Network Security

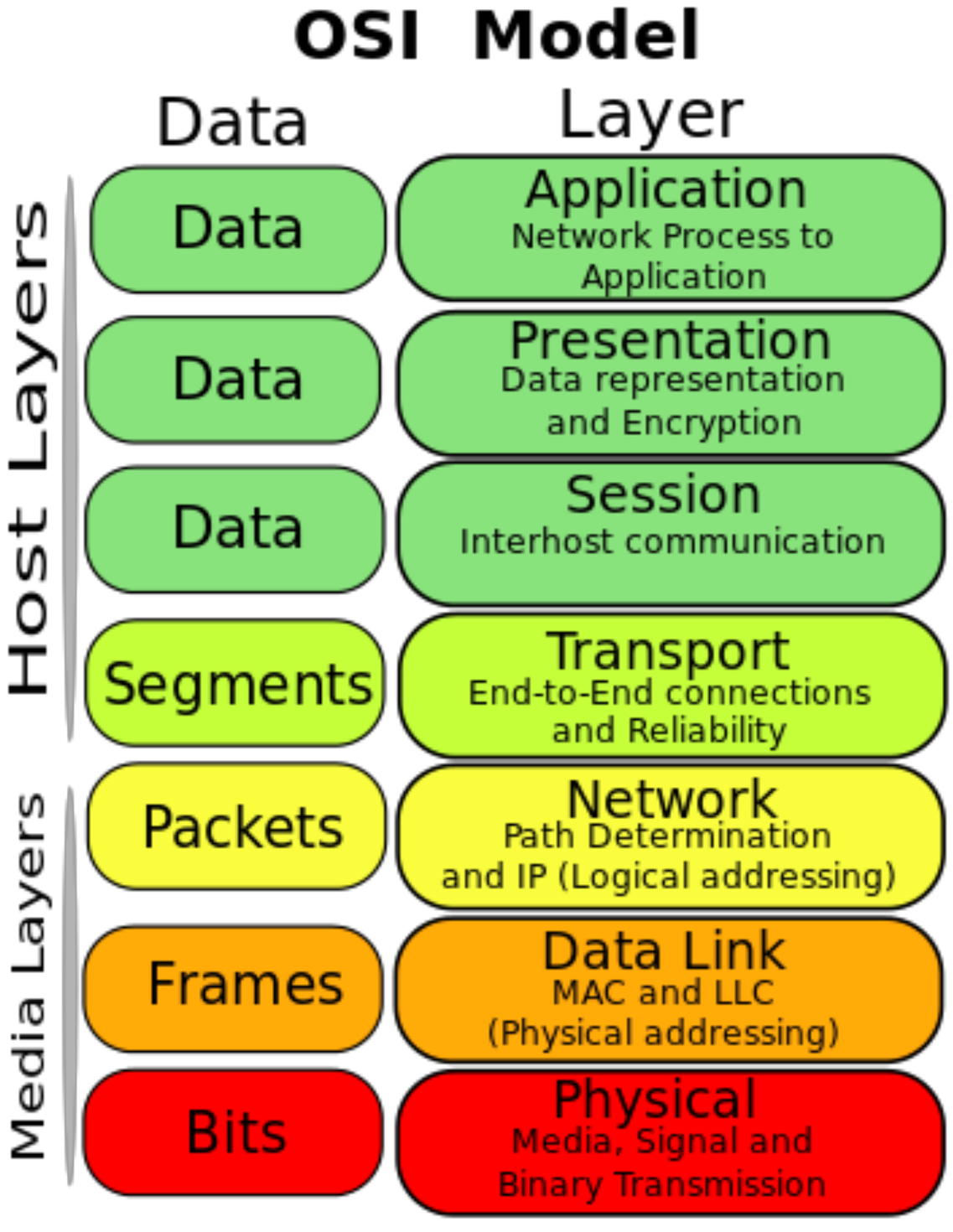
51.502 Systems Security

Paweł Szałachowski

Network Security

- Network
  - Set of interconnected computers that share resources
- Internet
  - Network of networks
- Threat model?

Network Layers and Protocols



- IP
- ARP
- TCP
- UDP
- ICMP
- SSL/TLS
- HTTP
- …

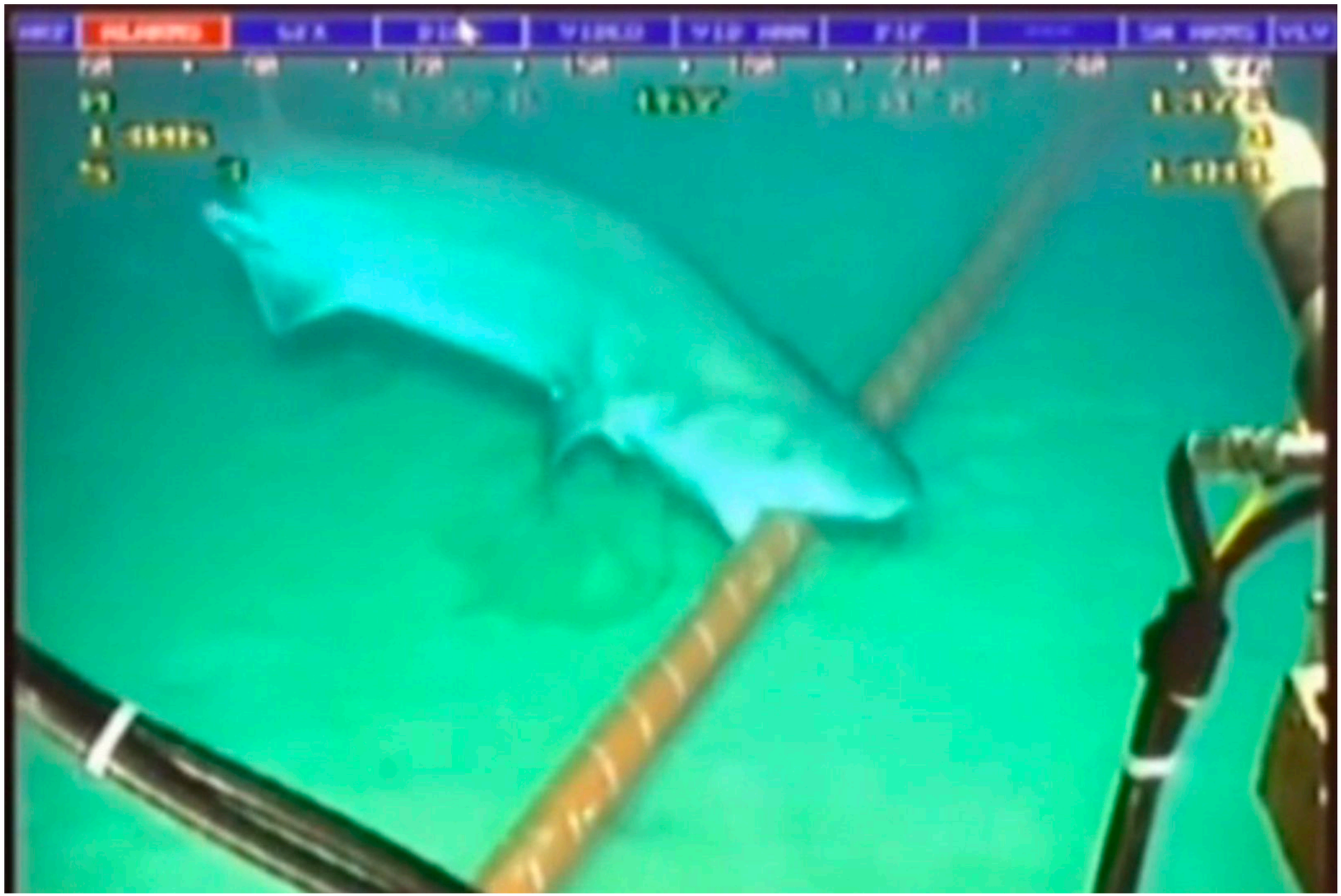
Layer 1

- PHY chip
- Different on different systems
- Operates on raw bits
- Encoding, decoding, transmission, signaling, …

Layer-1 Attacks

- Physical attacks
  - destruction, obstruction, manipulation, malfunction
- Jamming
- Eavesdropping
- …

Layer-1 Attacks



Layer 2

- **Ethernet**
  - Fairly simple
  - Frames as data units
  - Hubs and switches
- PPP, SLIP, MPLS, ATM, Frame relay, …

Layer-2 Attacks

- **ARP Attacks**
  - Hubs & Switches (CAM overflow)
  - ARP Sniffing & Spoofing
- VLAN Attacks
- MAC Spoofing
- DHCP Attacks

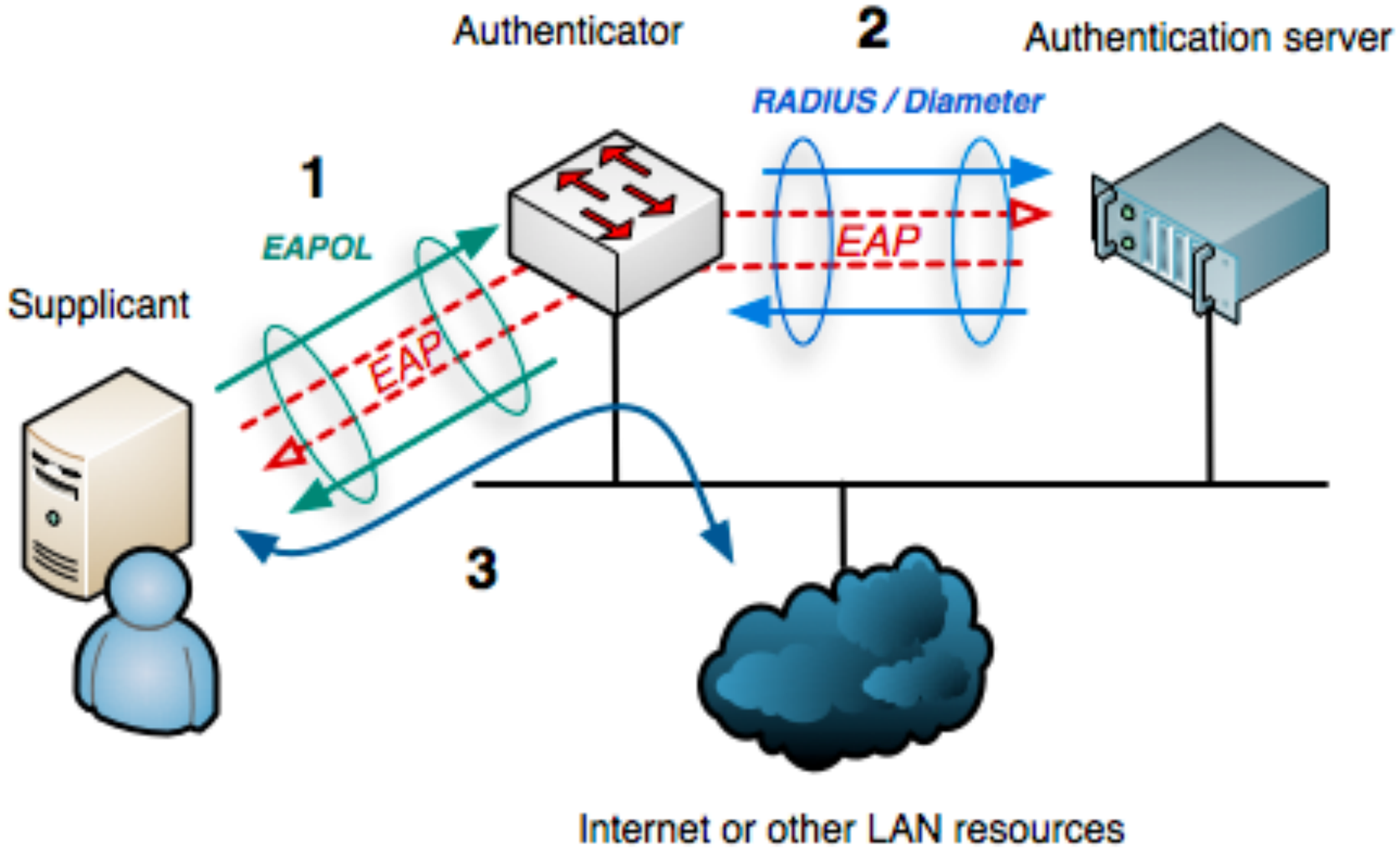
Layer-2 Prevention

- Port Security
  - Monitor ports, ARP messages and caches, ICMP redirect, TTLs
    - One address per port & check MAC of port
      - Annoying and difficult to maintain in dynamic networks
- MACsec (802.1AE)
  - Authentication + Encryption for ethernet frames

WiFi Security

- Open medium
  - Eavesdropping is easy
  - Easier to “access” network
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access II (WPA2)

802.1X


Authenticator
2
Authentication server
RADIUS / Diameter
1
EAPOL
Supplicant
EAP
EAP
3
Internet or other LAN resources

Layer 3

- IP
  - Addressing
    - IPv4 vs IPv6
      - Local and global addresses
  - Connection-less
  - Packet is the data unit
- Routing protocols

Layer-3 Attacks

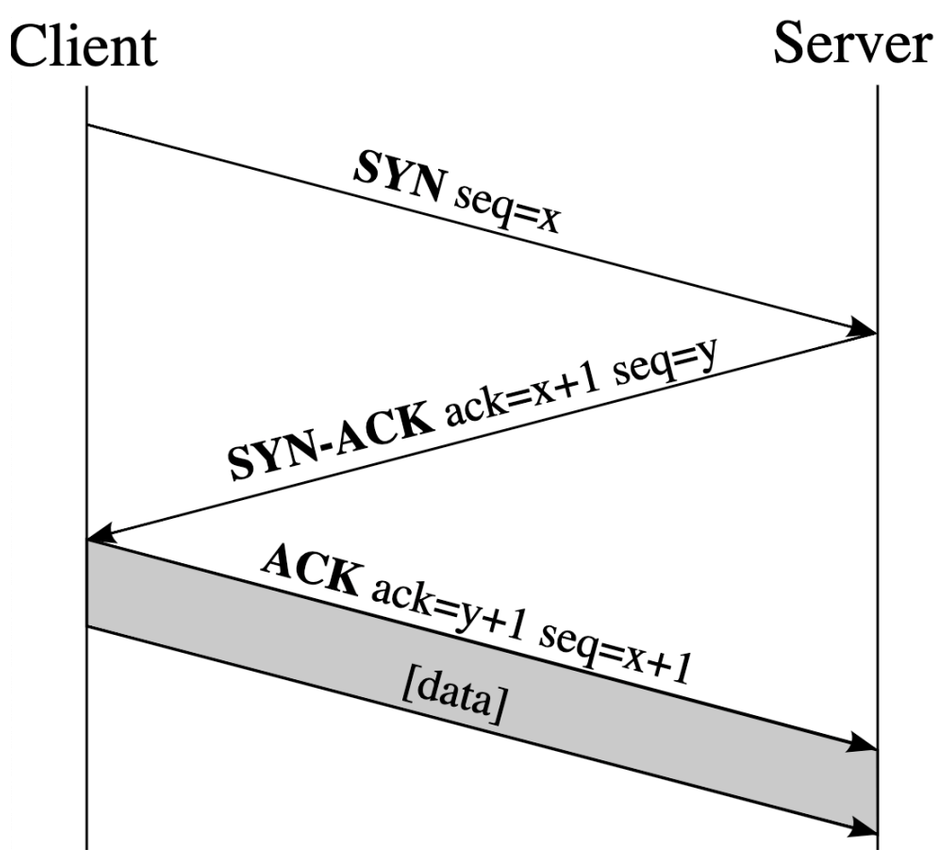
- Distributed Denial of Service (DDoS)
- IP spoofing
- Smurf Attack
- Routing Attacks
- Eavesdropping, modification, injection, …

Layer-3 Prevention

- Disable broadcast addresses
- Secure routing protocols
- IPSec

Layer 4

- Segments as data units
- The Transmission Control Protocol (TCP)
  - Reliable
  - Handshake
  - Sequence numbers
- User Datagram Protocol (UDP)

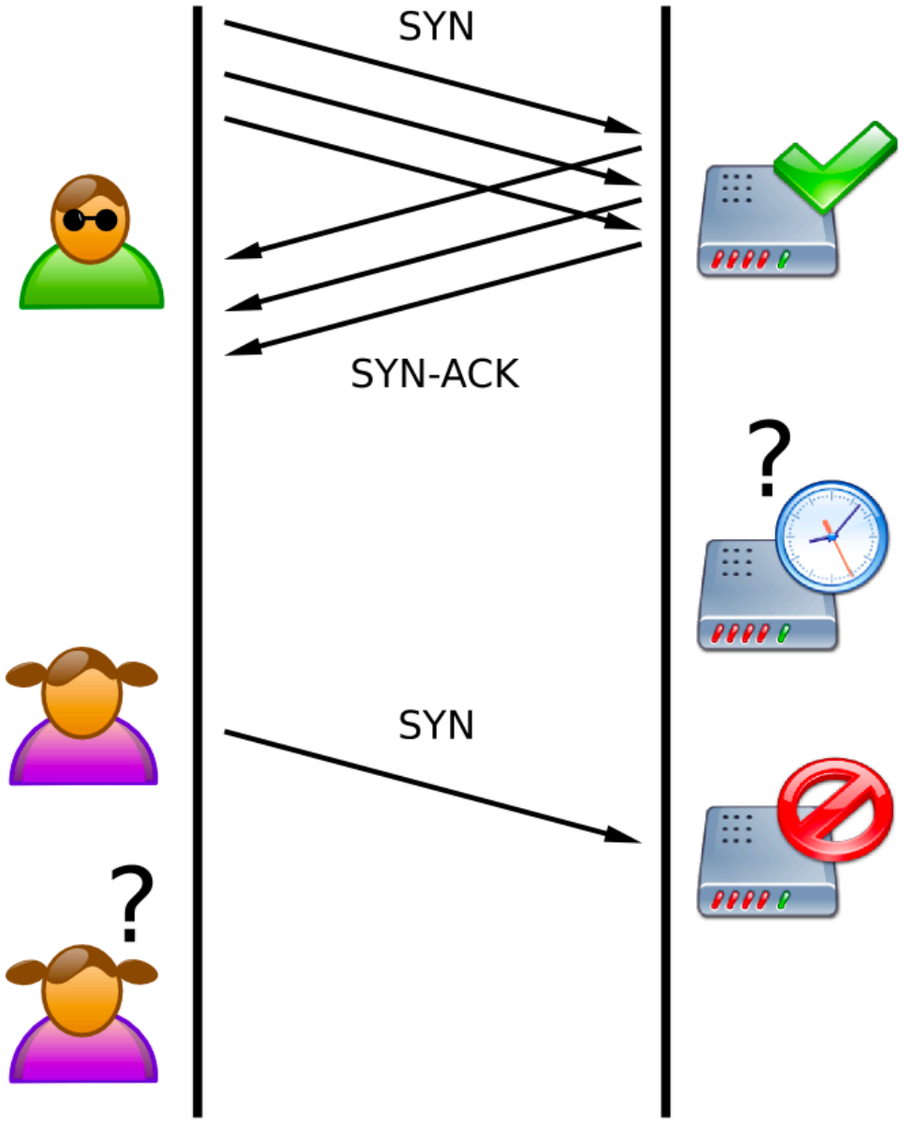


UDP vs TCP

- Fast vs slow
- Unreliable vs reliable
- Connectionless vs connection-oriented
- Security implications ?
  - Reflection and amplification attacks

Layer-4 Attacks

- DDoS
- UDP spoofing
- TCP hijacking
- Connection reset and slow-down
- SYN flooding
- DNS attacks …



Layer-4 Prevention

- Random source port and sequence numbers
- SYN Cookies
  - Don’t allocate resources after SYN
- Cryptography
  - TCPCrypt
  - TLS/SSH (not really L4)

Other issues

- Cross-layer attacks
- Malware
- Insiders
- Advanced persistent threat

Other Defenses and Mechanisms

Defense

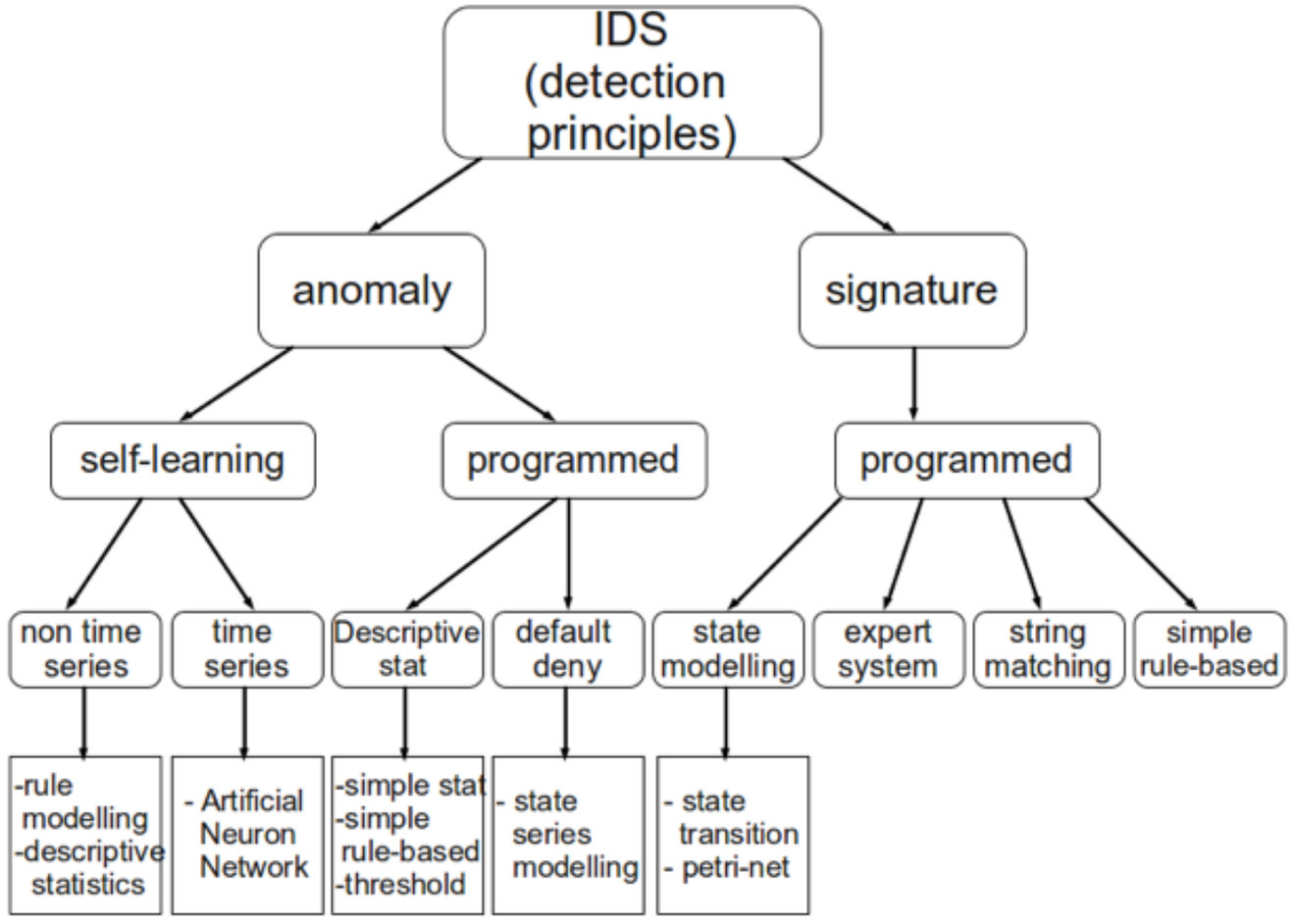
- Management
    - Keep your systems updated and configured to minimize the attack surface
- Filtering
    - Use firewalls to block attacks
- Intrusion Detection
    - Monitor network to find suspicious behavior
- Data protection
    - Encryption + authentication

Firewalls

- Network and host-based firewalls
    - Defense in depth
- Packet Filters (1st generation)
    - Make decisions (allow or reject or drop) basing on network addresses, protocol, and ports
- Stateful Filters (2nd generation)
    - Understand layer 4 and make decisions base on that
- Application layer (3rd generation)
    - Understand (some) applications and protocols
    - HTTP, DNS, SMTP, …
    - Often combines with intrusion detection/prevention systems

Intrusion Detection

- Monitor networks or systems for adversarial activities
- Can be placed in different locations
  - NIPS, WIPS, NBA, HIPS, …
- Different detection methods
  - Signature-based detection
  - Anomaly-based detection
  - *Protocol analysis detection
- Limitations and issues
  - False positives and false negatives
  - Encryption makes them almost useless
  - Many attacks (fragmentation, frog-boiling attacks, …)



Data Protection

- SSL/TLS
- SSH
- IPSec
- VPNs

Reading

- [And] Chapter 21

- https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

Questions?