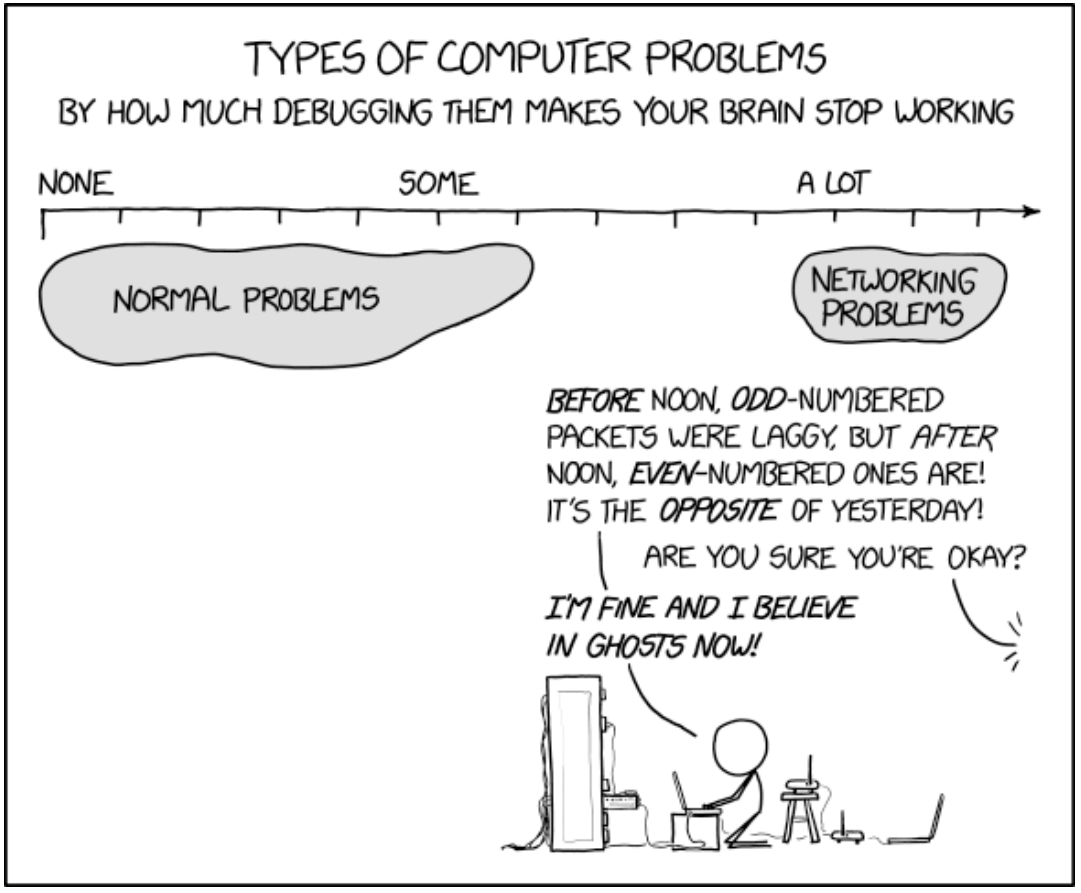
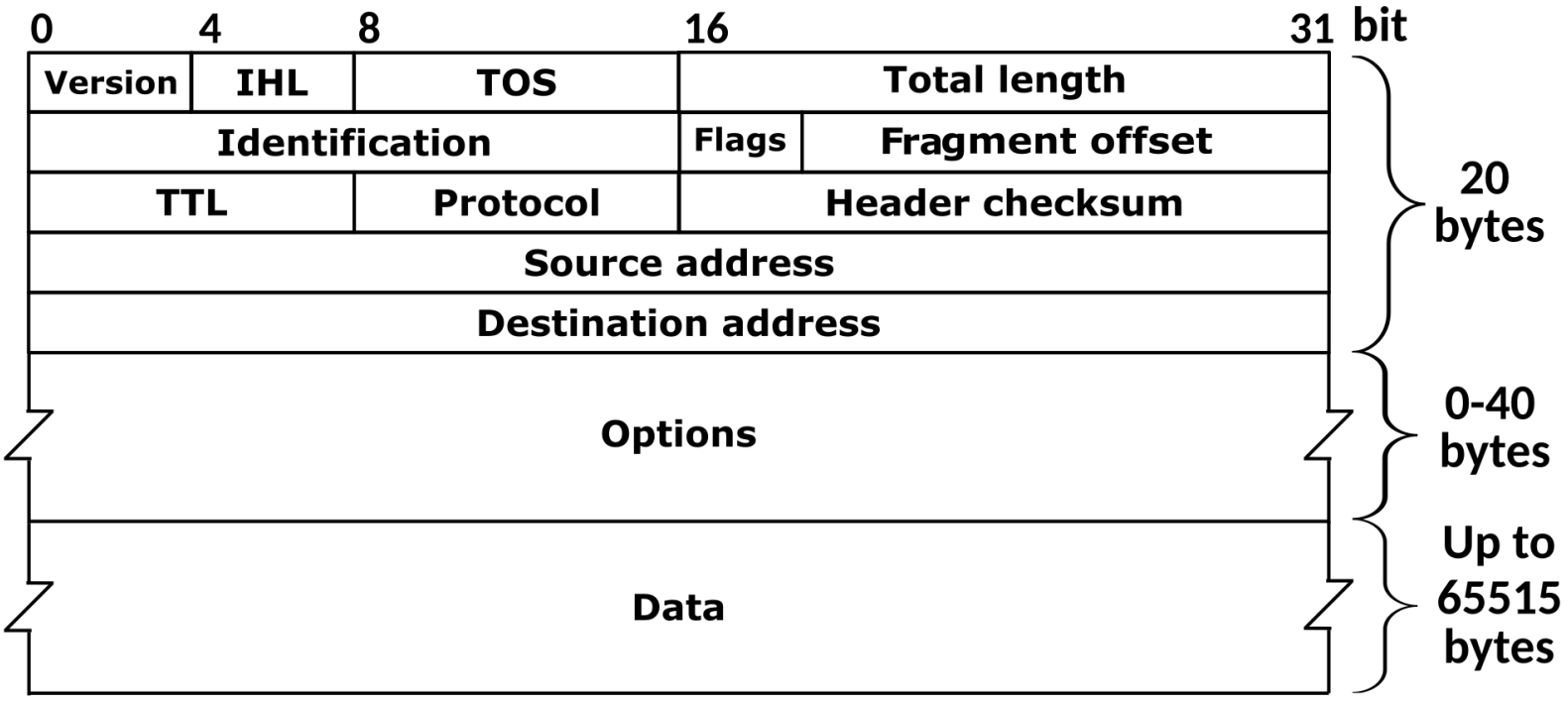
CSCI 3330 Cybersecurity



Word of the day

ONE-LINE FIX n. Used (often sarcastically) of a change to a program that is thought to be trivial or insignificant right up to the moment it crashes the system. Usually ‘cured’ by another one-line fix.

Internet protocol (IP): Layer 3



Three pillars of Information Security

- AKA CIA triad

CIA triad

- Confidentiality: private data should not be read by unauthorized people
- Integrity: data should not be modified or deleted by unauthorized people
- Availability: authorized users should have access to their data

Threat models

- On-path:
  - MITM (machine in the middle): can read, insert, modify, delete messages
  - MOTS (machine on the side): can only read and insert messages
- Off-path
  - Can insert messages (and must coerce hosts to send messages to attacker)

Who are our adversaries?

- Who might want to read or manipulate our traffic?

Who are our adversaries?

- ISPs (including VPN providers)
- Organizations
- Governments
- Traditional criminals

ARP spoofing

- Spoof response
- Gratuitous ARP response
- Who would you spoof?
- *Anyone on your network can read your traffic*

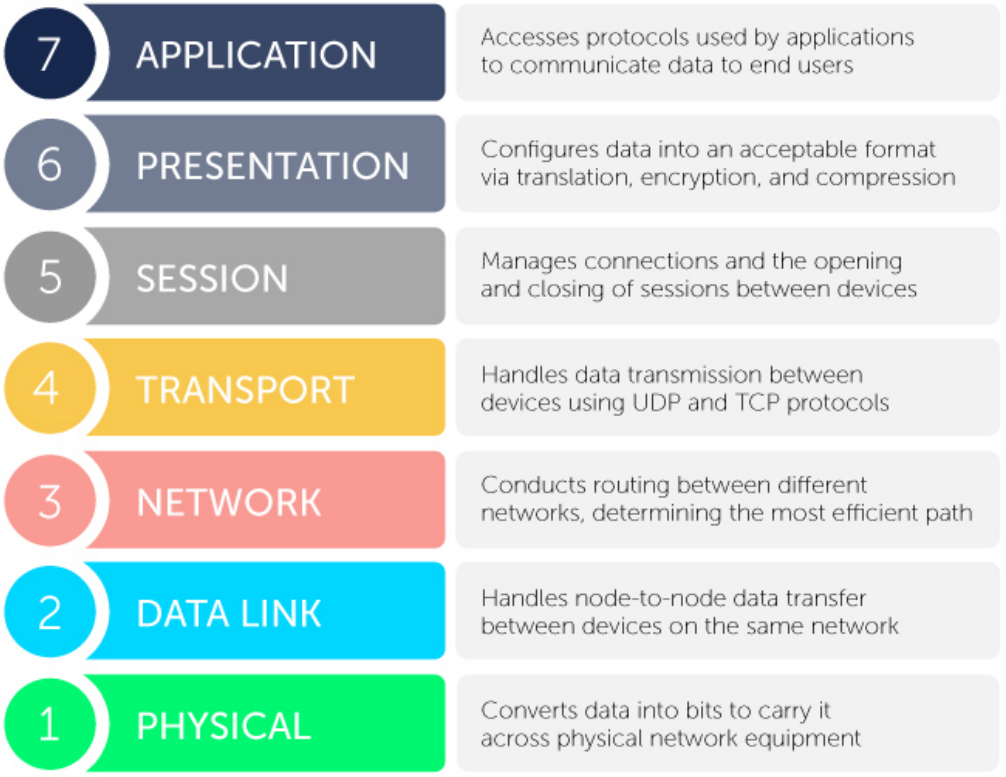
TCP connection hijacking

- If you have the right network position
- Initial sequence number randomization thwarts off-path attempts

SSL/TLS (Layer 6.5?)

- Secure Socket Layer
- Transport Layer Security
- Why layer 6.5?

Network layers (OSI model)



Port scanning

- Determine which services are running
- Why would we want to do this?

Port states

- Open port: SYNACK response
- Closed port: RST response
- Filtered: No response

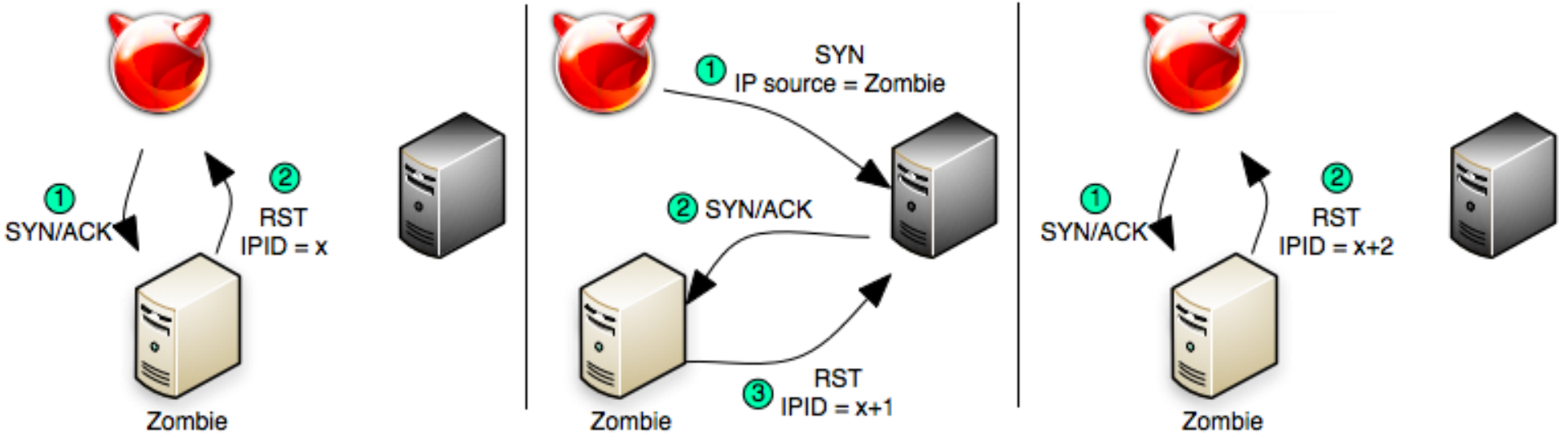
Idle Scan

- Off-path port scanning
- IP identifier
- *Spoofing*

Idle Scan

- IPID counters
- Global IPID
- Per-destination counter
- Hybrid approach (e.g., 2048 counters)

Idle Scan


1
SYN/ACK
2
RST
IPID = x
Zombie
1
SYN
IP source = Zombie
2 SYN/ACK
3
RST
IPID = x+1
Zombie
1
SYN/ACK
2
RST
IPID = x+2
Zombie

Domain Name System (DNS)

- Converts name to IP address
- Record types:
  - NS: nameserver
  - A: IPv4 address
  - AAAA: IPv6 address

Security in DNS

- DNSSEC: DNS Security
- DoT: DNS over TLS
- DoH: DNS over HTTPS

Why not just DNSSEC?

- DNSSEC only validates, does not encrypt
- Most end user clients don’t verify
  - WHY? Because breaking DNS is already too common…
- DNS over HTTPS: piggyback on protocol already considered secure

Putting it all together

- DNSSEC
  - Between servers and recursive resolvers
- DoH/DoT
  - Between you and your DNS server

Assignment 4

- Deadline: October 13, 2025, 10:00pm
- Advanced SQL information inference https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment4.pdf