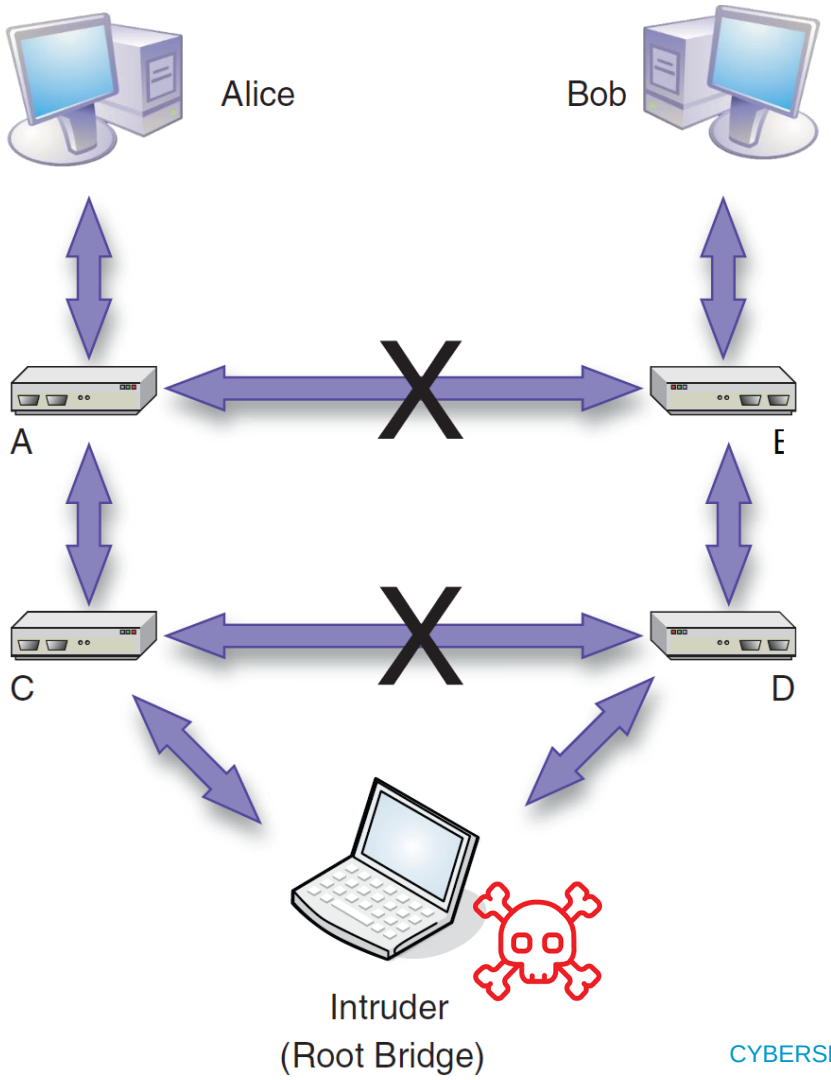
Network devices

- dynamic switching (transparent)
- static switching (VLAN + DTP=*Dynamic Trunking Protocol*, VxLAN + VTEP=*Virtual Tunnel EndPoint*) → VLAN hopping 
- autonomic protocols (STP, RSPT, MSTP, Channel Discovery , …)

© Michał Szychowiak, 2022

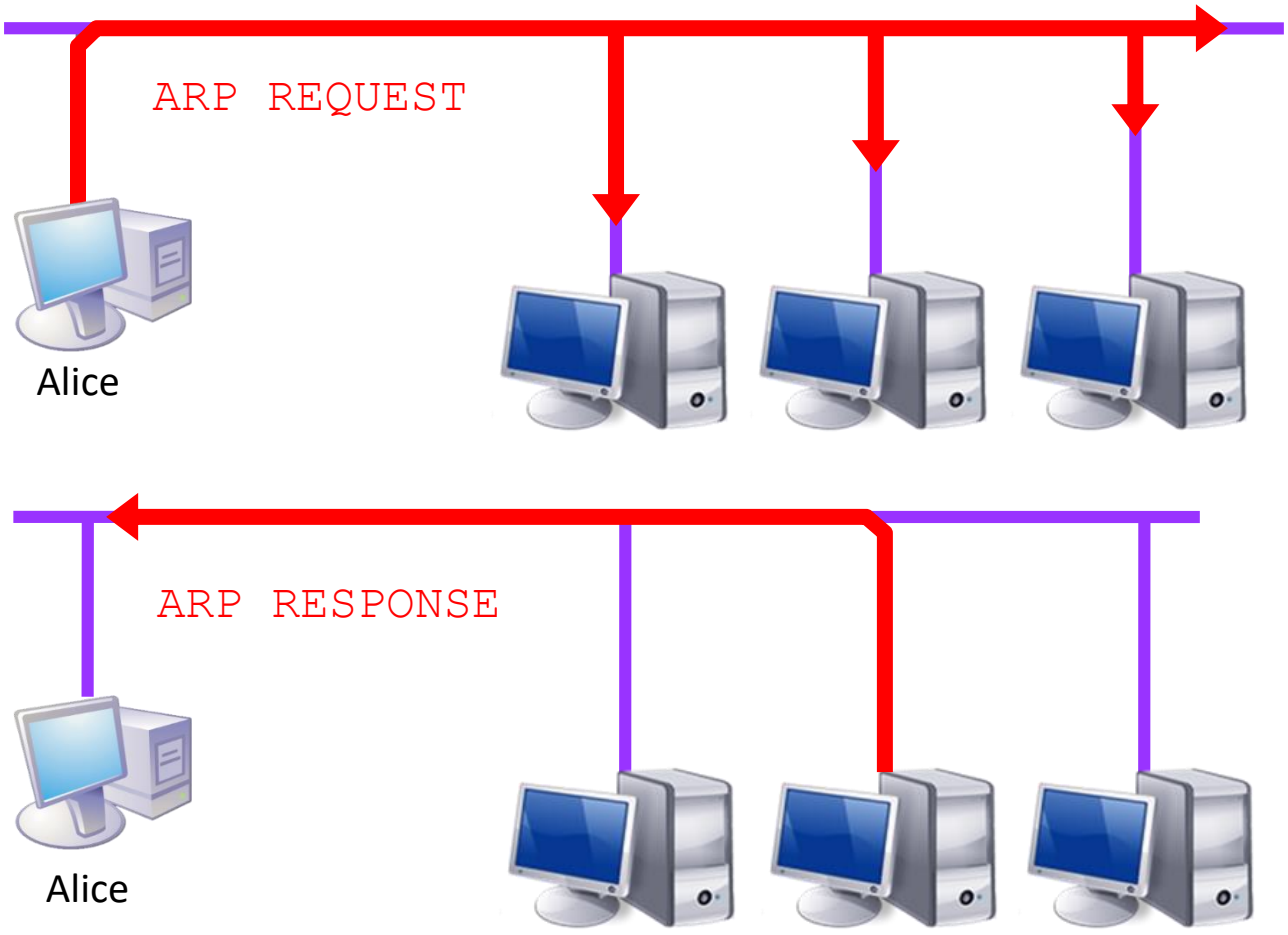
Data Link Layer

MitM attack on STP



ARP

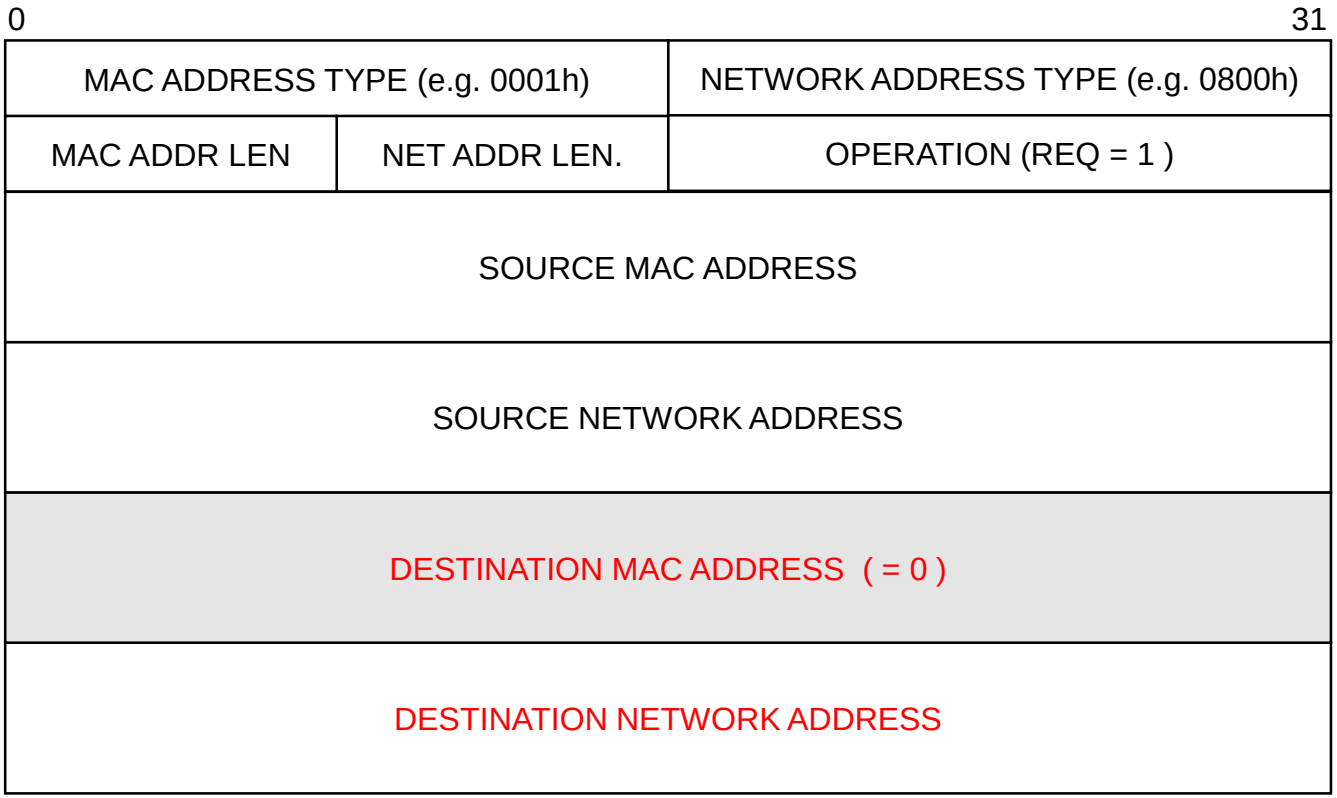
Address Resolution Protocol



© Michał Szychowiak, 2022

ARP

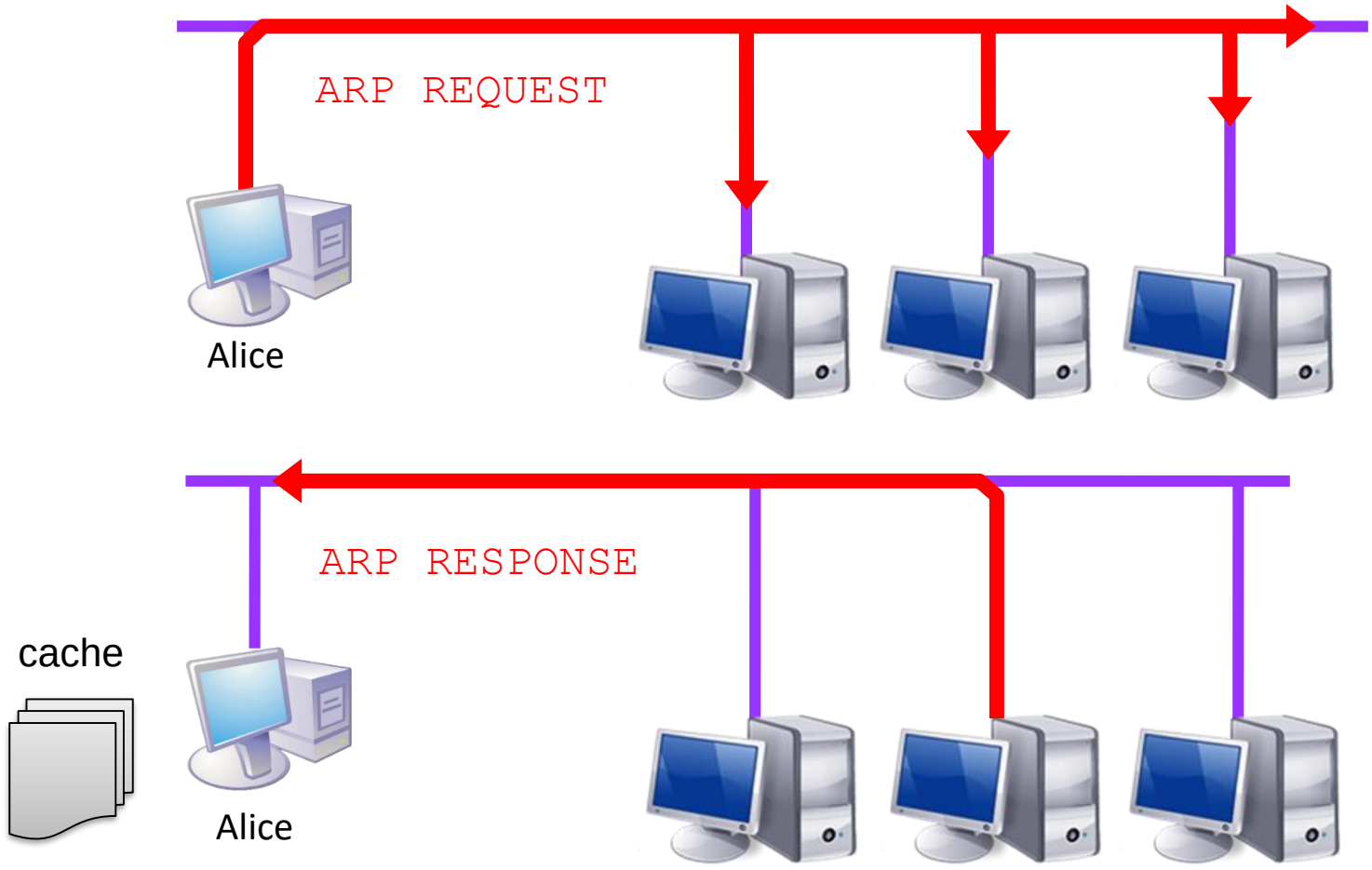
Address Resolution Protocol



© Michał Szychowiak, 2022

ARP

Address Resolution Protocol



© Michał Szychowiak, 2022

ARP

Address Resolution Protocol

- fake responses → ARP spoofing 
- to impersonate network stations and devices
- → ARP cache poisoning 
- static ARP?
- … not really!
- monitoring: *Dynamic Address Inspection* (DAI)
  e.g. Arpwatch, ArpON, Antidote

© Michał Szychowiak, 2022

Network Layer

Internet Protocol (IP)

- connectionless
- no delivery guarantee
- no packet order guarantee
- no packet duplication control
- integrity protection (really?)

- IPv4 vs. IPv6: > 30% of Internet traffic is IPv6
  → https://www.worldipv6launch.org/measurements/
  → https://www.google.com/intl/en/ipv6/statistics.html
  → https://w3techs.com/technologies/breakdown/ce-ipv6/ranking

© Michał Szychowiak, 2022

Network Layer

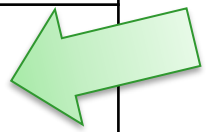
IPv4 Header

Version	IHL	Type of Service	Total Length			
Identification			0	DF	MF	Fragment Offset
Time to Live		Protocol	Header Checksum			
Source Address						
Destination Address						
Options			Padding			

→ IP spoofing

IPv6 Header

Version	Priority	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address (16 B)				
Destination Address (16 B)				

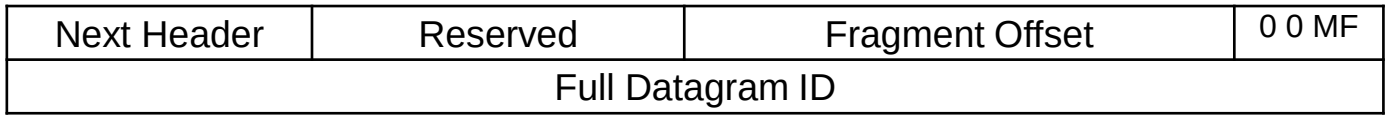


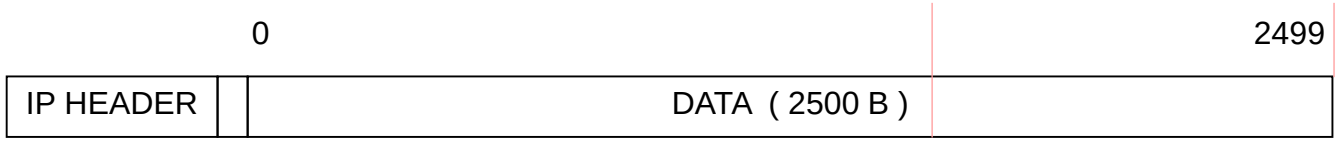
Network Layer

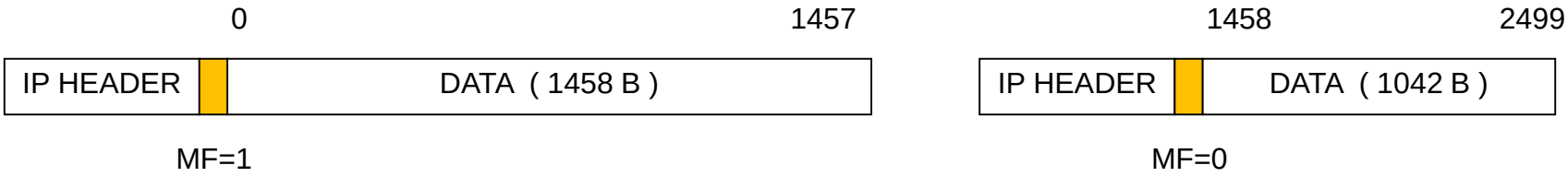
Fragmentation

- MTU (Maximum Transfer Unit)

IP v6 Fragment Header







© Michał Szychowiak, 2022

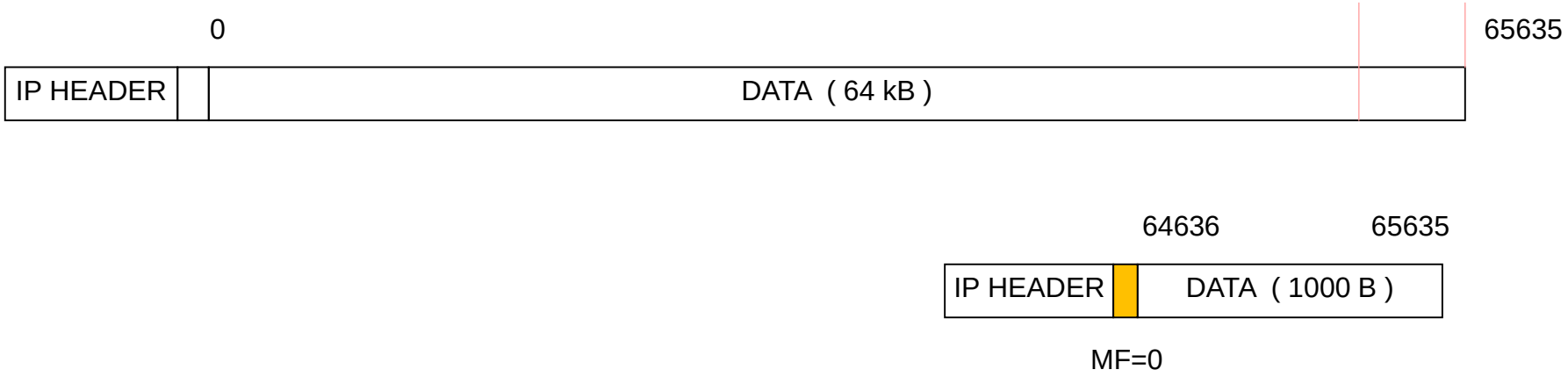
Network Layer

Fragmentation

- MTU (Maximum Transfer Unit)

IP v6 Fragment Header

Next Header	Reserved	Fragment Offset	0 0 MF
Full Datagram ID			

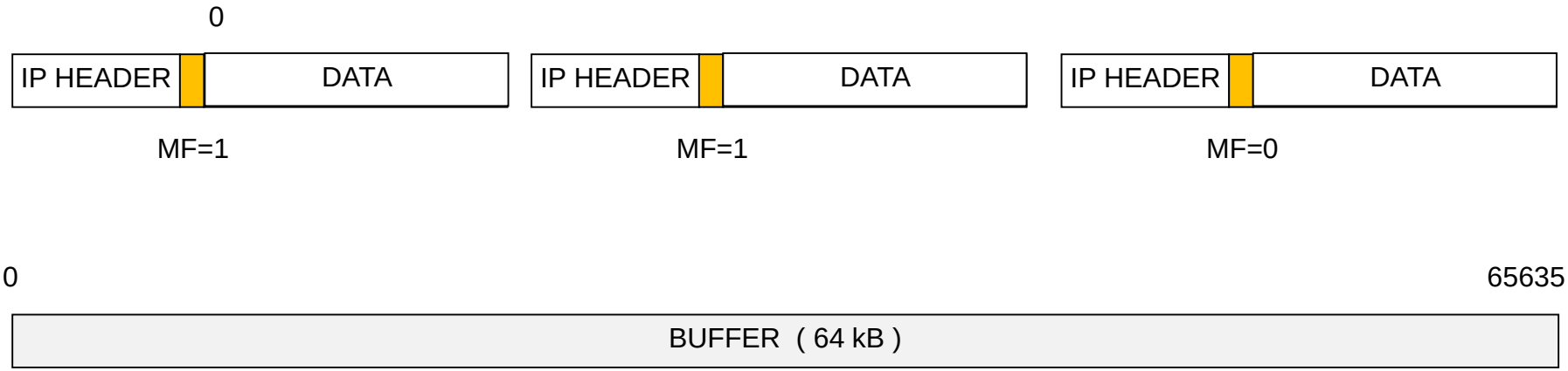


© Michał Szychowiak, 2022

Network Layer

Fragmentation

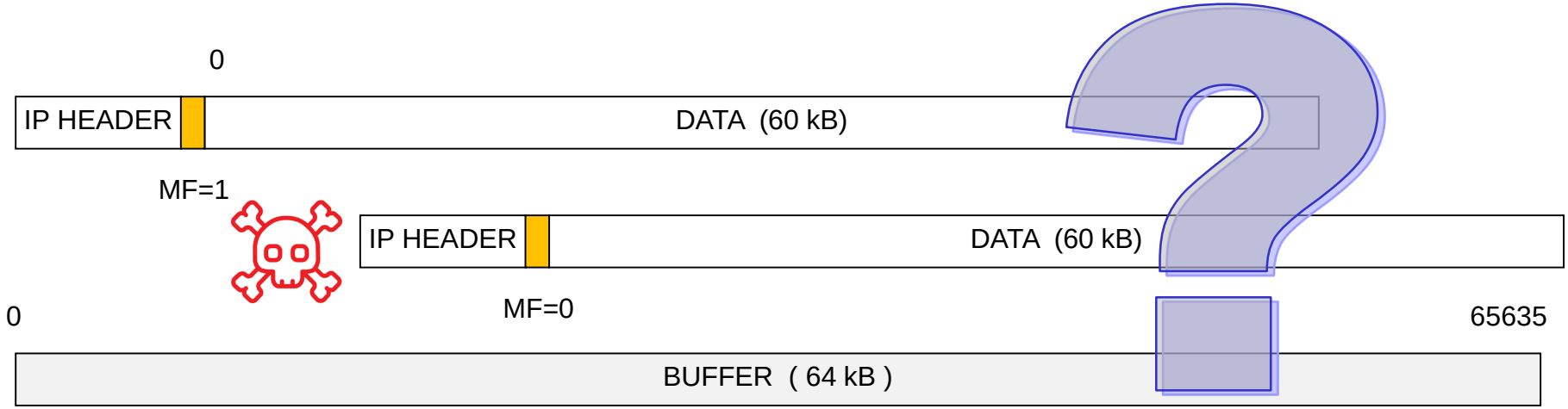
- defragmentation (merge)



Network Layer

Fragmentation

- defragmentation (merge)



© Michał Szychowiak, 2022

Network Layer

Routing

- inbound throughput vs. internal throughput → flooding
- dynamic routing → fake routing updates

- current solutions trend:
  - Resource Public Key Infrastructure (RPKI) for BGP
  - to certificate address block, called Route Origin Authorization (ROA)

© Michał Szychowiak, 2022

Transport Layer

User Datagram Protocol (UDP)

- stateless protocol = no session
- immense volume of risks:
  - difficult authentication (no session)
  - easy spoofing
  - easy replay attacks
  - DoS
  - …

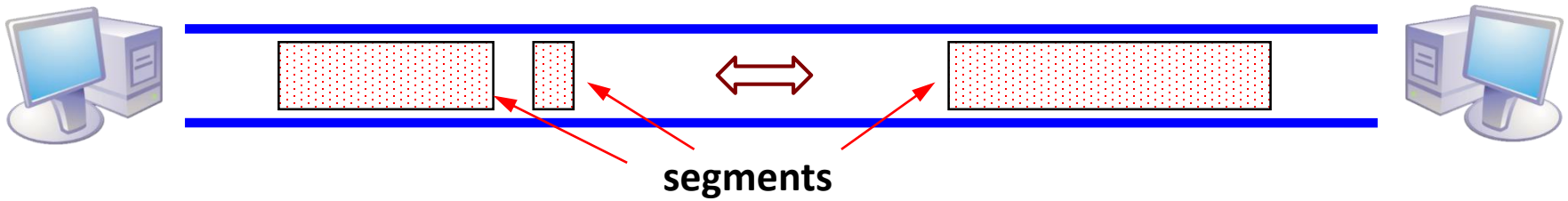
UDP Header (RFC-768)

Source Port	Destination Port
Length	Checksum

© Michał Szychowiak, 2022

Transport Layer

Transmission Control Protocol (TCP)



TCP Header (RFC-793)

Source Port								Destination Port
Sequence Number								
Acknowledgment Number								
Data Offset	ECN	URG	ACK	PSH	RST	SYN	FIN	Window
Checksum								Urgent Pointer
Options								Padding

© Michał Szychowiak, 2022

Transport Layer

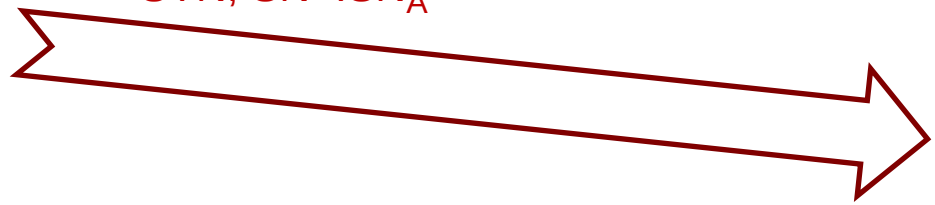
TCP 3-way handshake

active open

passive open

ISN = *Initial Sequence Number*

SYN, SN=ISN_A

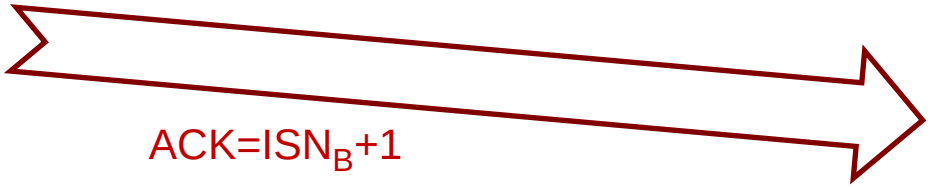


half-opened

SYN, SN=ISN_B, ACK=ISN_A+1

→ flooding

ACK=ISN_B+1



connected

© Michał Szychowiak, 2022

Transport Layer

TCP 3-way handshake

active open

ISN = *Initial Sequence Number*

SYN, SN=ISN_A

passive open

half-opened

- error reporting?

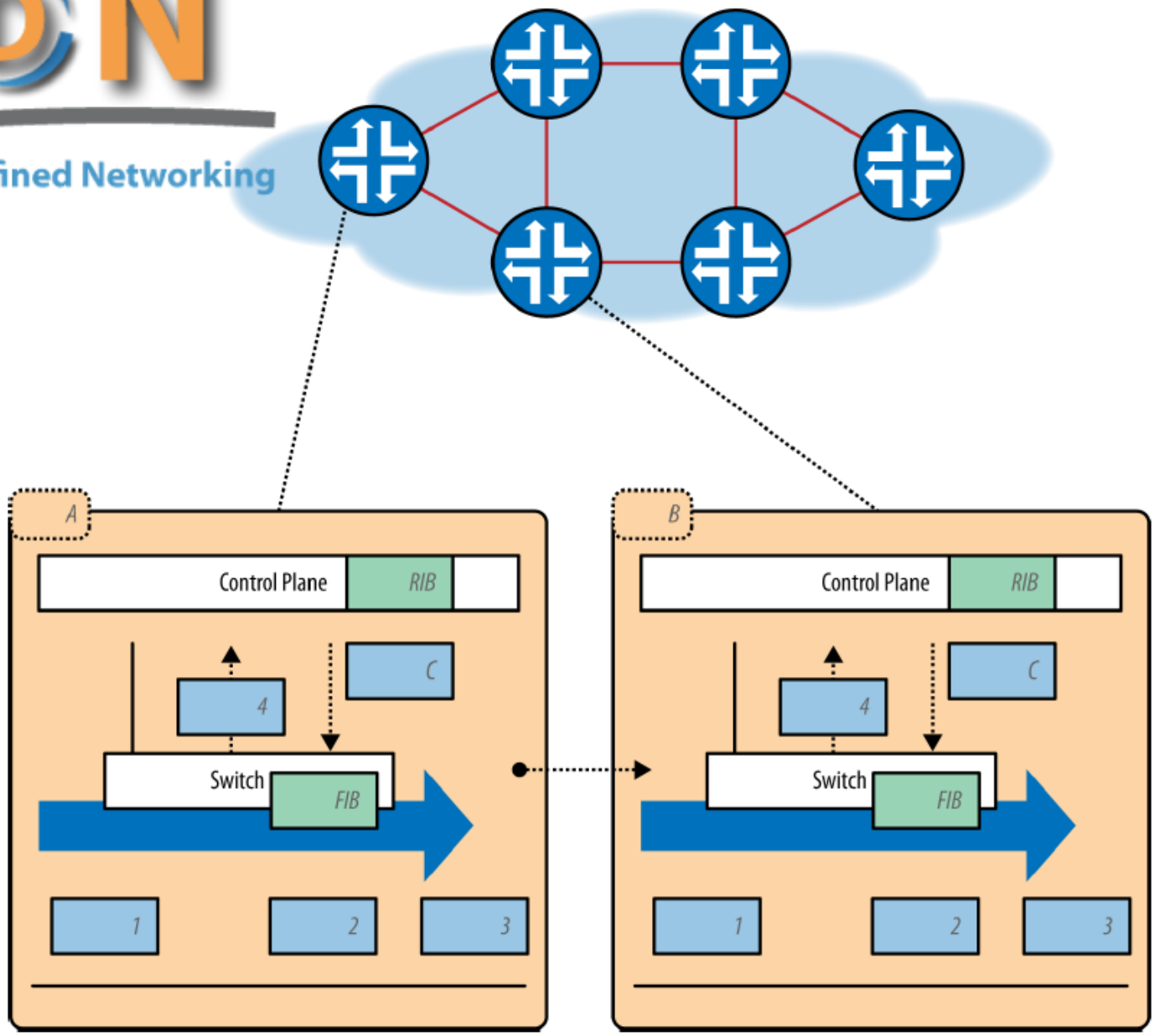
→ SYN flooding

connected

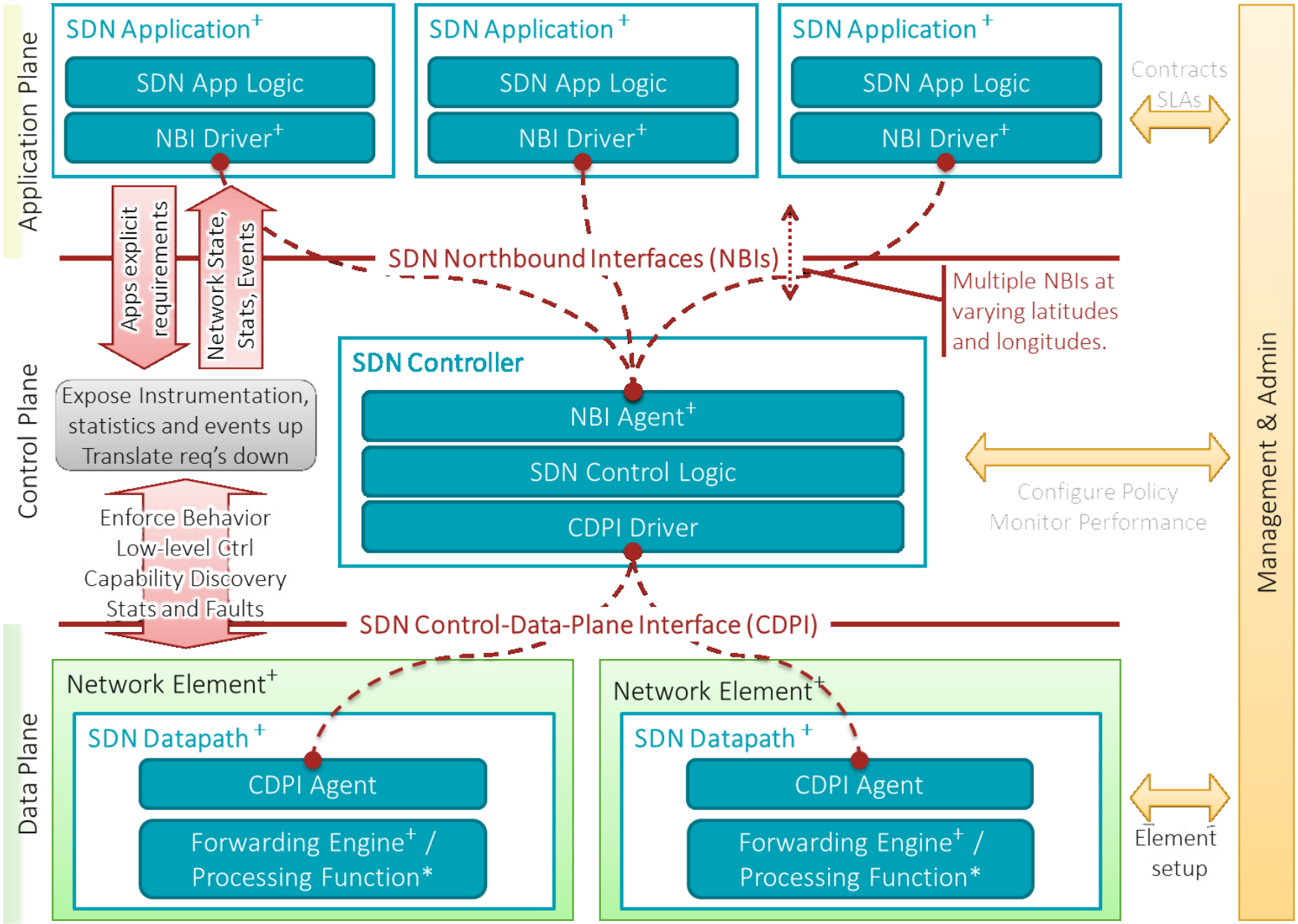
© Michał Szychowiak, 2022

SDN

Software Defined Networking



© Michał Szychowiak, 2022

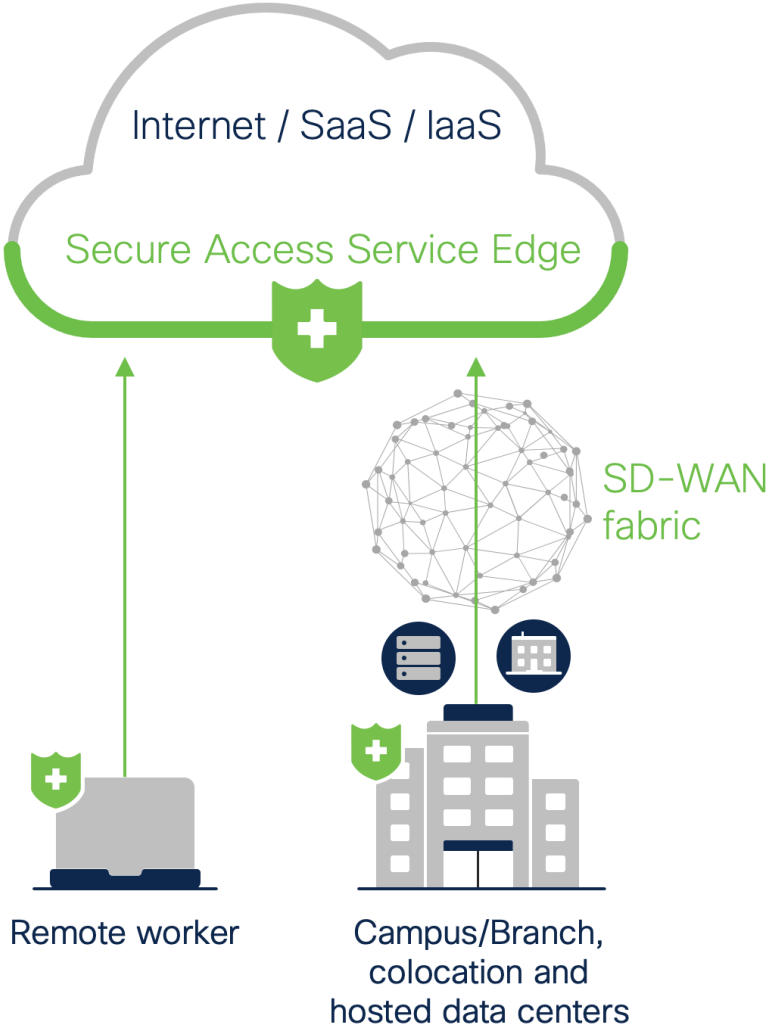


+ indicates one or more instances | * indicates zero or more instances

© Michał Szychowiak, 2022

Zero Trust Networking

➔ https://www.nist.gov/publications/zero-trust-architecture



source: Cisco
https://umbrella.cisco.com

© Michał Szychowiak, 2022

DNS

Domain Name Service

- directory service: RR records (WKS, HINFO, …)
- typically: domain name (or FQDN) ↔ IP address
- typically UDP
- also TCP (zone transfer)

→ domain name spoofing (remember tcp wrapper PARANOID check?)

→ cache poisoning = pharming

DNS

FIREEYE™ Solutions Services Customers

Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

January 10, 2019 | by Muks Hirani, Sarah Jones, Ben Read

DNS IRAN

Introduction

FireEye's Mandiant Incident Response and Intelligence teams have identified a wave of DNS hijacking that has affected dozens of domains belonging to government, telecommunications and internet infrastructure entities across the Middle East and North Africa, Europe and North America. While we do not currently link this activity to any tracked group, initial research suggests the actor or actors responsible have a nexus to Iran. This campaign has targeted victims across the globe on an almost unprecedented scale, with a high degree of success. We have been tracking this activity for several months, mapping and understanding the innovative tactics, techniques and procedures (TTPs)

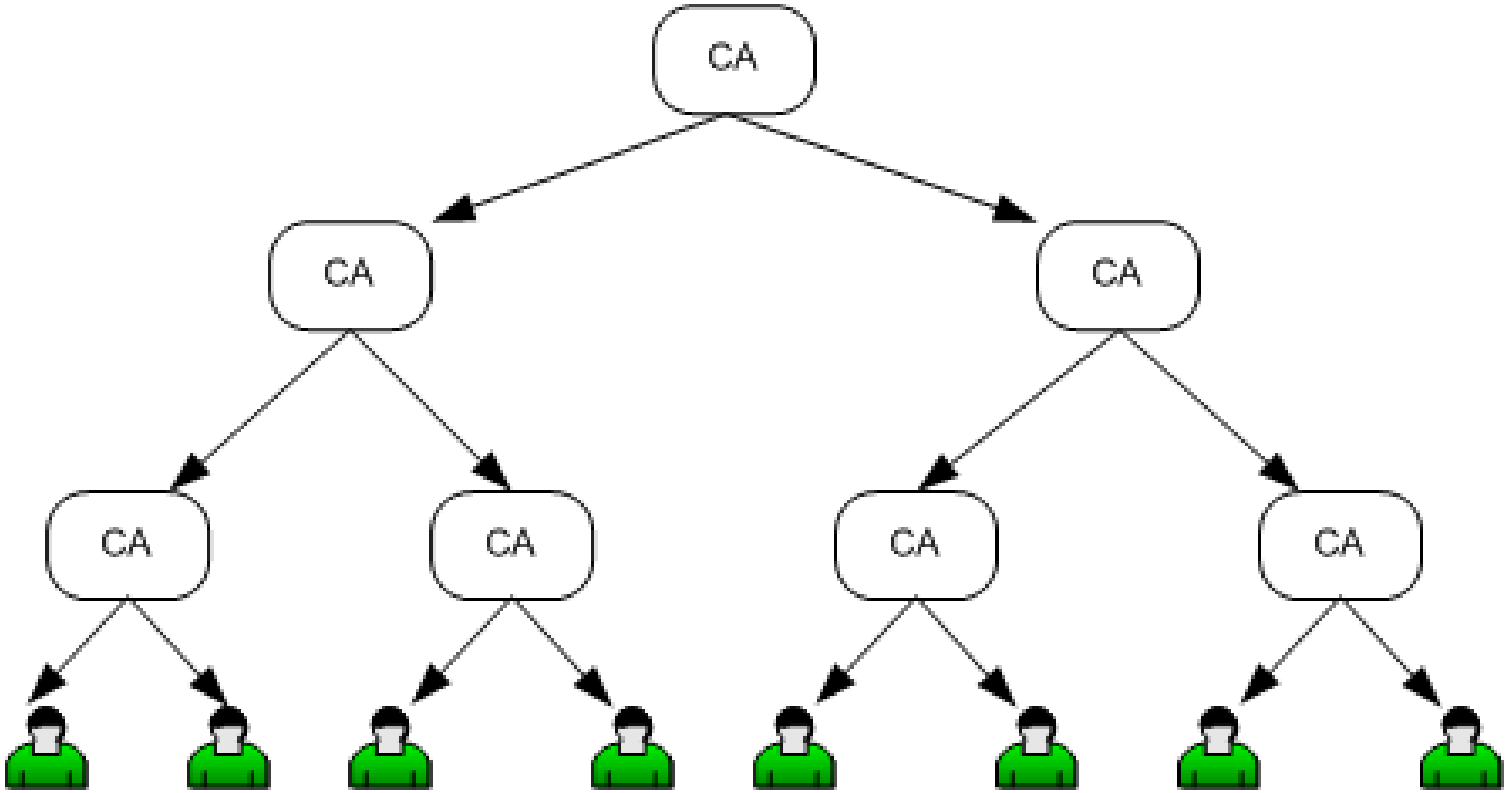
© Michał Szychowiak, 2022

DNSsec

- RFC 2535 (AD 1999) → RFC 6840
- RRSIG records = digital signature of RRset
- DNSkey records = PKI

© Michał Szychowiak, 2022

Public Key Infrastructure



REPLAY

© Michał Szychowiak, 2022

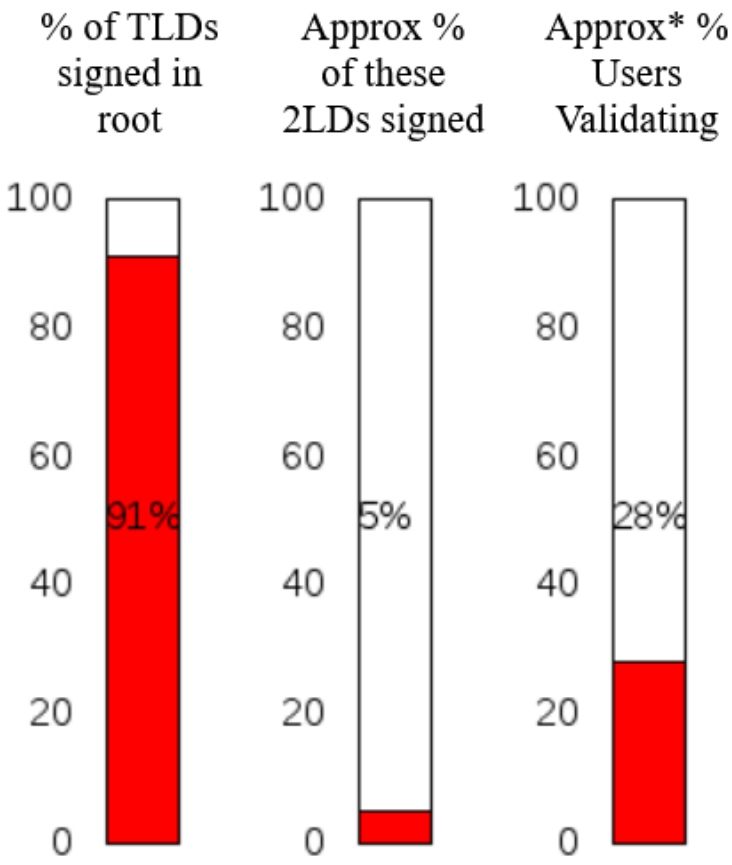
DNSsec

DANE (DNS-based Authentication of Named Entities, RFC 6698)

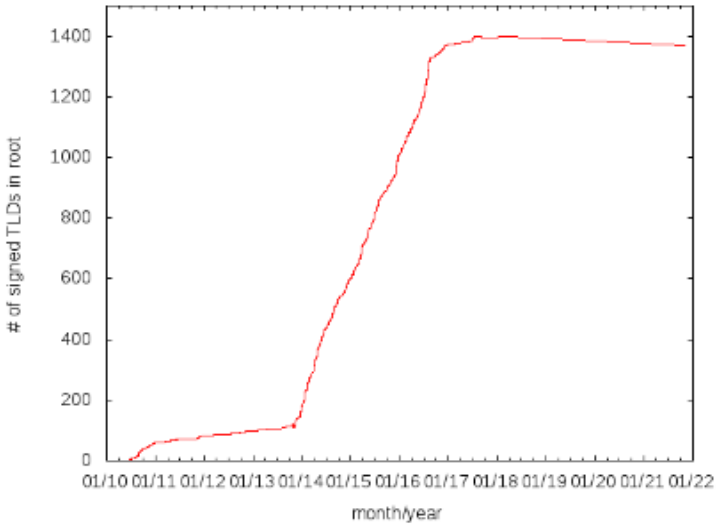
- PKI w/o CAs
- X.509 certificates within DNSsec

© Michał Szychowiak, 2022

DNSsec



Trend



https://rick.eng.br/dnssecstat/

© Michał Szychowiak, 2022

DNS

DNS over TLS (DoT) RFC 7858

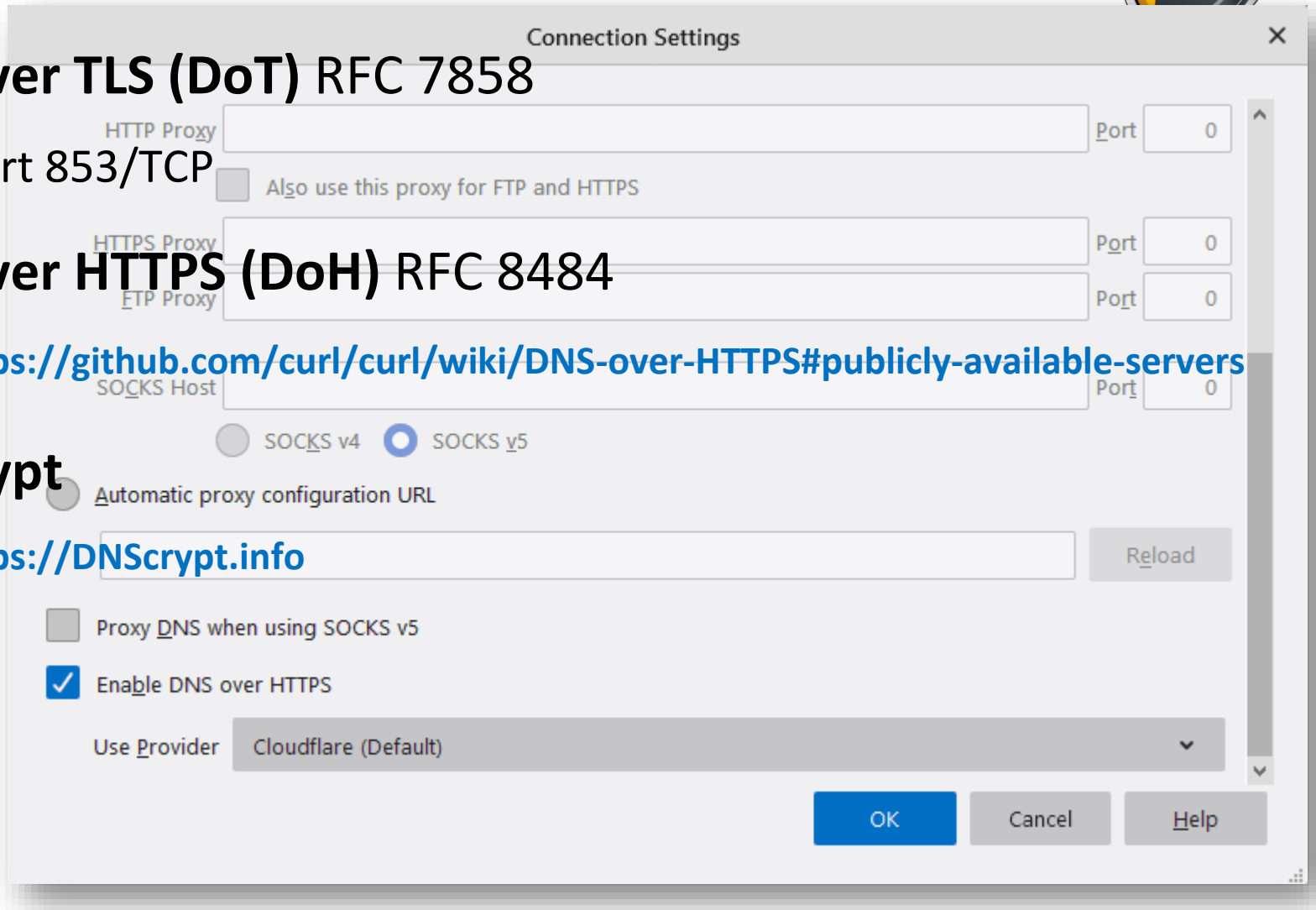
- port 853/TCP

DNS over HTTPS (DoH) RFC 8484

→ https://github.com/curl/curl/wiki/DNS-over-HTTPS#publicly-available-servers

DNScrypt

→ https://DNScrypt.info



© Michał Szychowiak, 2022

NETWORK ATTACKS

© Michał Szychowiak, 2022

Network-based attacks

Recon

- sniffing (packet snooping)
- network scanning, service enumeration

```
netcat  -v  -w 1  10.0.0.1  -z 1-65535
```

```
nmap  -PT 10.0.0.1-255
```

© Michał Szychowiak, 2022

Network-based attacks

Recon

- sniffing (packet snooping)
- network scanning, service enumeration

```
nmap  -T4  -v  -oA myshares  --script smb-enum-shares
--script-args smbuser=jbond,smbpass=Walther9mm
-p445 192.168.0.1-255 && cat myshares.nmap |
grep '|\|192' | awk '/[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+/
{ line=$0 } /\|/ { $0 = line $0}1' |
grep \| | grep -v -E '(smb-enum-shares|access:
<none>|ADMIN\$|C\$|IPC\$|access: READ)' |
awk '{ sub(/Nmap scan report for /, ""); print }' >>
sharelist.txt
```

© Michał Szychowiak, 2022

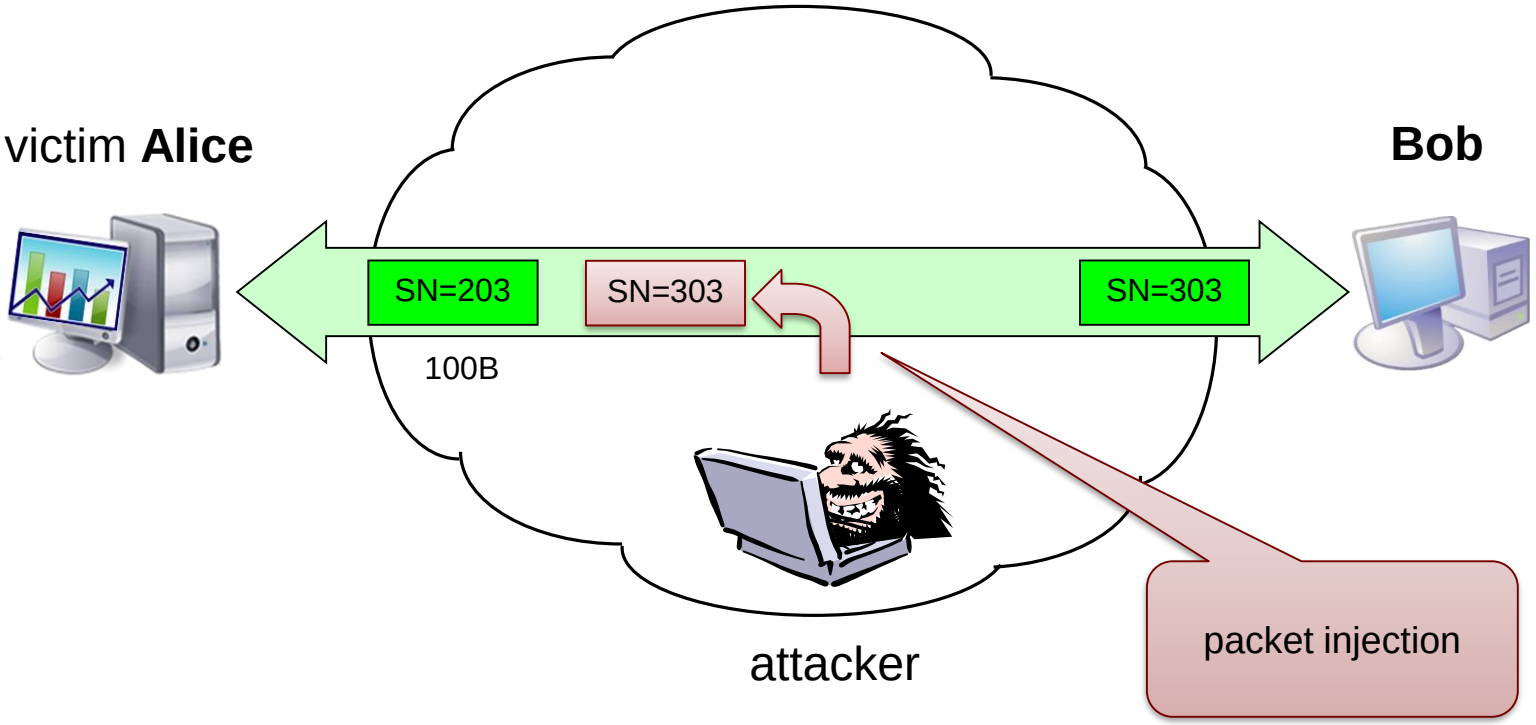
Network-based attacks

Spoofing

- IP spoofing
- session hijacking
- TCP spoofing
- UDP spoofing
- . . .

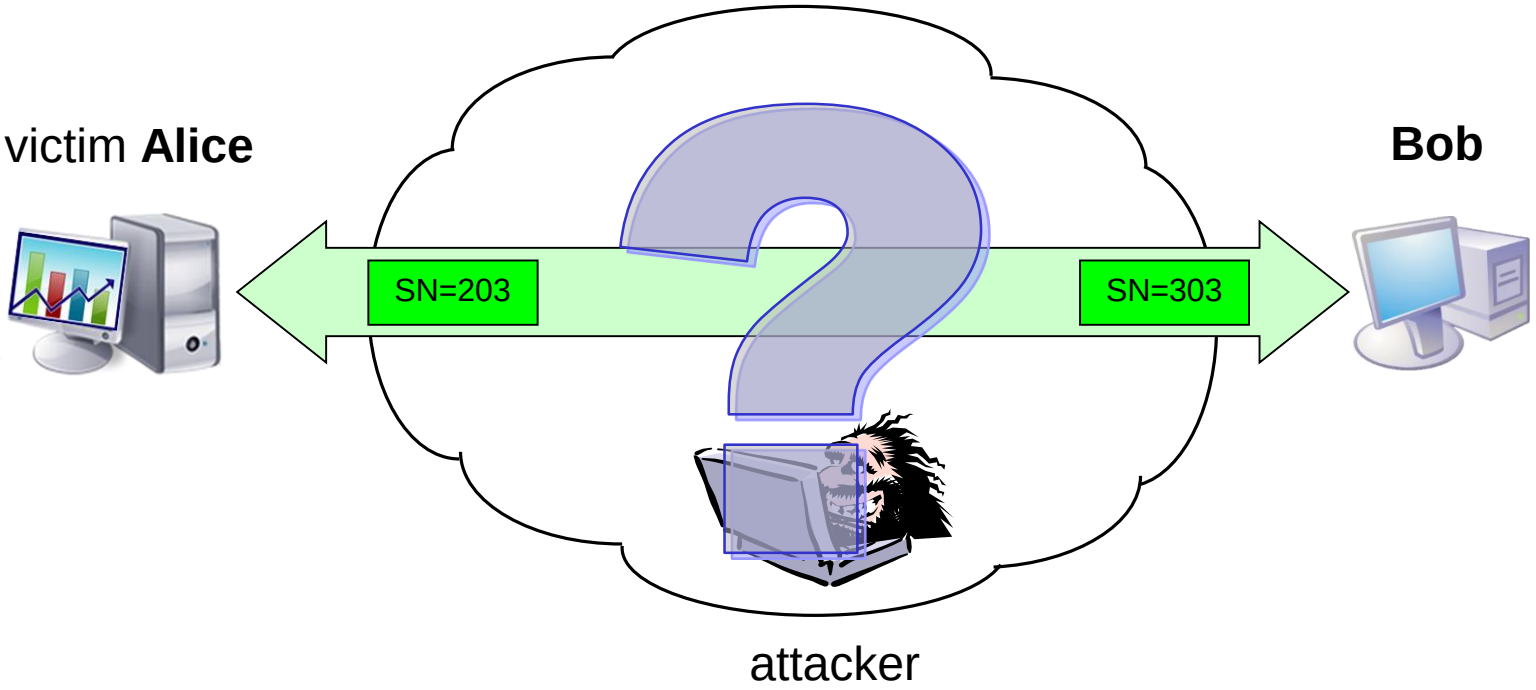
© Michał Szychowiak, 2022

Session hijacking



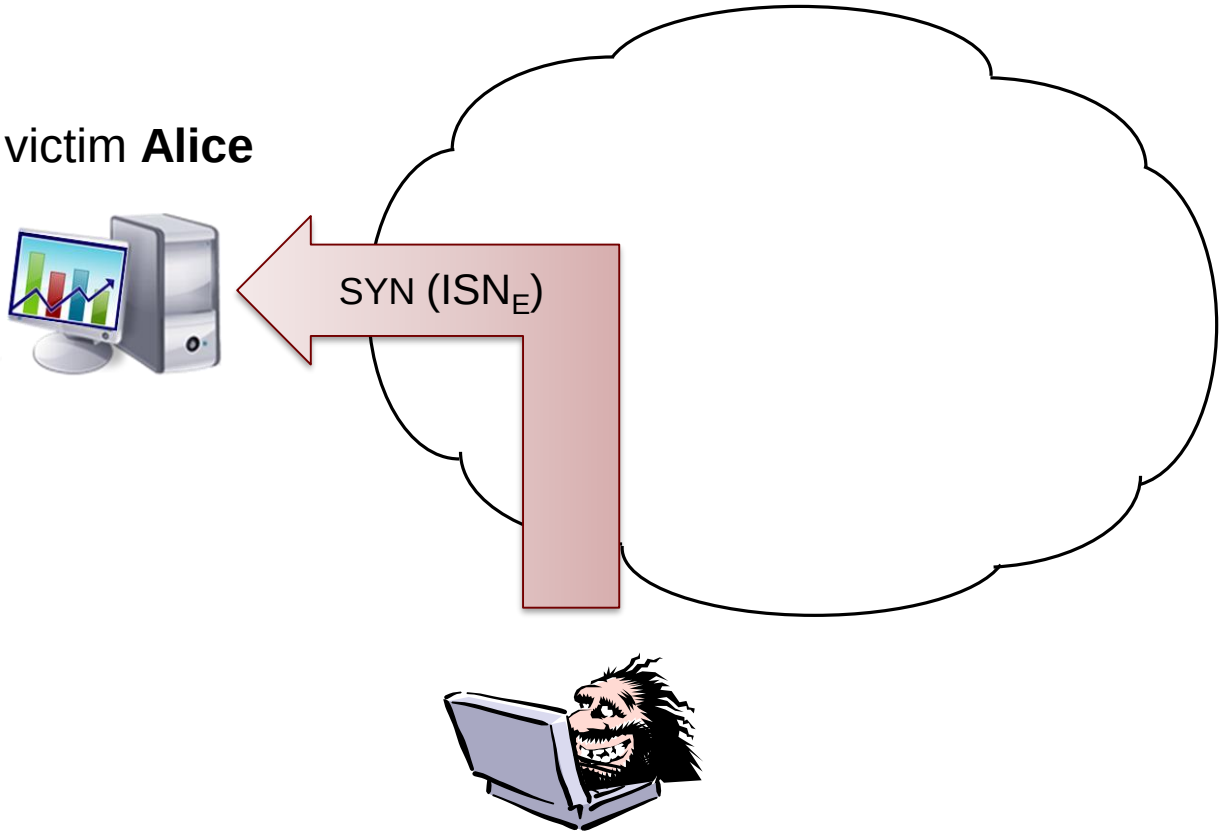
© Michał Szychowiak, 2022

TCP spoofing



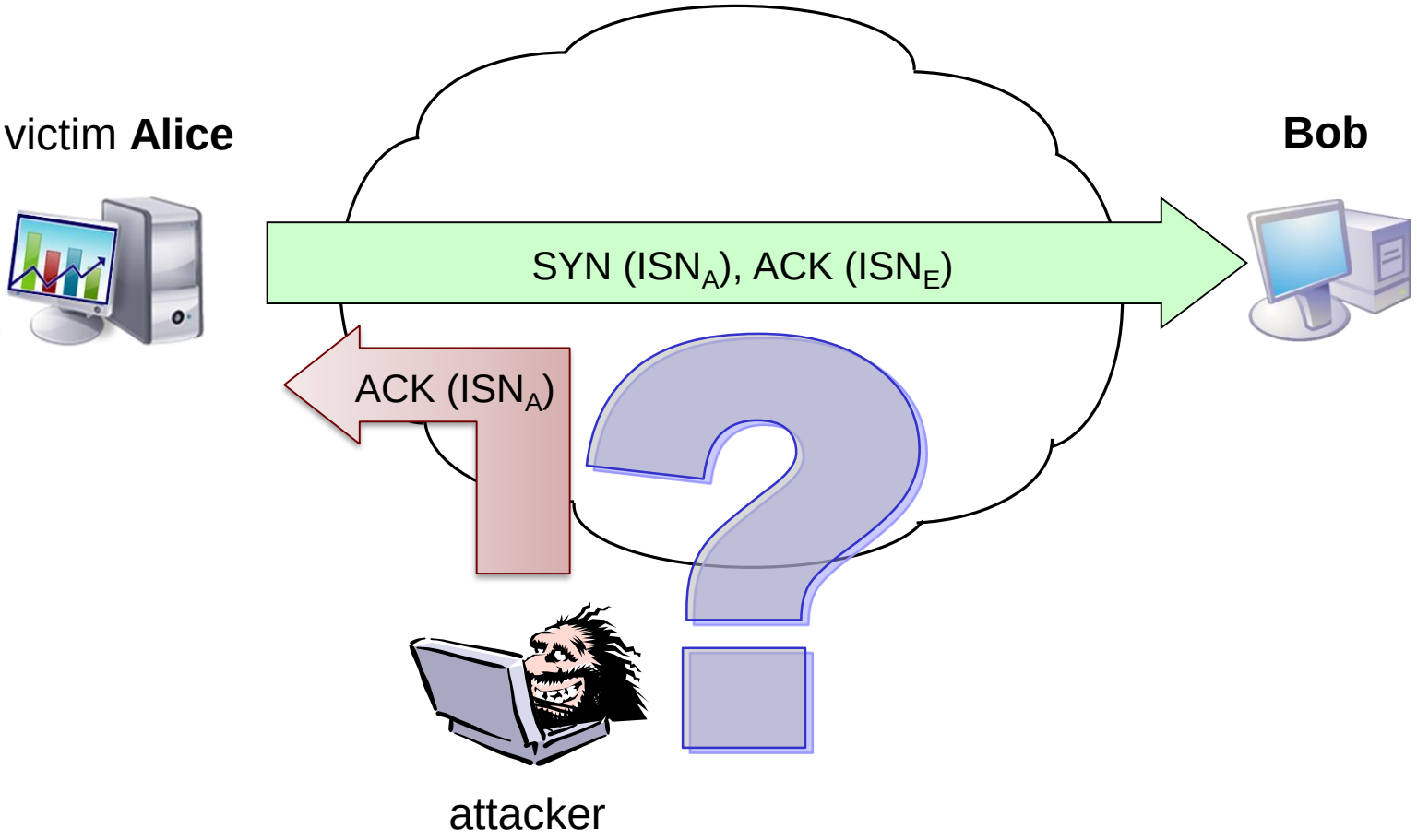
© Michał Szychowiak, 2022

TCP spoofing



© Michał Szychowiak, 2022

TCP spoofing



© Michał Szychowiak, 2022

TCP spoofing

ISN pseudo-random generator

- 32b = $4 \cdot 10^9$
- ISN prediction?

TCP spoofing

ISN pseudo-random generator

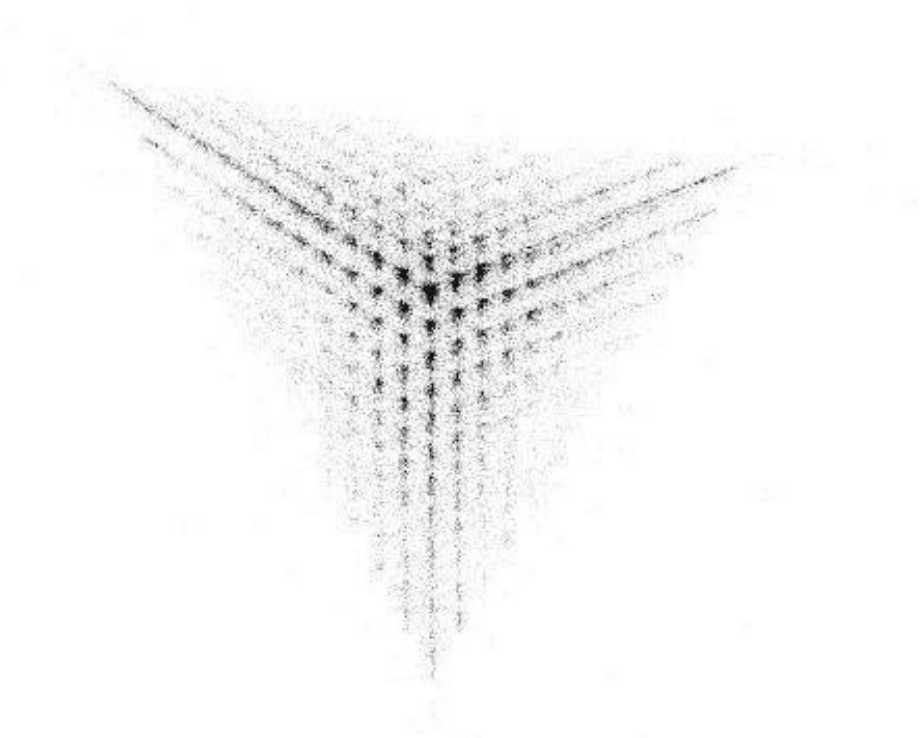
- 32b = $4 \cdot 10^9$
- successful attack requires sending ca. 80 GB before timeout!
- not really feasible
- unless …

© Michał Szychowiak, 2022

TCP spoofing

ISN pseudo-random generator

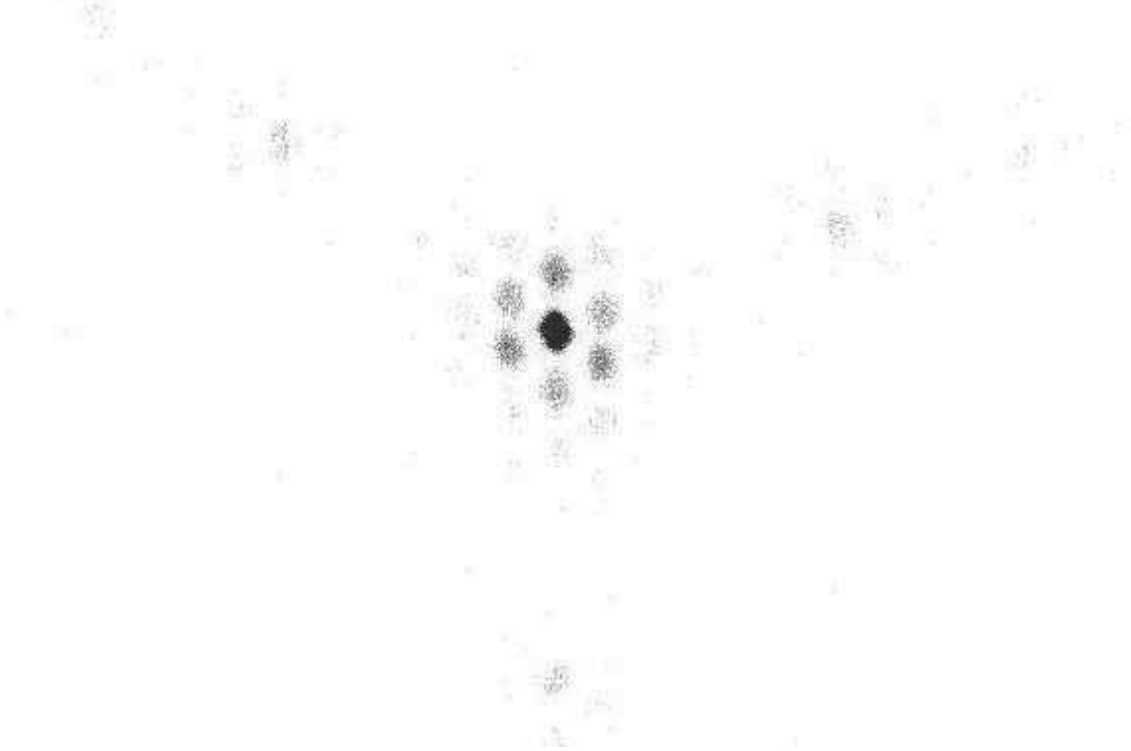
Cisco IOS 12.0



TCP spoofing

ISN pseudo-random generator

IRIX 6.5.15

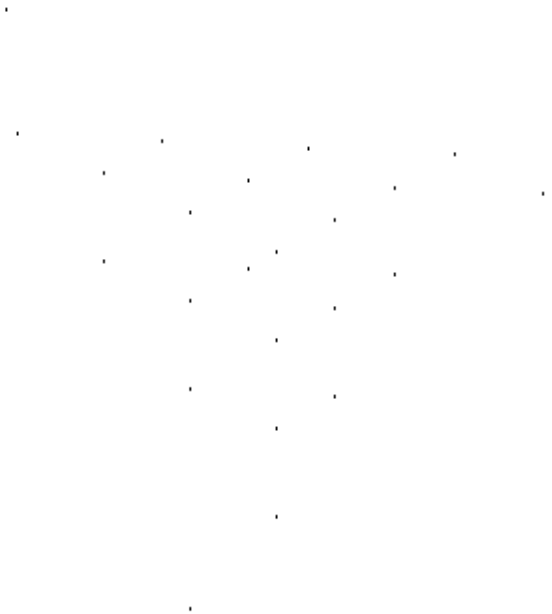


© Michał Szychowiak, 2022

TCP spoofing

ISN pseudo-random generator

MacOS 9



© Michał Szychowiak, 2022

TCP spoofing

ISN pseudo-random generator

NextSTEP

© Michał Szychowiak, 2022

Network-based attacks

Poisoning

- ARP poisoning
- DNS cache poisoning (pharming)
- DHCP redirection = DHCP lease starvation + rouge DHCP server
- ICMP redirection
- various SNMP attacks
- . . .

© Michał Szychowiak, 2022

Network-based attacks

Denial of Service (DoS)

- flooding (SYN flood, ICMP flood, UDP storms)
- TCP RST, ICMP destination unreachable
- Ping of Death, Teardrop
- Land Attack
- Smurf, Fraggle
- LDoS (Low rate DoS)
- . . .

OSI L7:

- e-mail bombing
- HTTP floods (GET, POST, HEAD)
- XML-RPC
- . . .

© Michał Szychowiak, 2022

Denial of Service (DoS)

SYN flood

TCP Reset

Ping of Death

Land attack

© Michał Szychowiak, 2022

HOMEWORK

=

Half Of My Energy Wasted On Random Knowledge

→ **Slow Read attack**

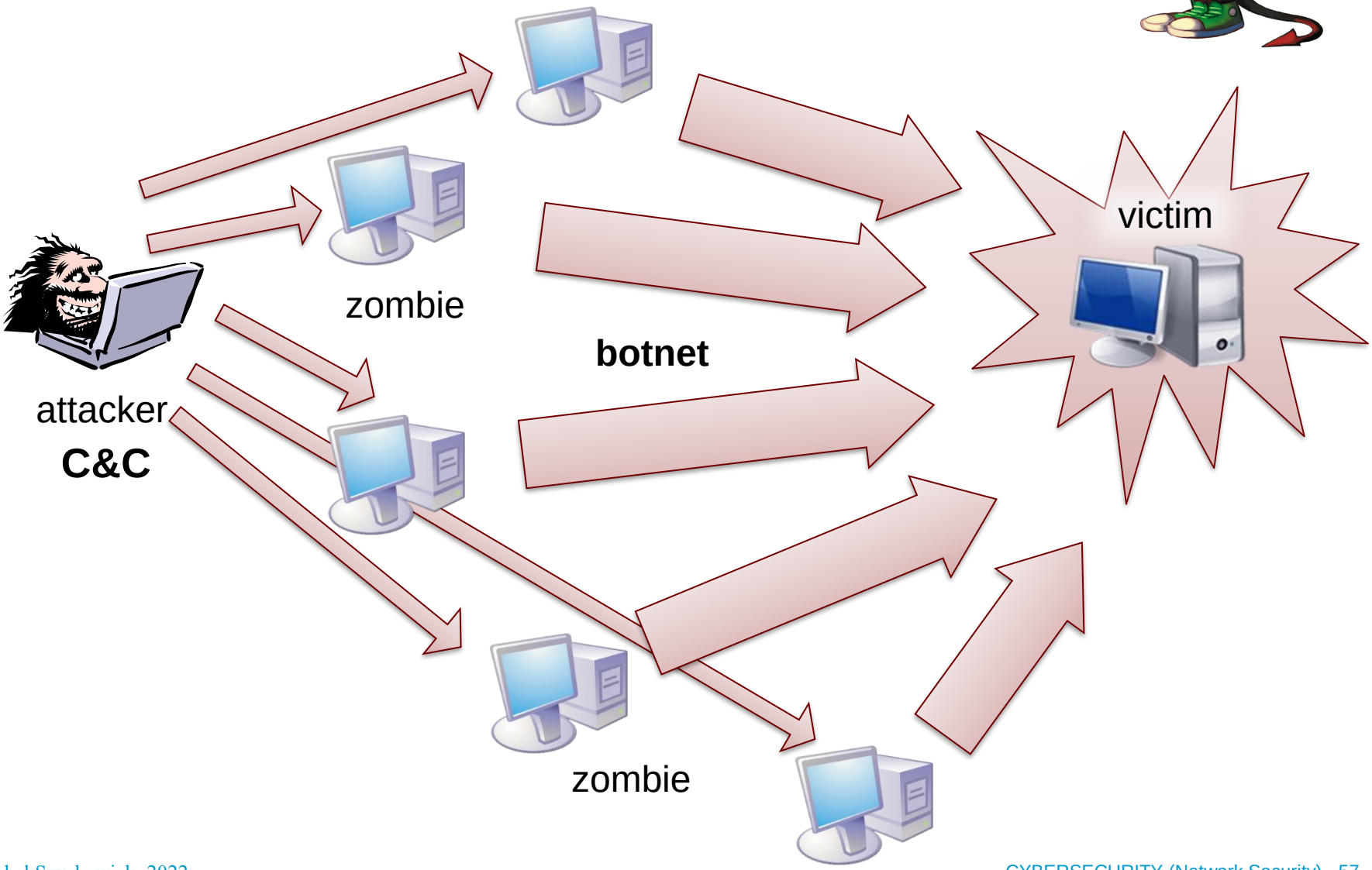
© Michał Szychowiak, 2022

Denial of Service (DoS)

attacker

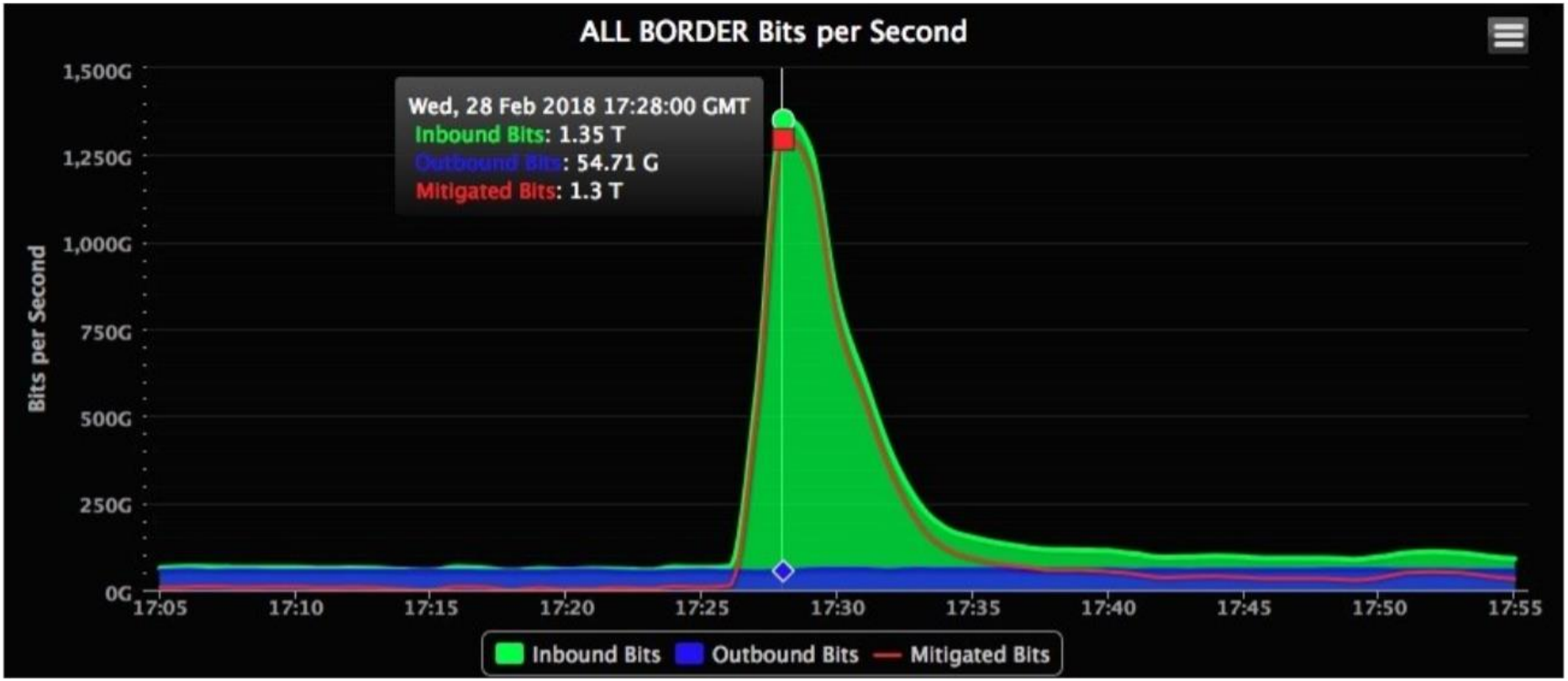
victim

Distributed DoS (DDoS)



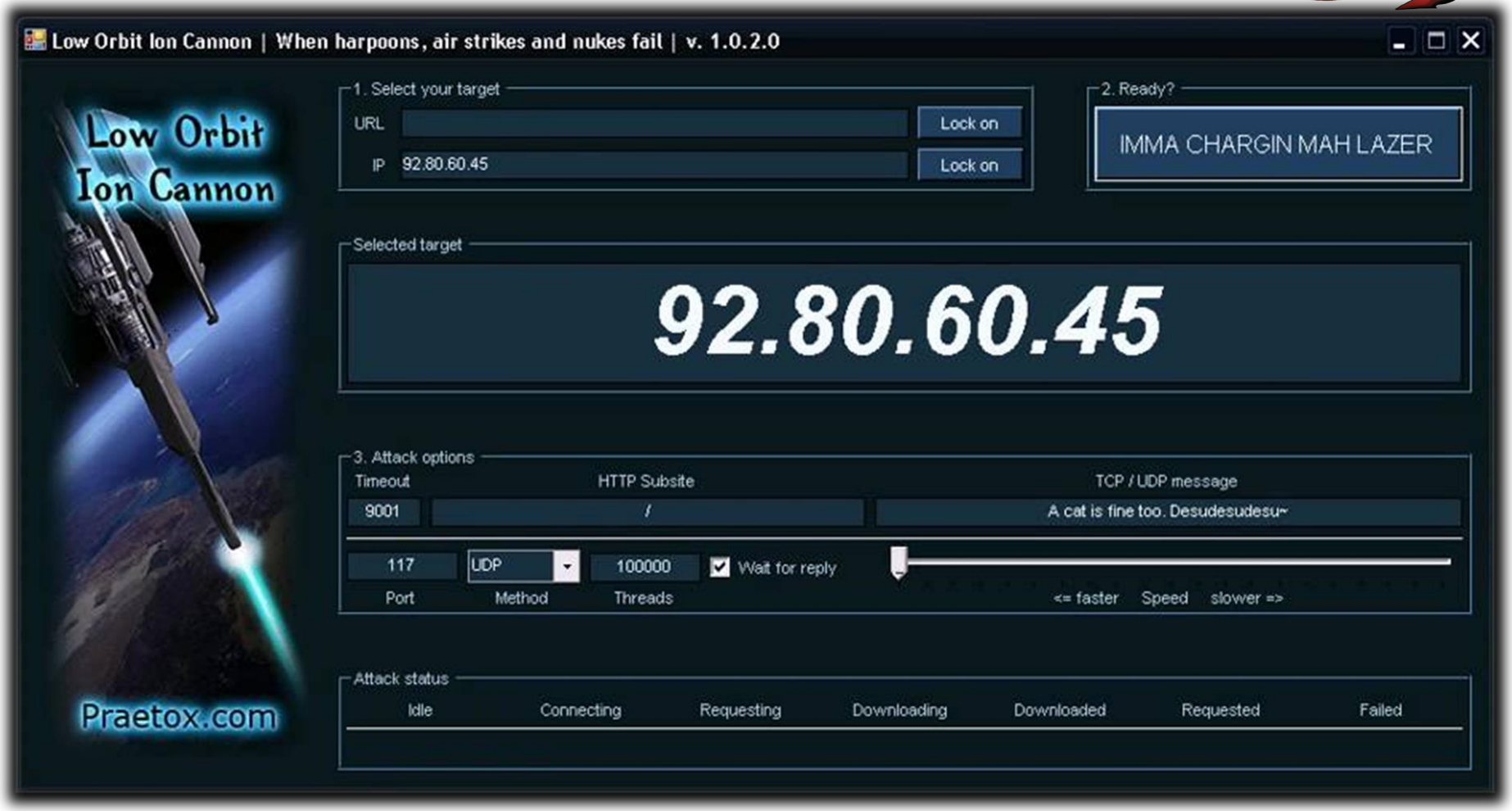
© Michał Szychowiak, 2022

Distributed DoS (DDoS)



© Michał Szychowiak, 2022

Botnets



© Michał Szychowiak, 2022

Botnets

Blackhole β | СТАТИСТИКА | ПОТОКИ | ФАЙЛЫ | БЕЗОПАСНОСТЬ | НАСТРОЙКИ | Выйти

Начало: Конец: Применить Автообновление: 5 сек.

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 хиты **11506** хосты **1187** загрузки

10.32% пробив

ЗА СЕГОДНЯ

3013 хиты **2760** хосты **300** загрузки

11.55% пробив

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48
Windows 7	5059	4490	478	10.66
Windows Vista	3173	2752	264	9.61
Mac OS	978	900	18	2.00

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00
Другое	327	222	41	18.55

Создать виджет

Amplification Attacks

Distributed Reflection DoS (DRDoS)

- Smurf attack: directed broadcast ping
- Fraggle attack: similar, only with UDP echo service
- DNS open resolver:
  - ANY records lookup
  - RFC 1035 limits DNS responses (UDP) to 512 B
  - but RFC 2671 (EDNS) allow more than 4000 B
  - how about DNSsec?

© Michał Szychowiak, 2022

Amplification Attacks

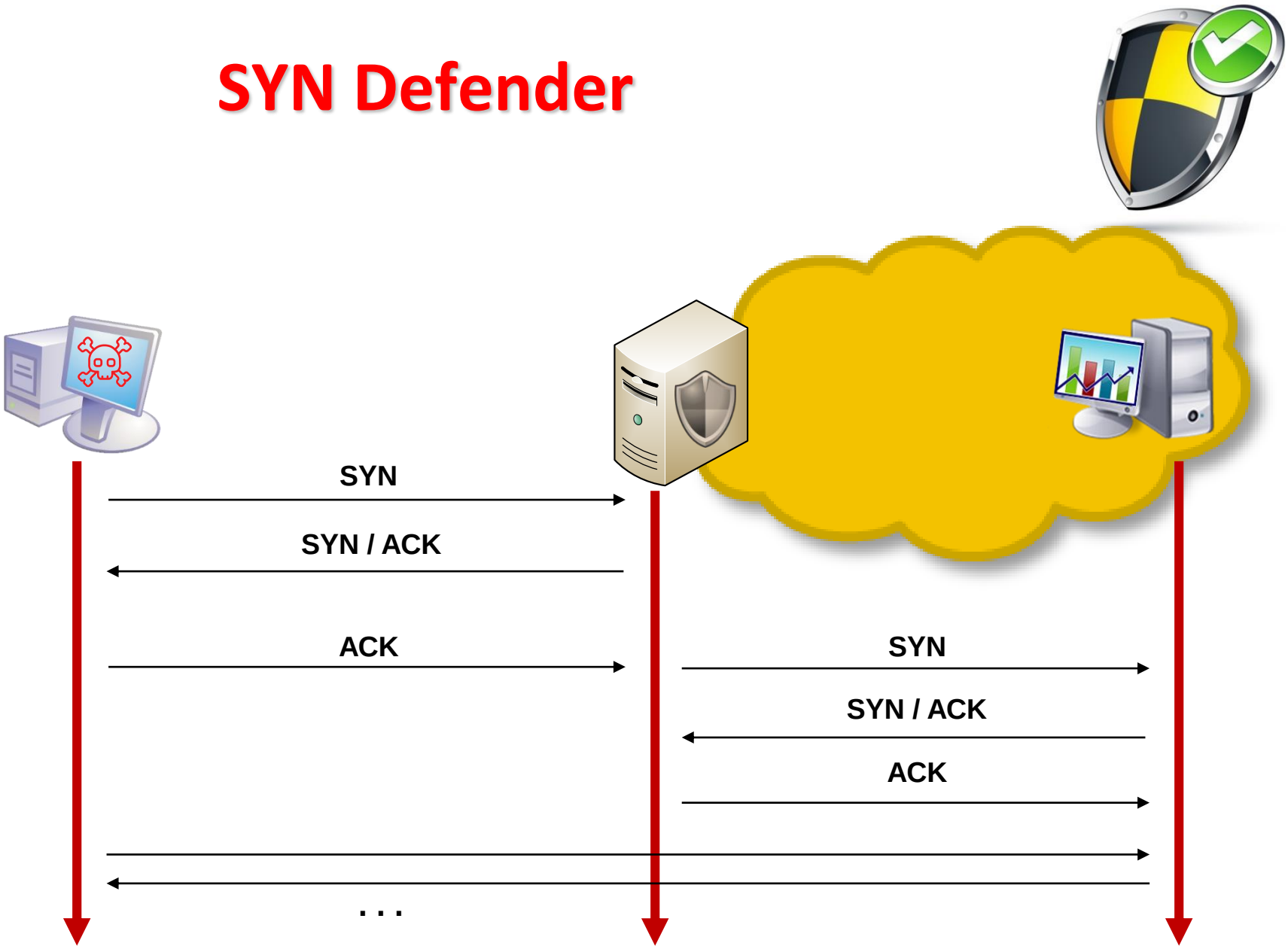
Distributed Reflection DoS (DRDoS)

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [1]
NTP	556.9	see: TA14-013A [2]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

© Michał Szychowiak, 2022

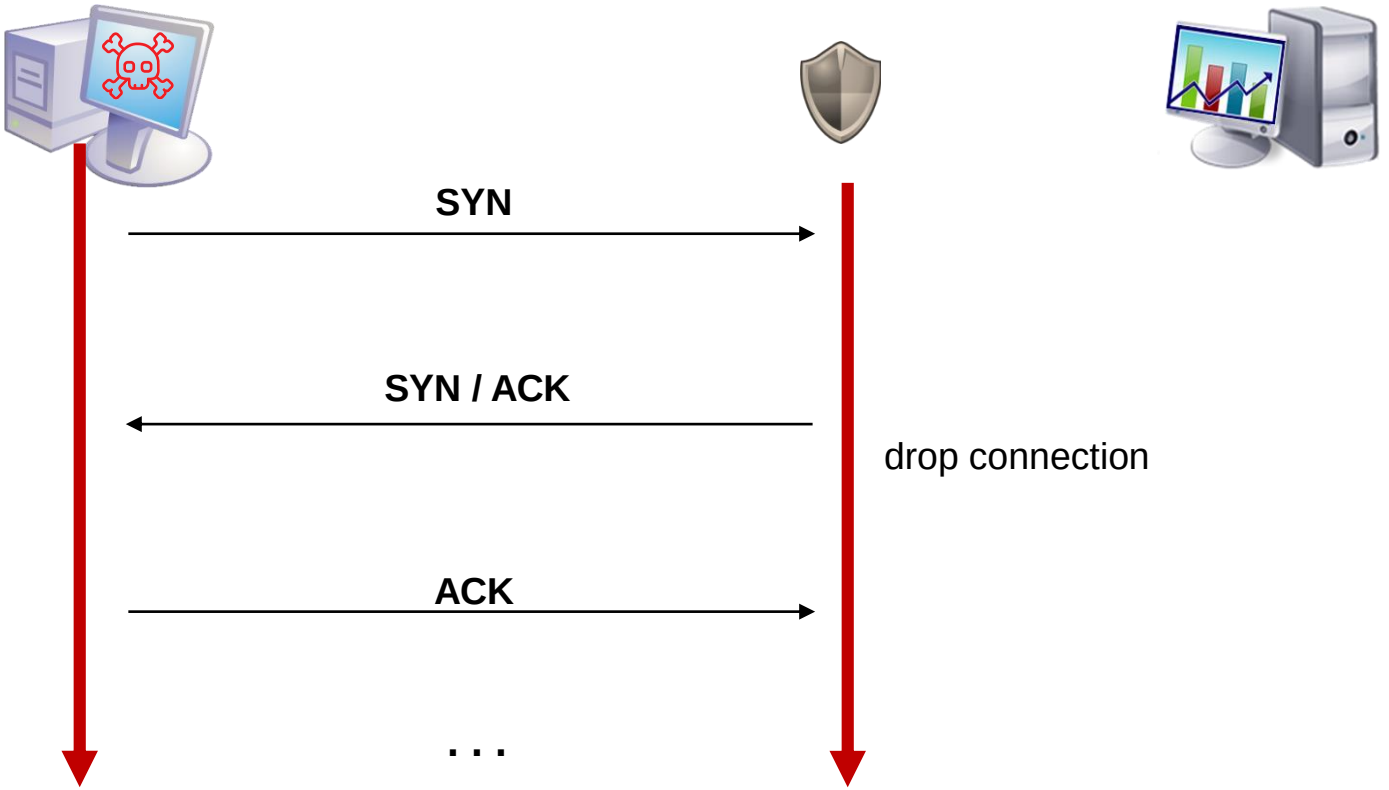
DEFENSE

SYN Defender



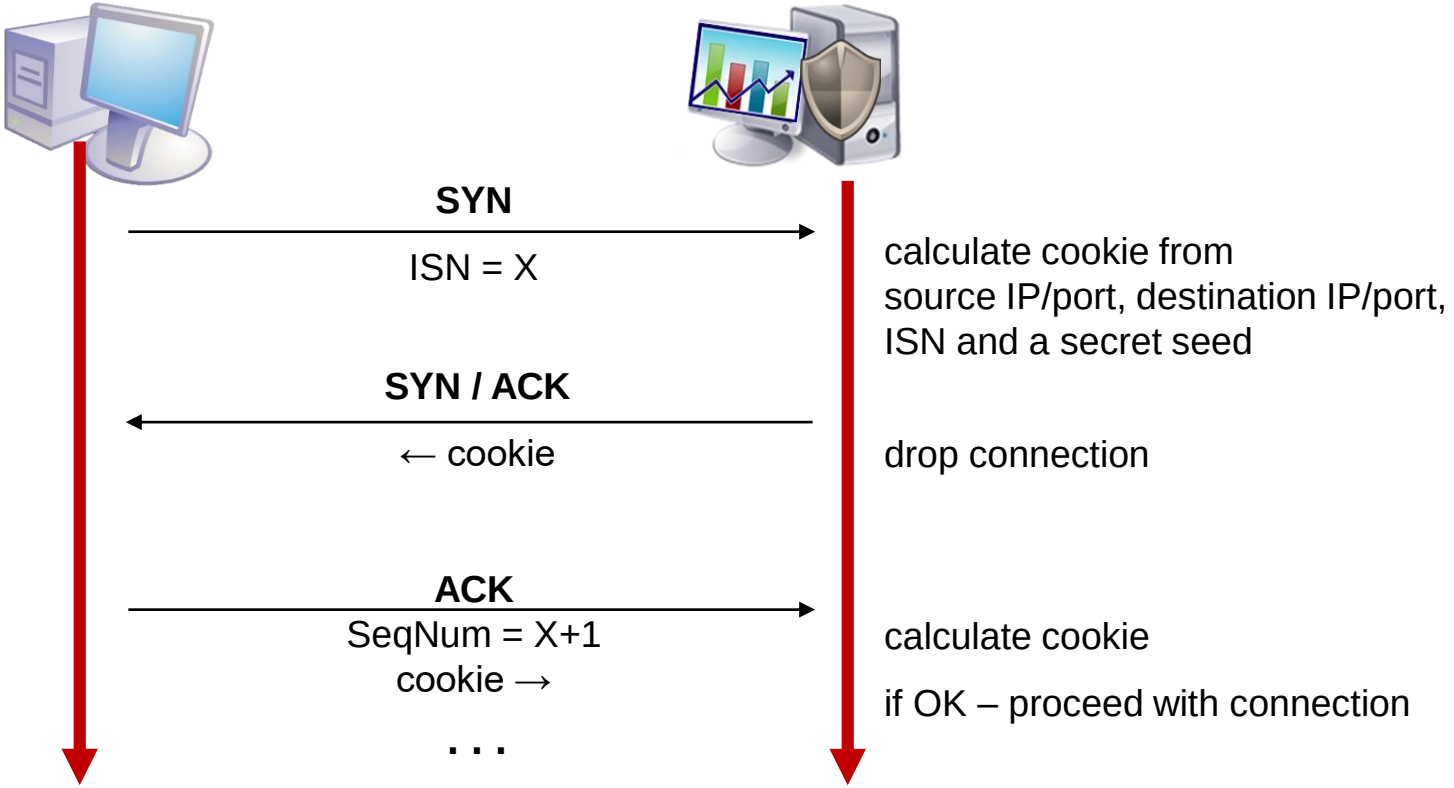
© Michał Szychowiak, 2022

SYN cookies



© Michał Szychowiak, 2022

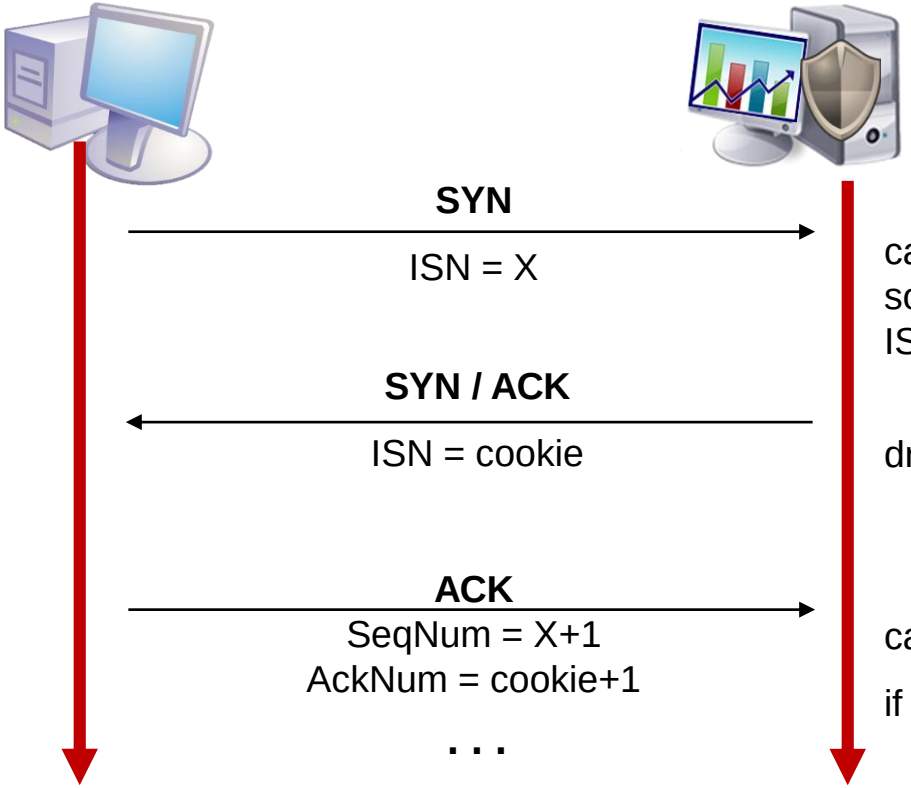
SYN cookies



© Michał Szychowiak, 2022

SYN cookies

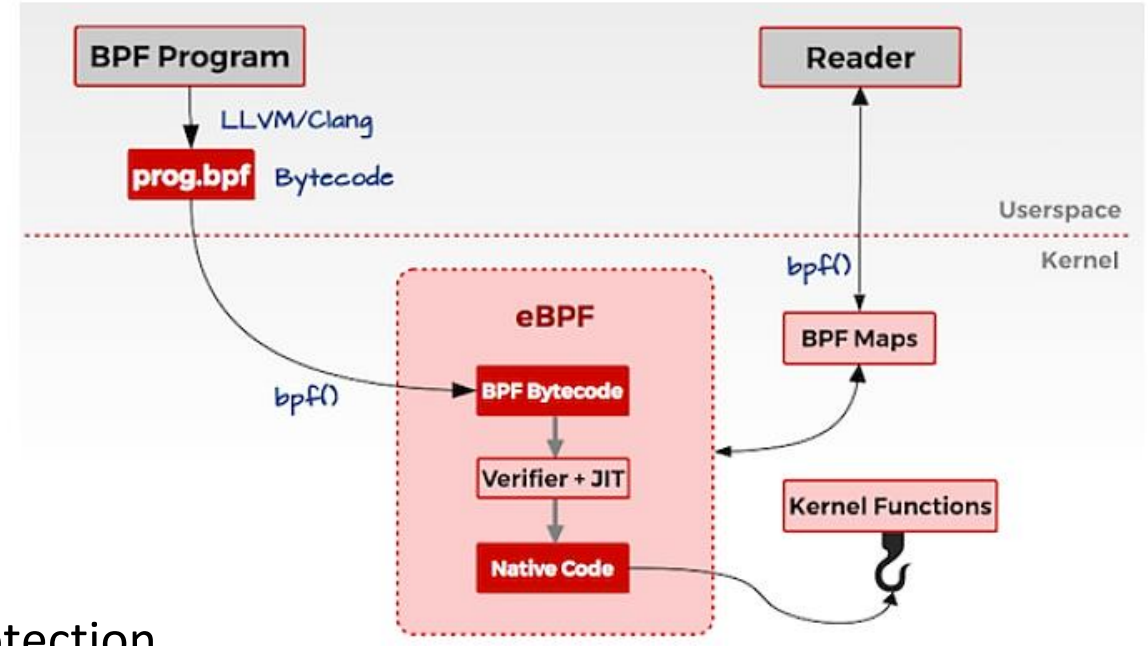
```
sysctl -w net.ipv4.tcp_syncookies=1
```



© Michał Szychowiak, 2022

eBPF DoS protection

Extended Berkeley Packet Filter



- example:

  Cloudflare DDoS protection
  "How to drop 10 million packets per second" by Marek Majkowski
  https://blog.cloudflare.com/how-to-drop-10-million-packets/

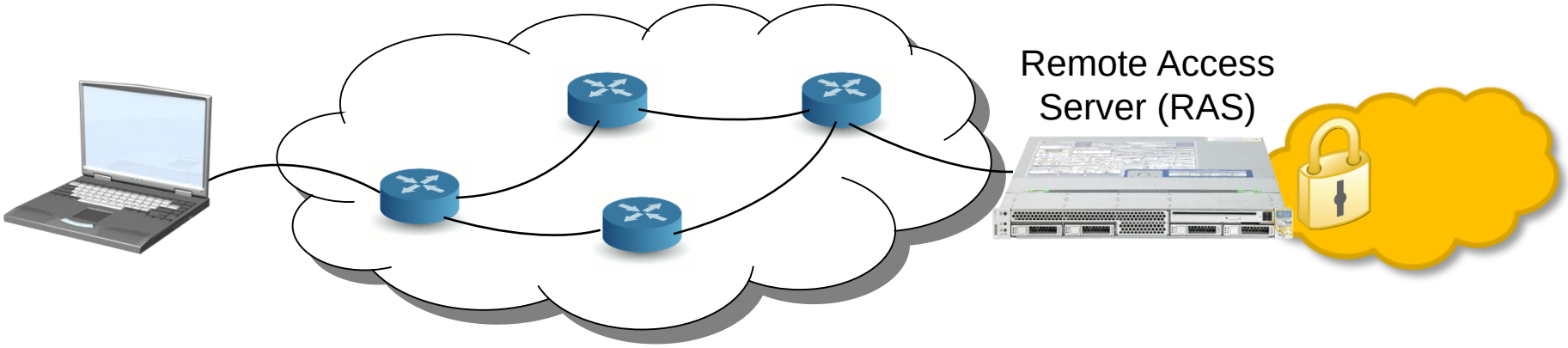
→ for using eBPF and XDP for network filtering see the Firewall lecture

© Michał Szychowiak, 2022

NETWORK AUTHENTICATION

© Michał Szychowiak, 2022

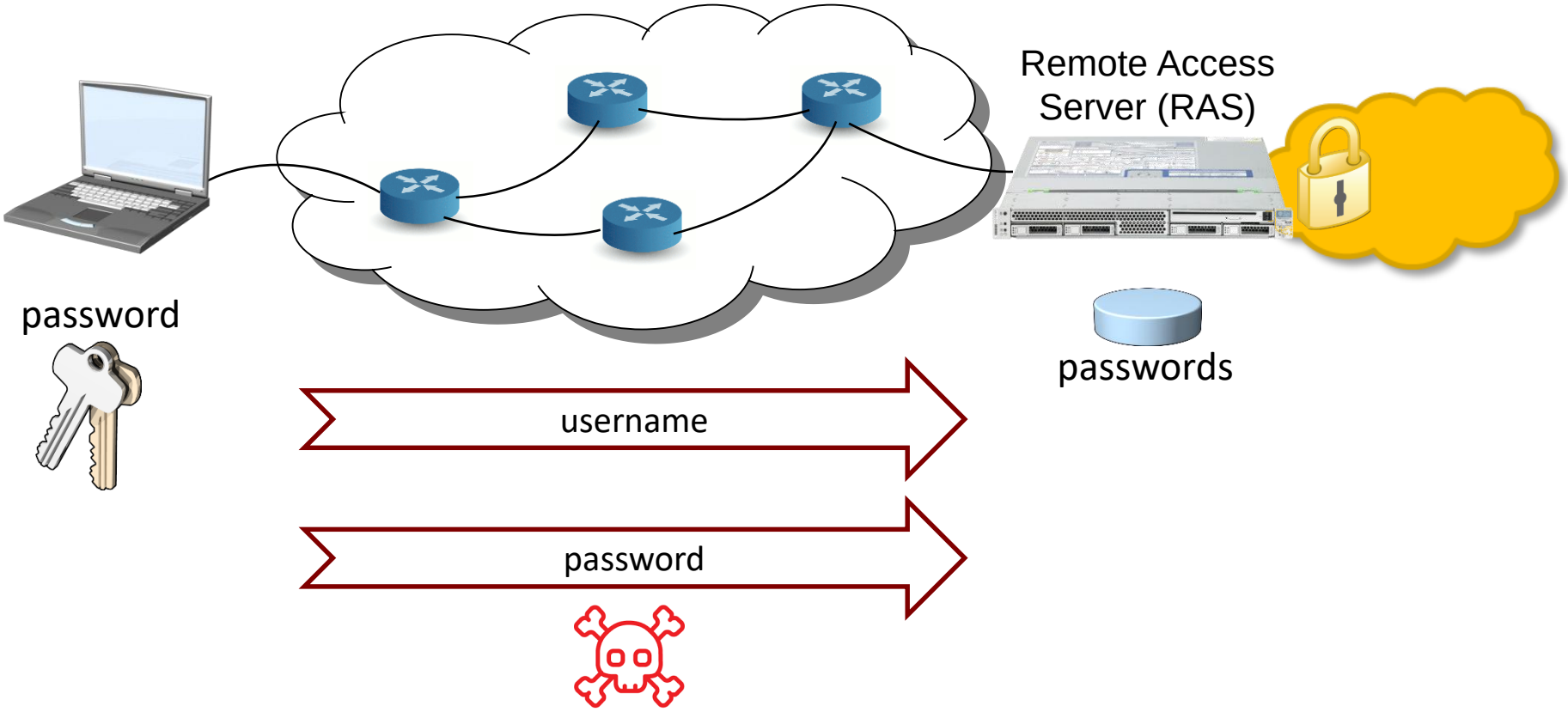
Network access



© Michał Szychowiak, 2022

Network access

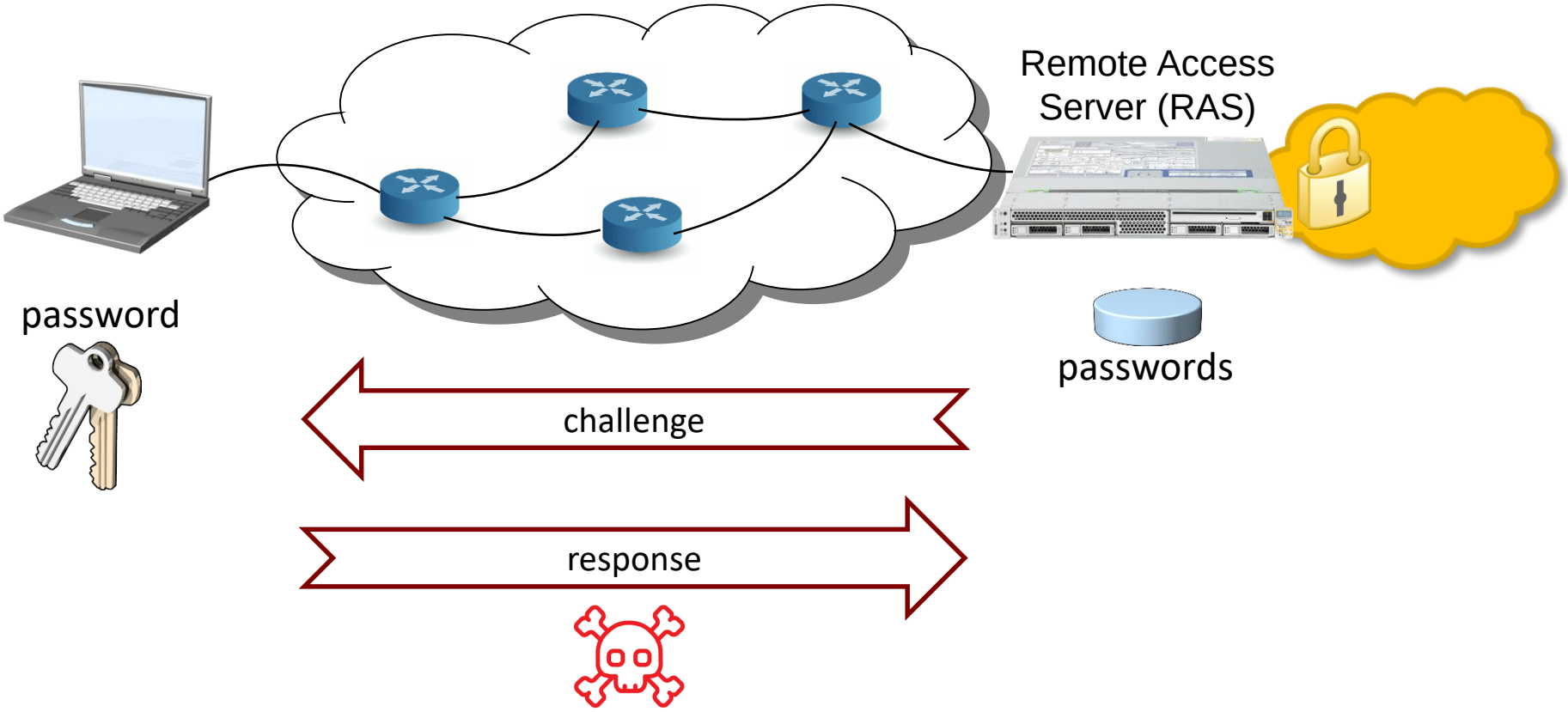
PAP (Password Authentication Protocol) RFC 1334



© Michał Szychowiak, 2022

Network access

CHAP (Challenge Handshake Authentication Protocol) RFC 1994



© Michał Szychowiak, 2022

Network access

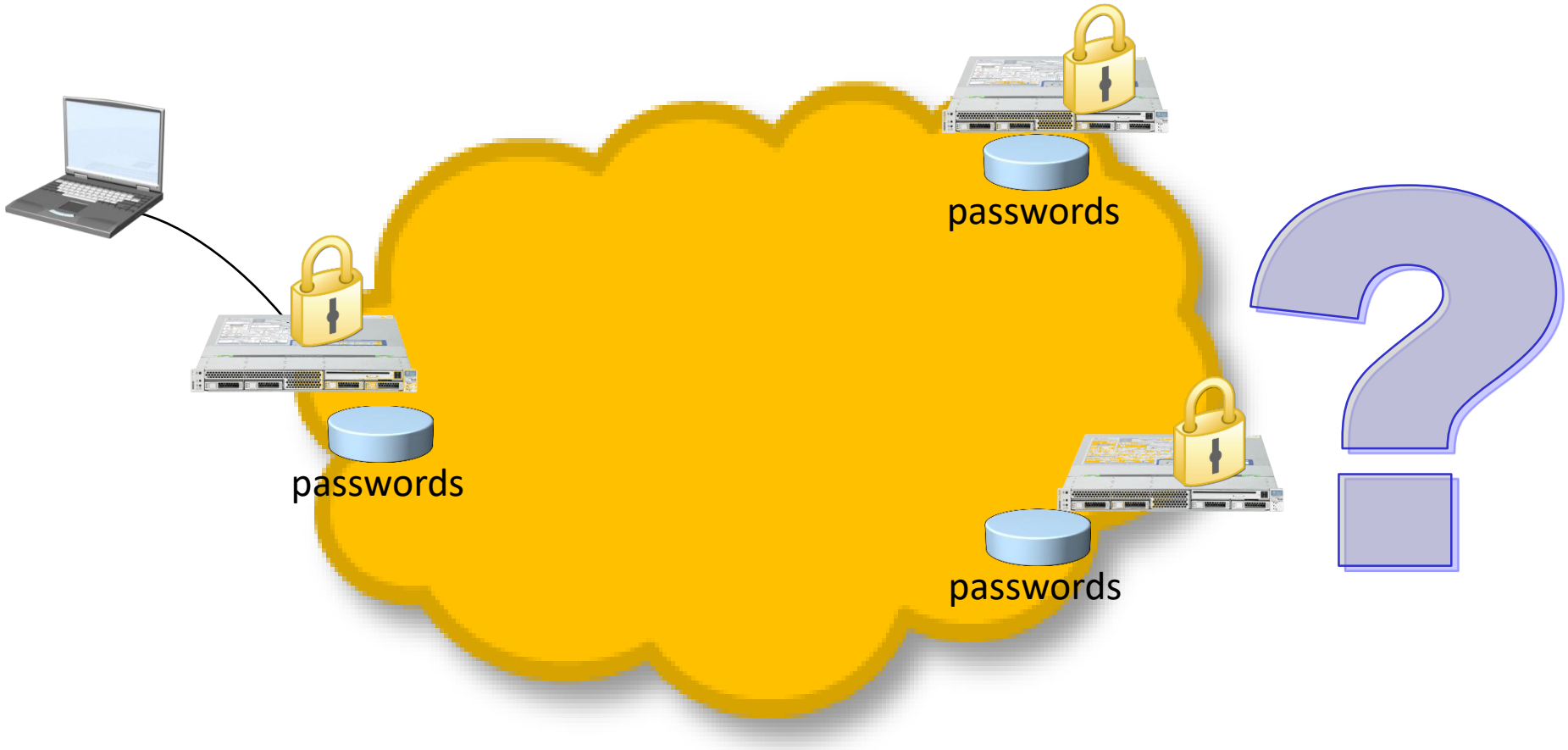
EAP (Extensible Authentication Protocol) RFC 2284

- allows multiple network access authentication methods
- supports 2-directional authentication
- specific authentication mechanism is chosen through a simple negotiation
  - EAP-TLS
  - EAP-TTLS (= Tunneled TLS)
  - EAP-FAST (= Flexible Authentication via Secure Tunneling)
  - EAP-PWD (= EAP Using only Password)
  - PEAP (= Protected EAP)
  - EAP-GTC (= Generic Token Card)
  - …

© Michał Szychowiak, 2022

RADIUS

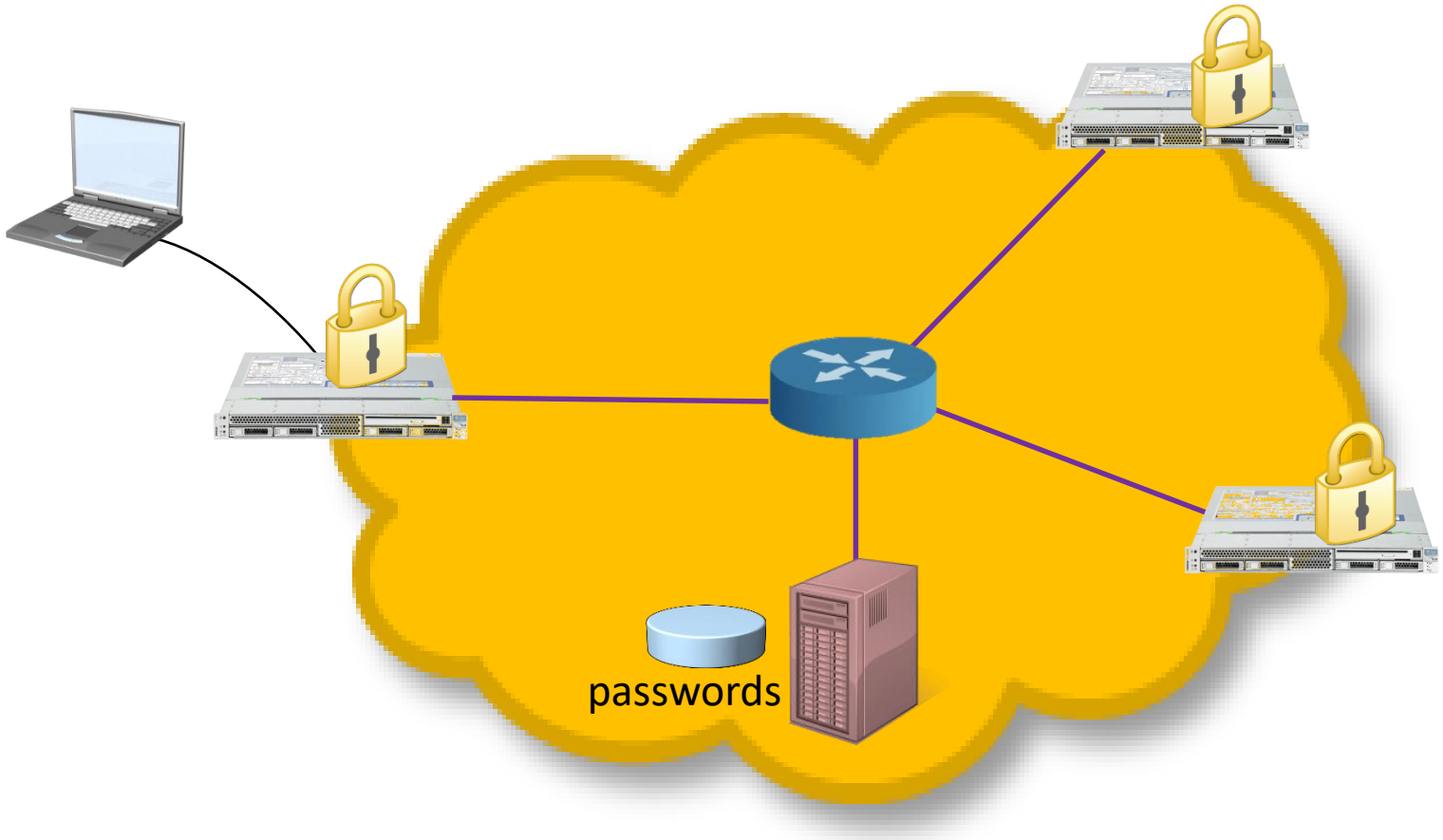
Remote Authentication Dial-In User Service RFC 2138



© Michał Szychowiak, 2022

RADIUS

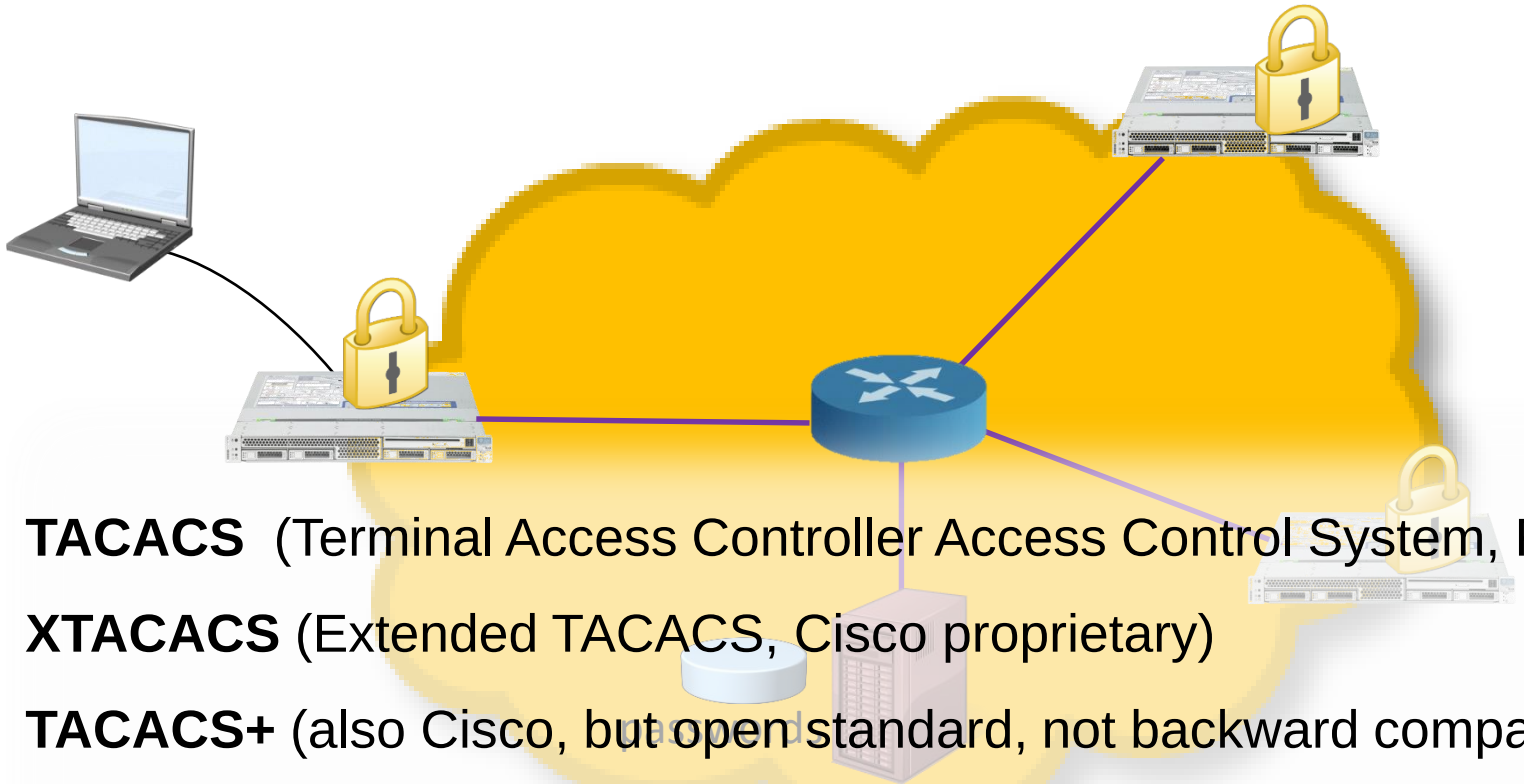
Remote Authentication Dial-In User Service RFC 2138



© Michał Szychowiak, 2022

RADIUS

Other AAA (Authentication-Authorization-Accounting) protocols



TACACS (Terminal Access Controller Access Control System, RFC 1492)

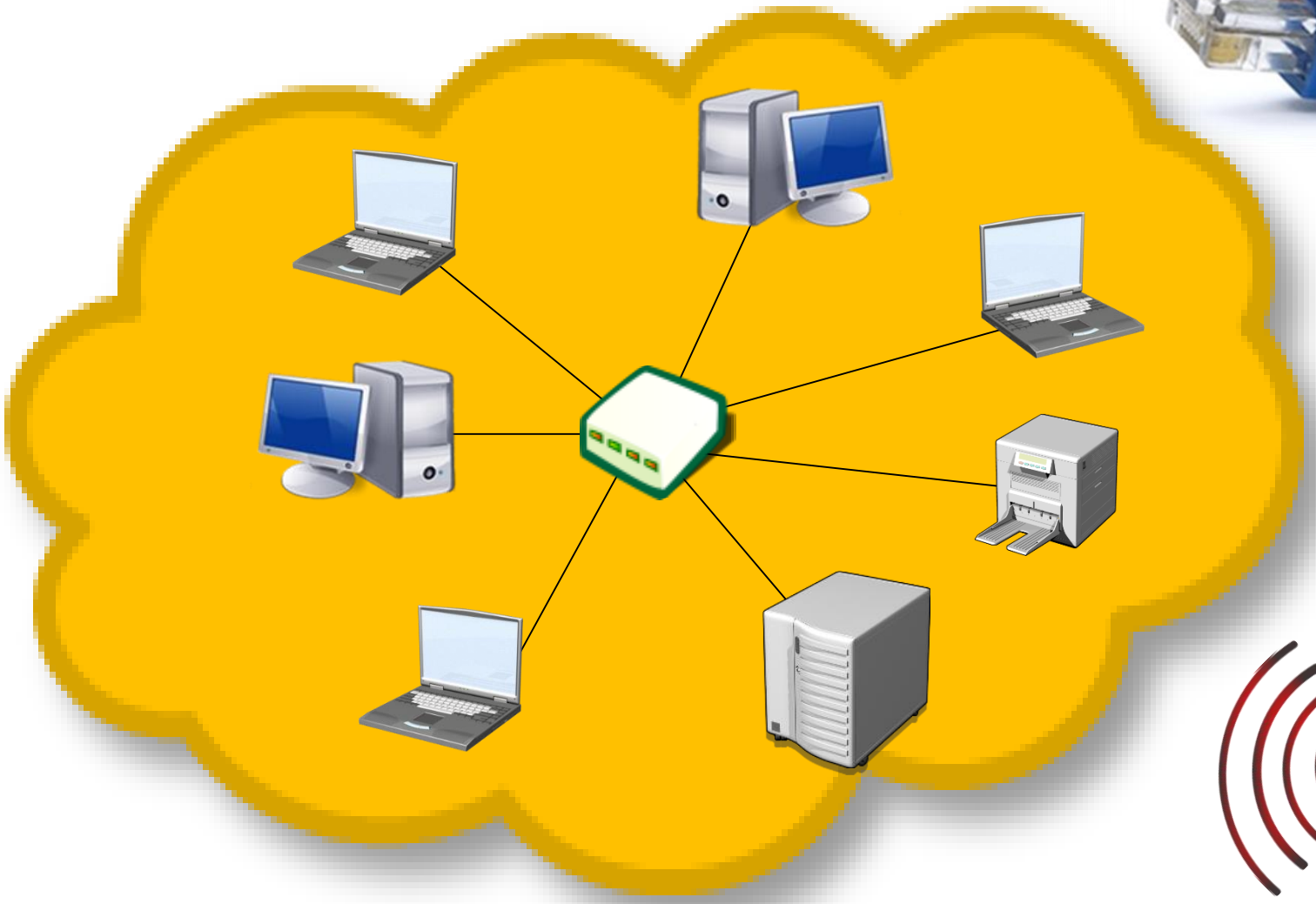
XTACACS (Extended TACACS, Cisco proprietary)

TACACS+ (also Cisco, but open standard, not backward compatible)

Diameter (RFC 3588, 6733 → LTE, IMS networks)

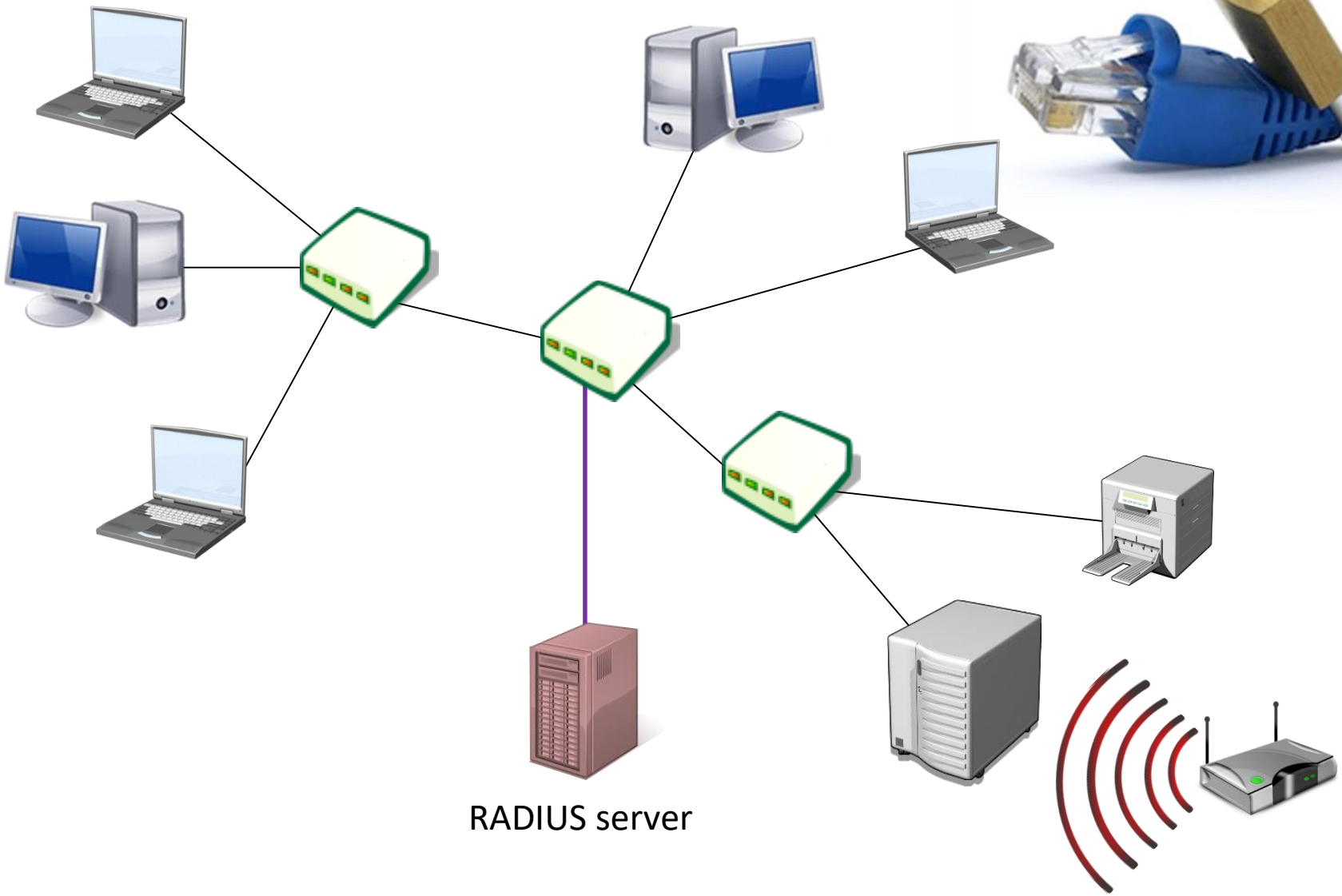
© Michał Szychowiak, 2022

IEEE 802.1X



© Michał Szychowiak, 2022

IEEE 802.1X



© Michał Szychowiak, 2022

IEEE 802.1AE

Media Access Control Security: MACSec

= authentication with 802.1X

+ MACSec encapsulation:

- provides ICV (*Integrity Check Value*)
- optional AES encryption

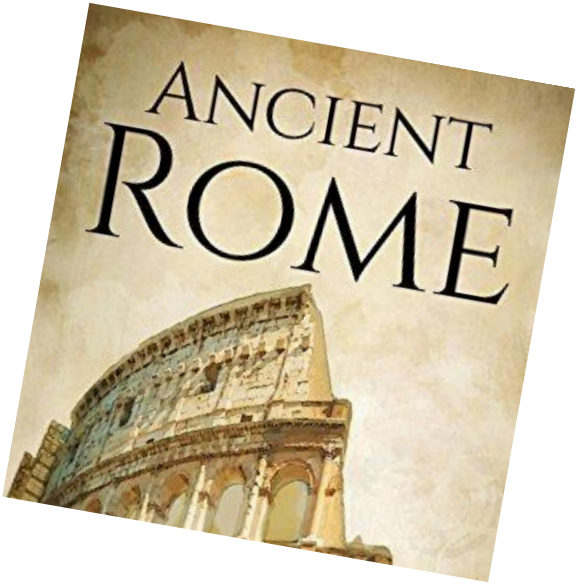
+ support:

- 802.1af Authenticated Key Agreement for MACSec
- 802.1AR Secure Device Identity

© Michał Szychowiak, 2022

© Michał Szychowiak, 2022

IEEE 802.11



WEP (Wired Equivalency Privacy)

- small key RC4-based stream cipher
- small IV
- low-level integrity (CRC-32)
- a lot of cracking tools

© Michał Szychowiak, 2022

IEEE 802.11

WPA (WiFi Protected Access)

- EAP 2-directional authentication
- AAA support
- TKIP (Temporal Key Integrity Protocol) = improved RC4
- crypto ICV (*Integrity Check Value*)
- WPA-Personal = WPA-PSK (Pre-Shared Key)
- WPA-Enterprise = WPA-802.1x = WPA-RADIUS

© Michał Szychowiak, 2022

IEEE 802.11

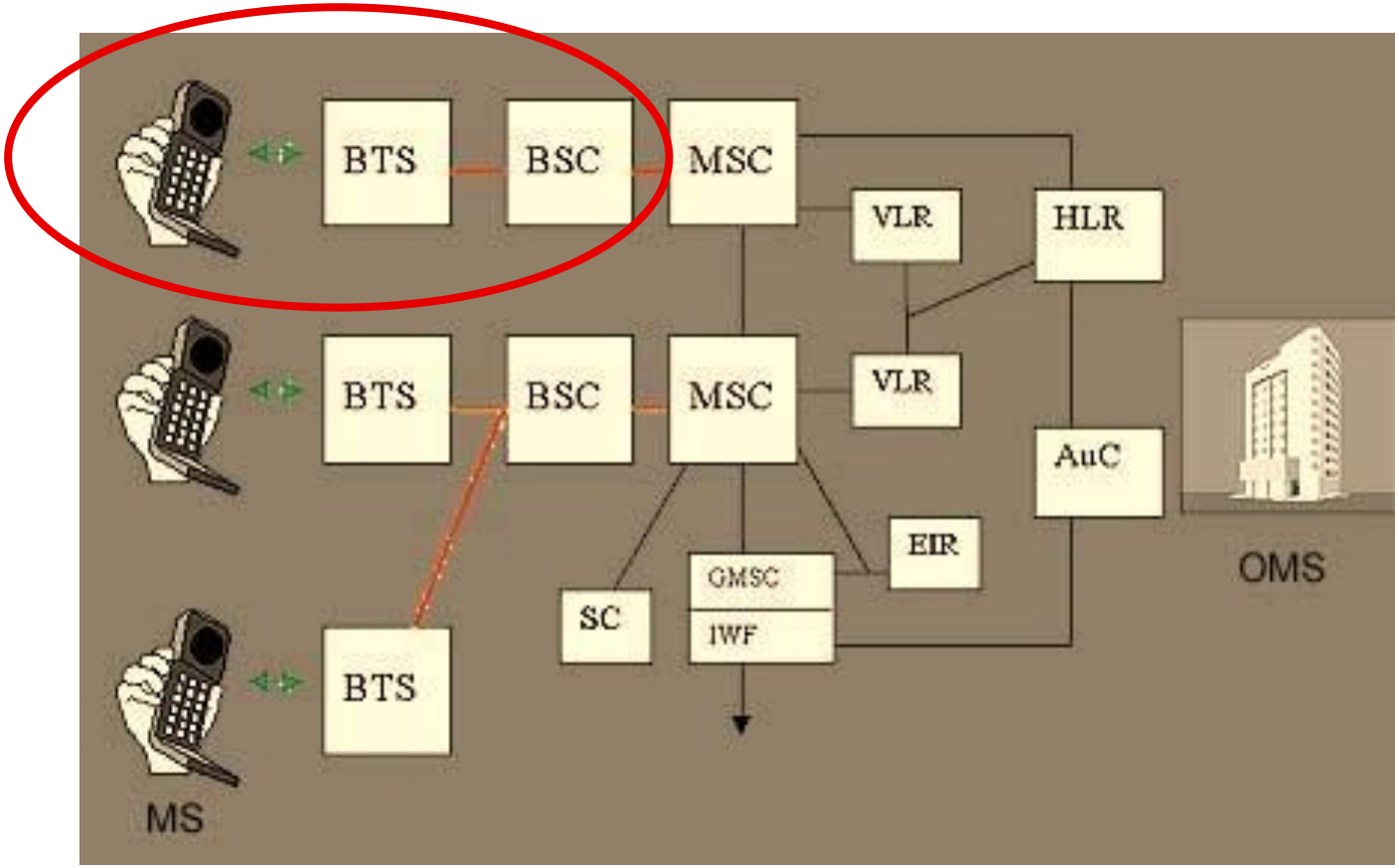
IEEE 802.11i (aka RSN, WPA2, WPA3)

- EAP + WRAP (*Wireless Robust Authentication Protocol*)
- AES-CCMP (*Counter-mode cipher block Chaining Message Authentication Protocol*) = AES-CM + CBC-MAC
- AES-GCMP (*Galois* …)
- implementation issues:
  - Krack (Key Reinstallation Attacks, 2017)
  - Kr00k (2019)
- WPA3:
  - no more PSK ⟶ Dragonfly Key Exchange (RFC 7664, Dan Harkins)
  - Dragonblood ⟶ WPA 3.1 update (2020)

© Michał Szychowiak, 2022

© Michał Szychowiak, 2022

GSM

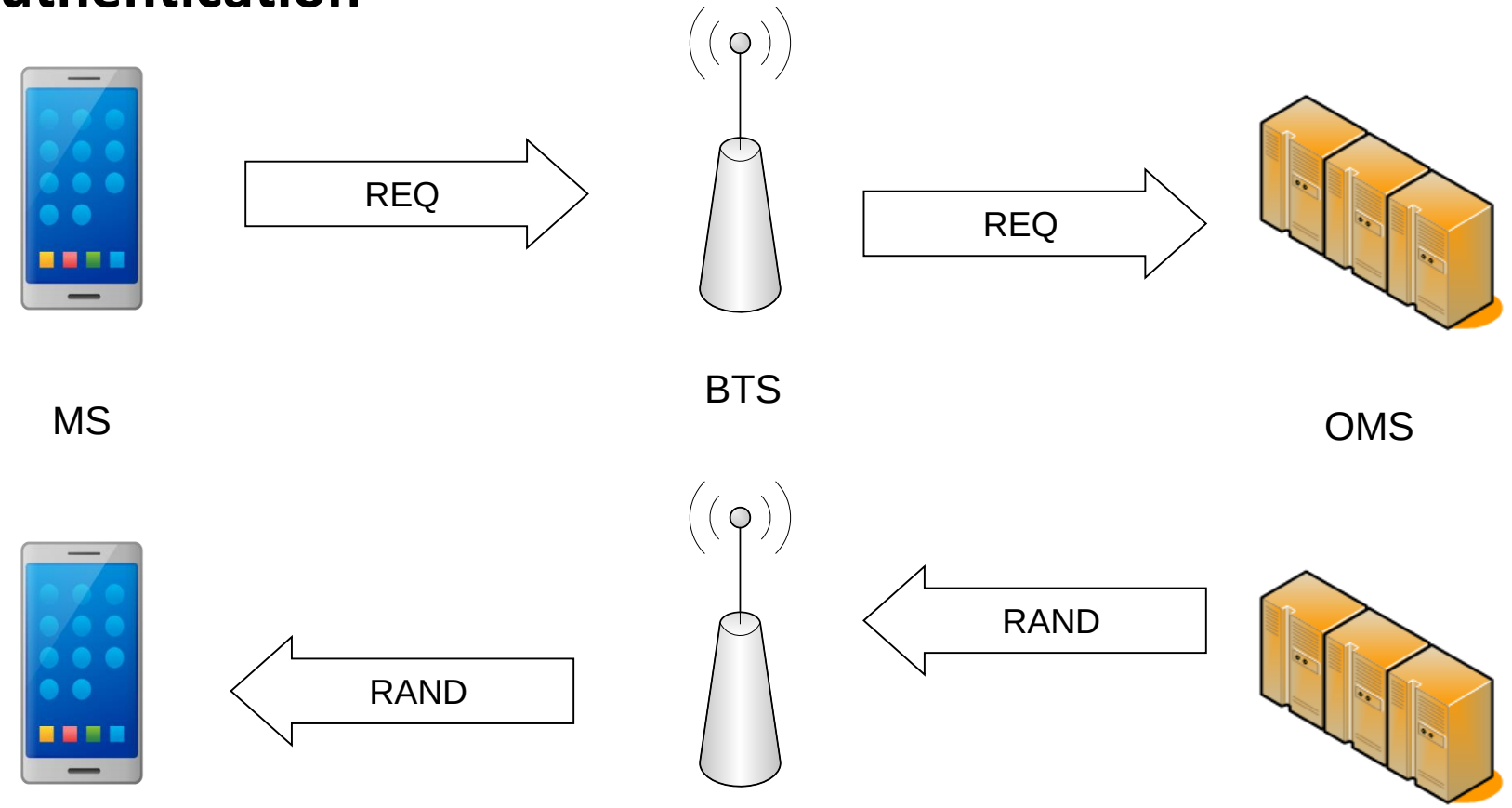


© Michał Szychowiak, 2022

- voice transmission: 114b packets,
- symmetric crypto algorithm **A5**
  - A5/1 , and weakened A5/2
  - EDGE → A5/3, A5/4
  - GPRS: GEA2, GEA3, GEA4 (Mitsubishi Electric Corp.)
- SIM (Subscriber Identity Module) contains:
  - IMSI (*International Mobile Subscriber Identity*)
  - $\mathbf{K_{SIM}}$
- crypto authentication:
  - algorithm **A3**
  - algorithm **A8**

© Michał Szychowiak, 2022

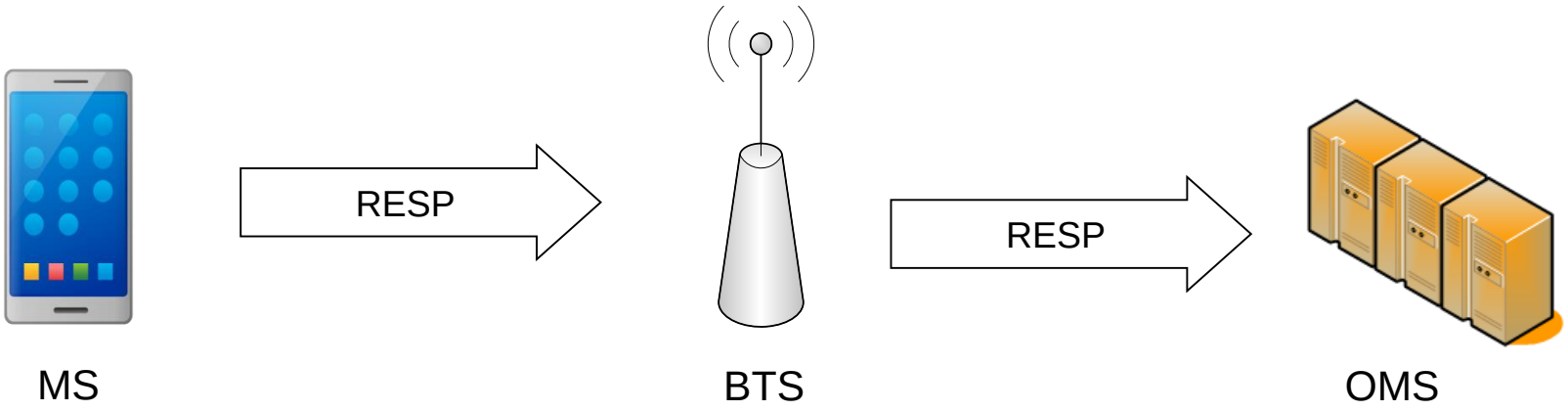
Authentication



© Michał Szychowiak, 2022

Authentication

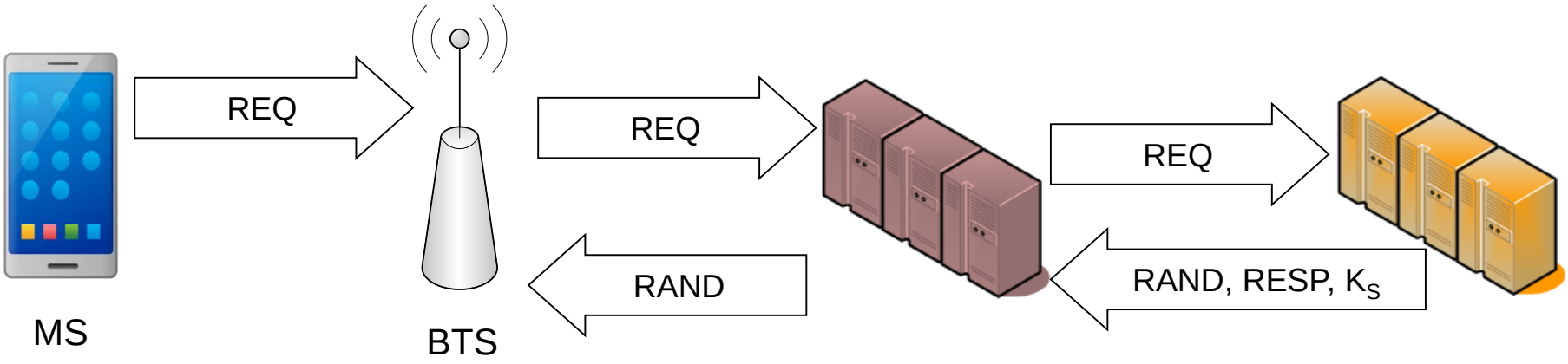
- SIM card prepares RESP = A3 [K_{SIM}, RAND]



- and 64b session key K_S = A8 [K_{SIM}, RAND]
- A5 is basically XOR with IV derived from K_S

© Michał Szychowiak, 2022

Roaming



© Michał Szychowiak, 2022

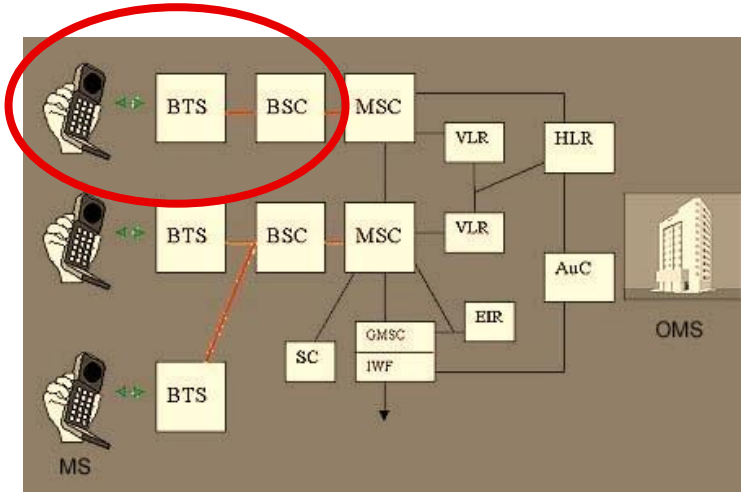
Threats

- unilateral authentication

© Michał Szychowiak, 2022

Threats

- unilateral authentication
- only radio transmission encrypted



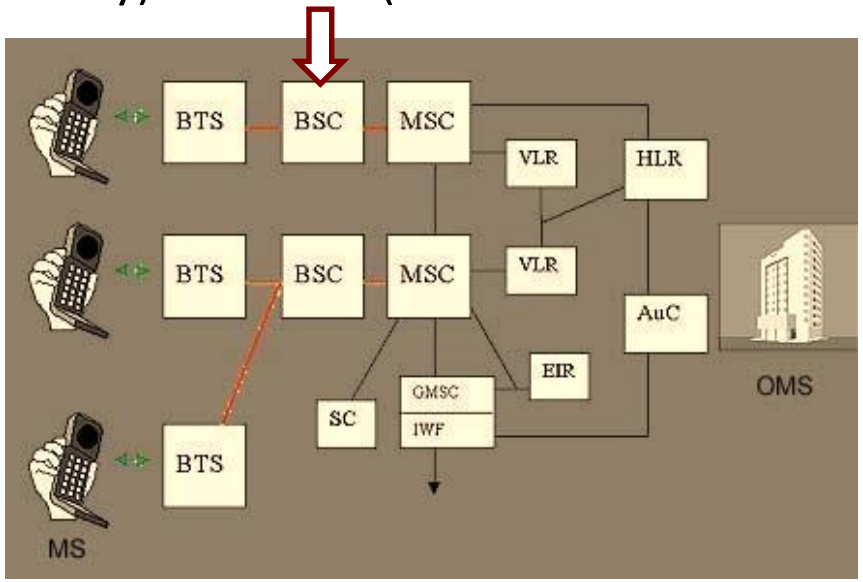
© Michał Szychowiak, 2022

Threats

- unilateral authentication
- only radio transmission encrypted
- no crypto signature
- no seq numbers
- vulnerable signalization protocols:
  - SS7 (North America)
  - C7 (others)

© Michał Szychowiak, 2022

- better signalization protocols: SS7 /C7 → Diameter (IP, see VoLTE)
- AKA (Authentication and Key Agreement) protocol
  = BTS is now also authenticated
- seq. no. + crypto integrity
- packets encrypted (optionally) until RNC (*Radio Network Controller*)



© Michał Szychowiak, 2022

3G UMTS (*Universal Mobile Telecommunications System*)

- protocols by Mitsubishi: UEA1 (encryption) and UIA1 (integrity)
- block cipher KASUMI 128b

4G LTE (*Long Term Evolution*), LTE-A (… *Advanced*)

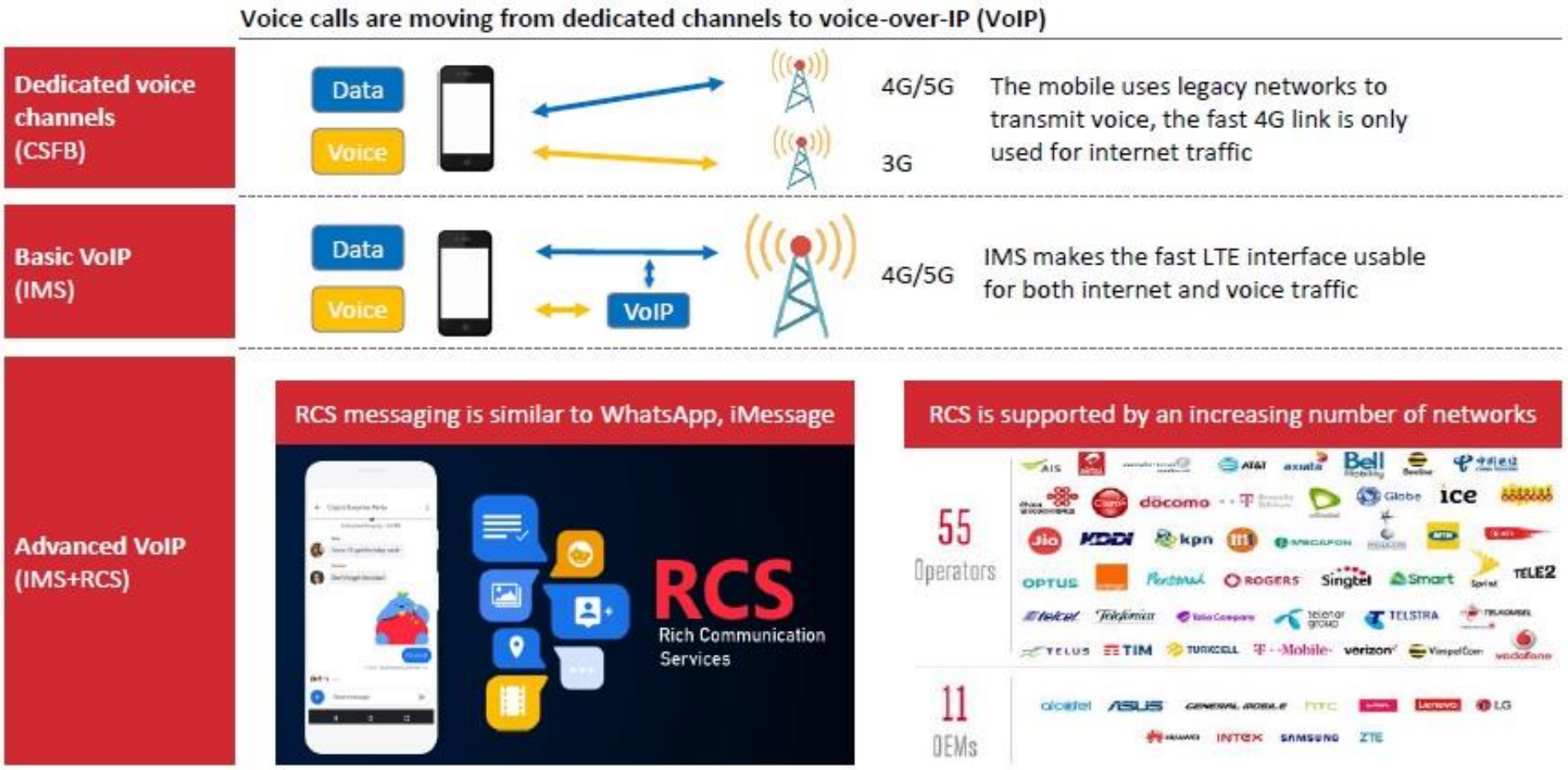
- UEA2 (SNOW 128b/256b) and UIA2
- EEA1 (AES) and EIA1
- EEA3 (stream cipher ZUC 128b by Chinese Academy of Sciences), EIA3

5G NR (New Radio)

© Michał Szychowiak, 2022

5G and beyond

IMS (IP Multimedia Subsystem) – VoLTE (Voice over LTE), VoWiFi



© Michał Szychowiak, 2022


"That's all Folks!"