Imperial College London

Network and Web Security

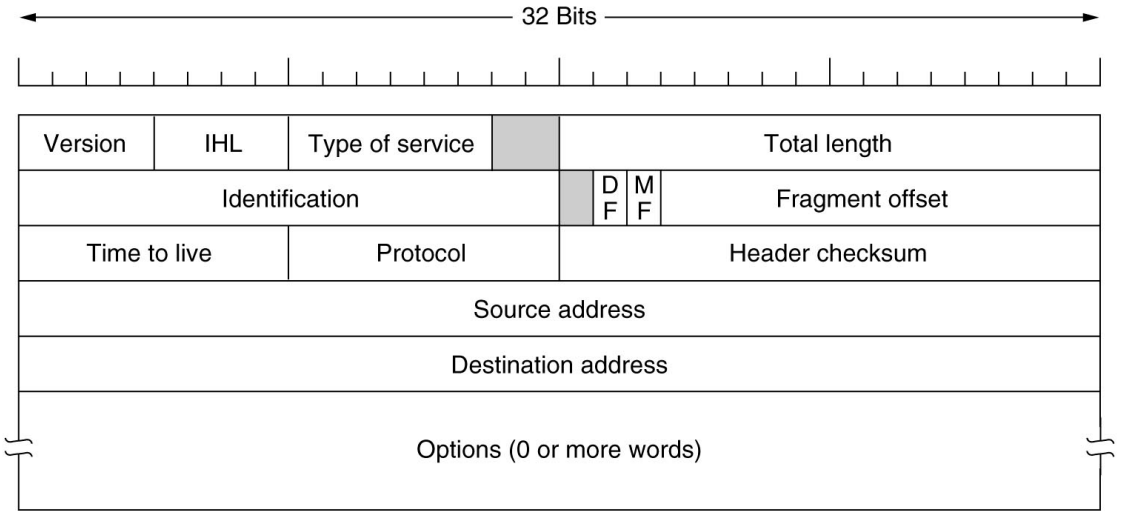
IP security

Dr Sergio Maffeis
Department of Computing
Course web page: https://331.cybersec.fun

Internet Protocol

Imperial College London

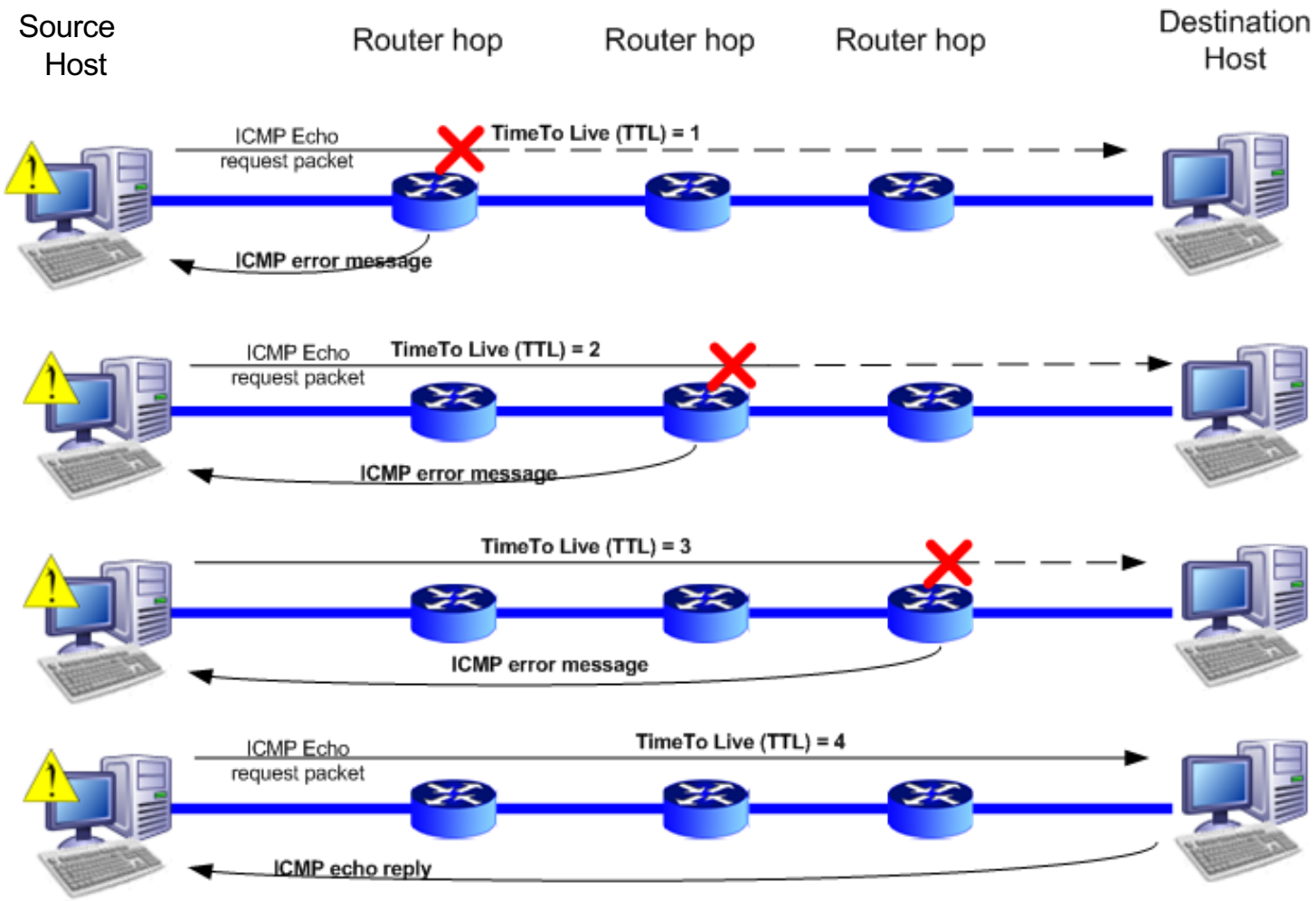
- The IP protocol delivers packets between *Source* and *Destination* hosts
- Structure of IP addresses is hierarchical and guides routing
- Protocol is “best effort”: may drop or reorder packets
- IP packet can be fragmented when it transits on networks with smaller packet sizes
  - **D**on’t **F**ragment, **M**ore **F**ragments flags indicate fragment type
  - *Fragment offset* gives position of fragment in original packet
  - *Identification* differentiates fragments for different packets
  - Various OSs treat duplicate IP fragments in different ways: used for OS fingerprinting
- *Time to live* (TTL) is used to discard packets that take too many steps to reach destination
  - TTL is decremented at each step (“hop”) in the network until it reaches 0
  - At 0, packet is discarded and ICMP error message is sent to source



Traceroute

Imperial College London

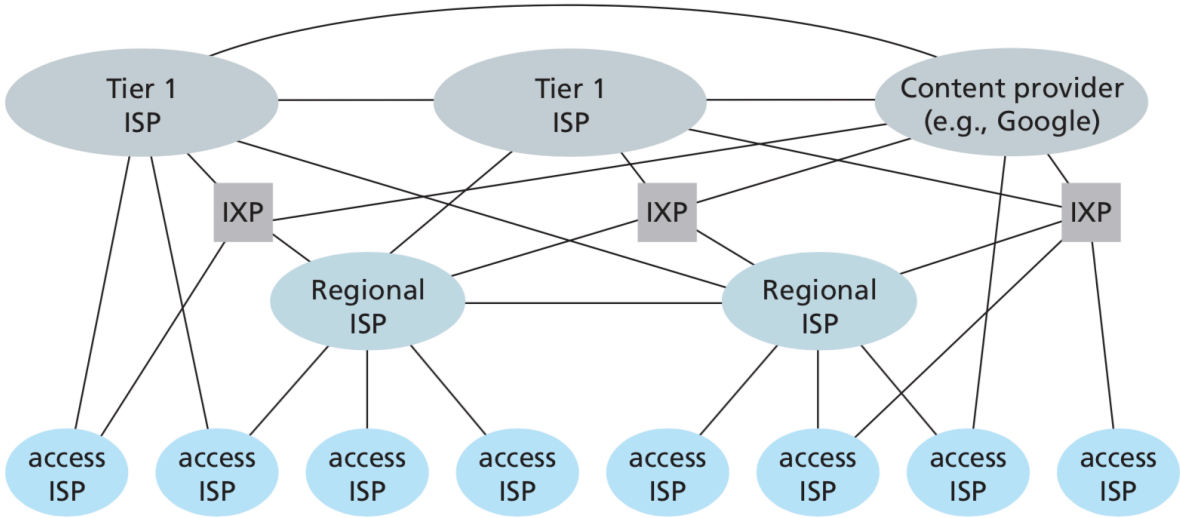
- Traceroute algorithm uses TTL to identify hosts/routers on path to target
  - Send packets increasing TTL (1, then 2, then 3, …) until destination is reached
  - Each ICMP error message should be from a host on the path to the destination



IP security

Imperial College London

- The source IP is not authenticated and easy to spoof
  - Off-path attacker can send packets with target IP as source
    - The target will receive response
    - Used for attacks including idle scanning, DDoS
  - Hard to trace back malware infections, attribute cyber attacks
- The Internet is a *decentralised* network of *untrusted* networks
  - Packets travel through untrusted hosts
    - MITM attacker can directly read packets and modify payload
  - BGP routing is partly based on *trust*
    - One AS cannot keep track of all IP addresses
    - ASs ask each other the *route* to reach an IP of a distant AS
    - *BGP hijacking*: malicious AS can advertise false routes, divert traffic, and become MITM



BGP hijacking levels

Imperial College London

- Clumsy: in 2008 Pakistan wanted to prevent its own users from accessing YouTube
  - Their BGP hijacking ran out of control
  - For 2 hours the world was without YouTube
  - Global panic ensued
- Medium: in 2017 China Telecom diverts selected communications from its Texan ISP
  - *The Hidden Story of China Telecom's BGP Hijacking*

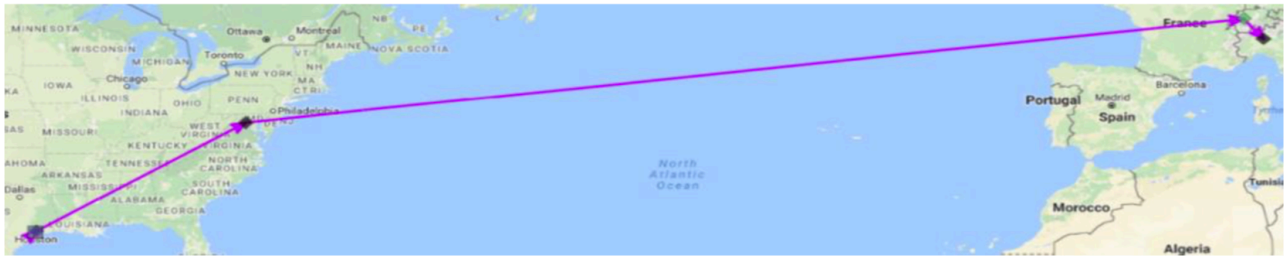


Figure 3a: US large bank to Italy normal route

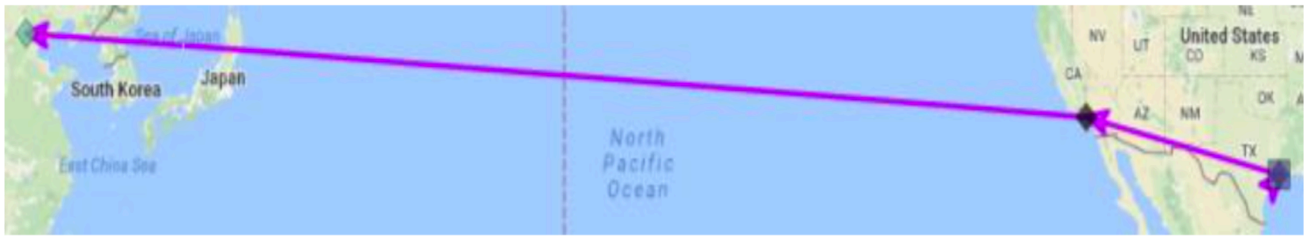
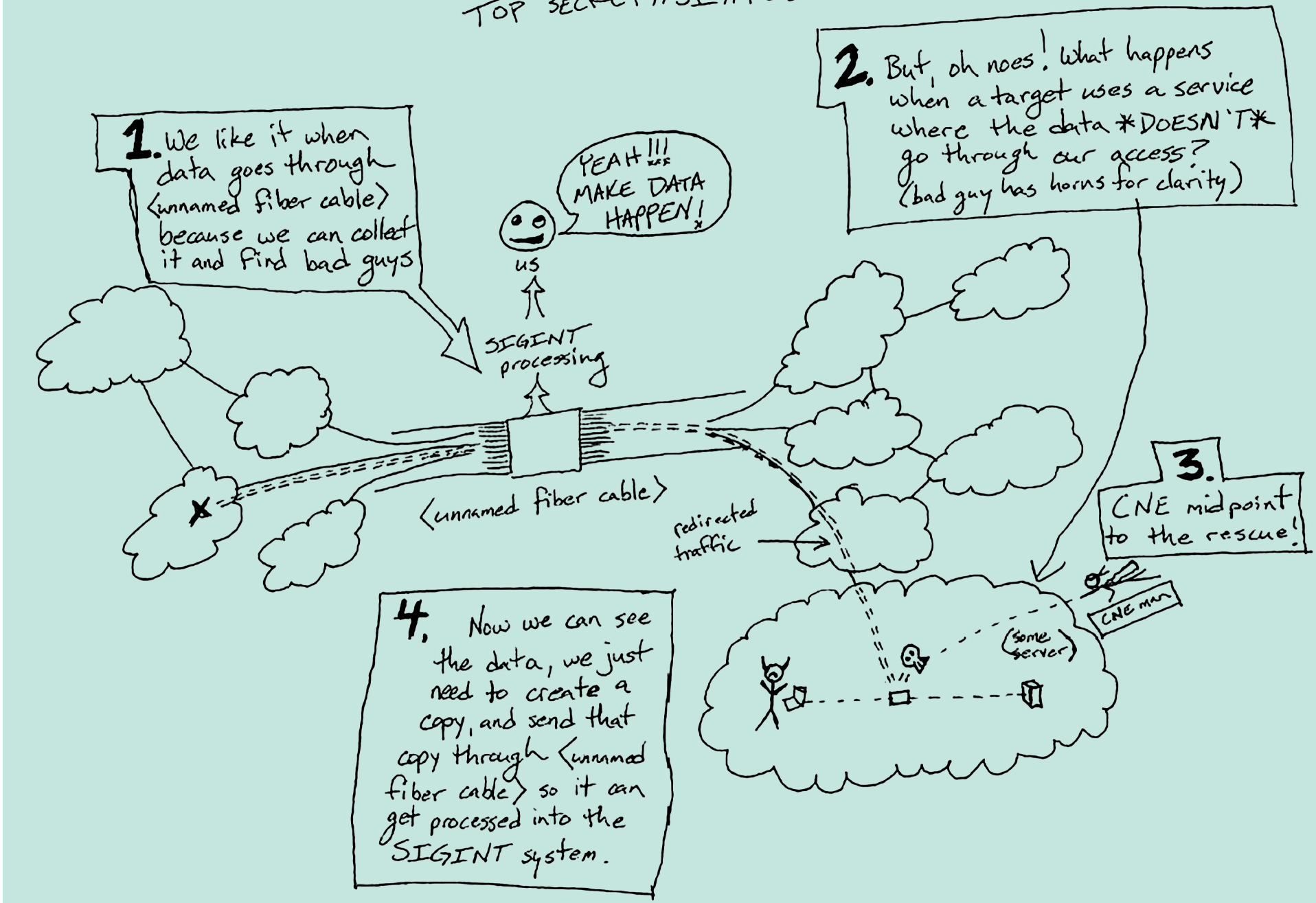


Figure 3b: US large bank to Italy but after hijack, traffic never arrives, seems to terminate in China.

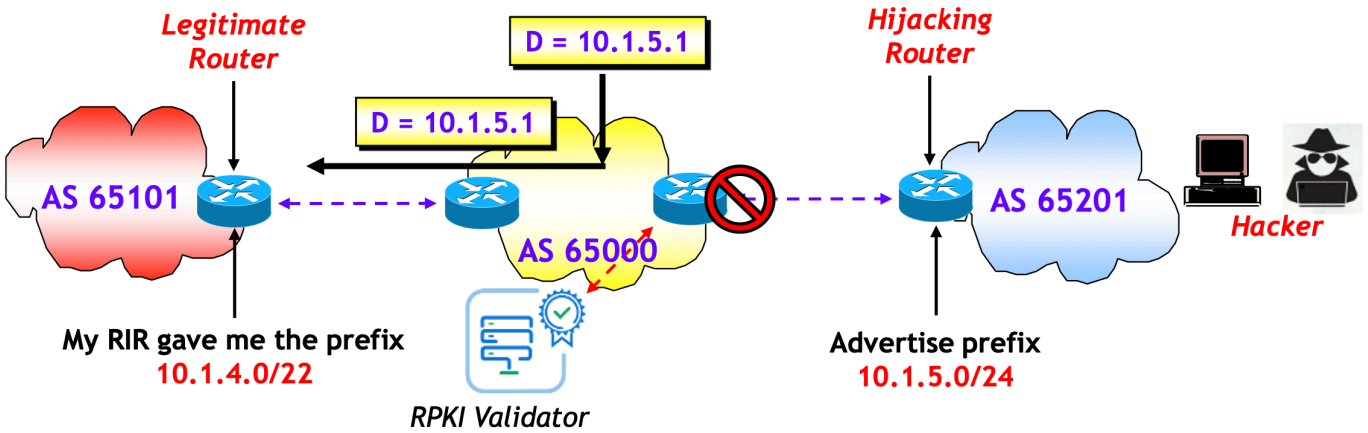
- Tough: in 2018 3ve ad fraud operation created zombie AS to protect malicious IPs from takedown
  - *The Hunt for 3ve*
- Insane: *NSA-Network-Shaping-101*


1. We like it when data goes through <unnamed fiber cable> because we can collect it and find bad guys
YEAH!!! MAKE DATA HAPPEN!
us
SIGINT processing
2. But, oh noes! What happens when a target uses a service where the data *DOESN'T* go through our access? (bad guy has horns for clarity)
<unnamed fiber cable>
redirected traffic
3. CNE midpoint to the rescue!
CNE man
(some server)
4. Now we can see the data, we just need to create a copy, and send that copy through <unnamed fiber cable> so it can get processed into the SIGINT system.

MANRS

Imperial College London

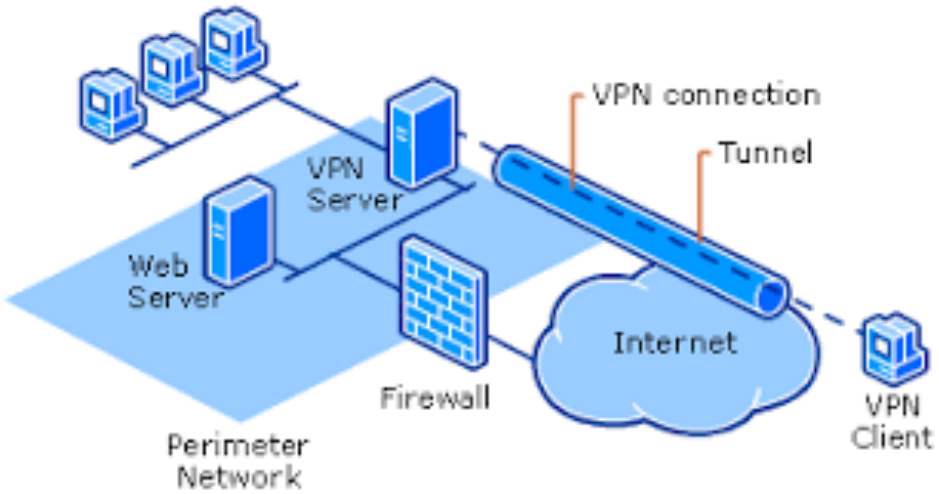
- Mutually Agreed Norms for Routing Security (MANRS)
  - Ongoing effort to secure BGP and prevent
  - Supported by Internet Society and big internet players
  - Best practices for Network Operators (ISPs), Internet Exchange Points (IXPs), Content Delivery Networks (CDNs) and Cloud Providers
- Resource Public Key Infrastructure (RPKI)
  - The idea is to use public key infrastructure and certificates to propagate trust down the Internet address hierarchy



IPsec

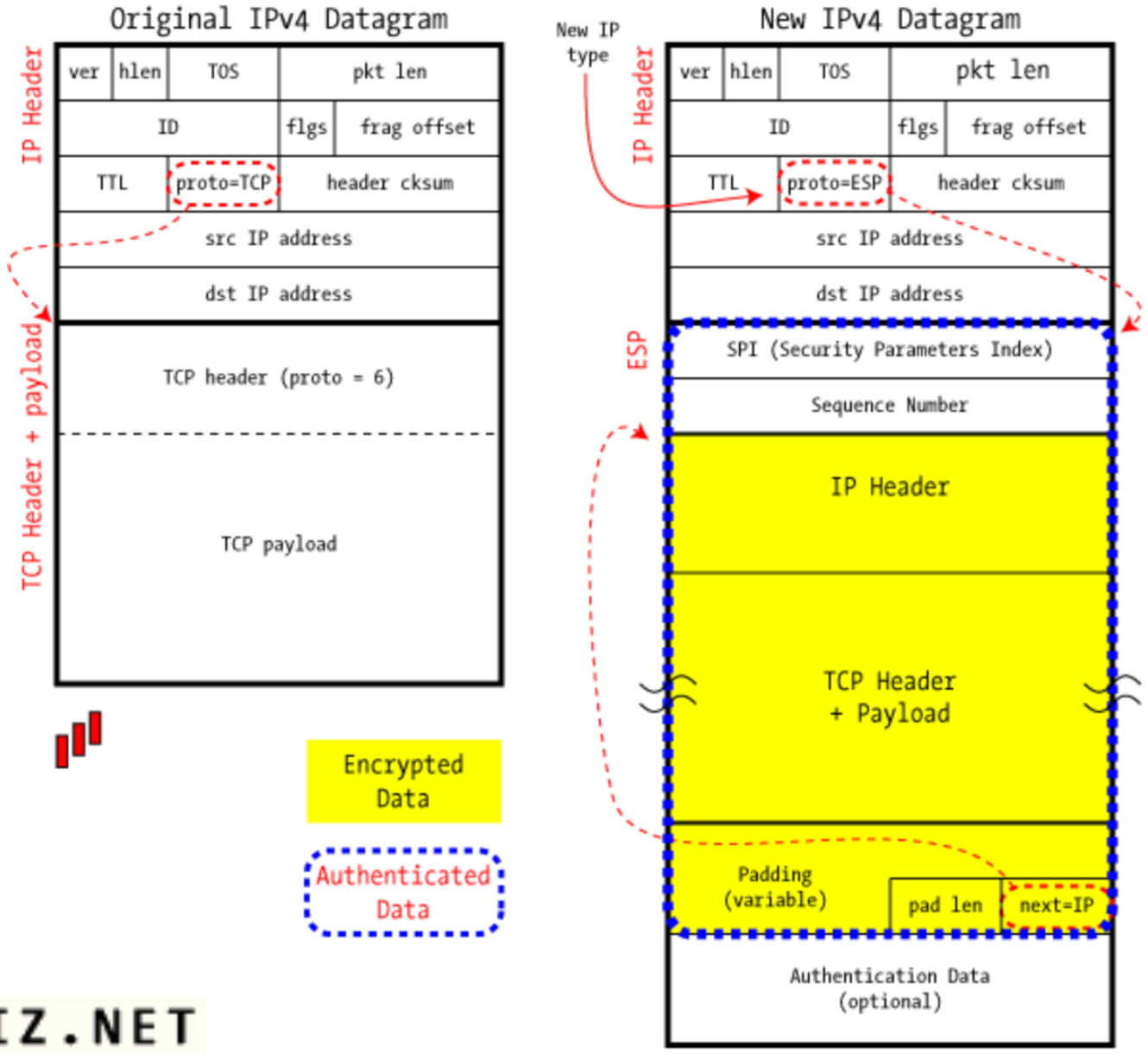
Imperial College London

- *IPsec* adds security to IP protocol
  - Two main protocols: AH and ESP
- Authentication Header (AH)
  - Authentication and integrity of whole packet
    - Does not interoperate with NAT
  - Allows packet inspection, not blocked by firewalls
- Encapsulating Security Payload (ESP)
  - Confidentiality of payload
  - Optional authentication
- Two modes: *Transport* and *Tunnel*
  - Transport mode protects the IP payload only
  - Tunnel mode: protects also the IP header
- ESP Tunnel Mode
  - Most used: to implement VPNs
  - For each connection, a Security Association (SA)
    - IP of origin and destination interfaces to protect with IPsec
    - An identifier: Security Parameter Index (SPI)
    - Encryption and authentication keys
    - Other parameters
  - Gives network layer confidentiality, source authentication, data integrity, replay-attack prevention
  - Hard to configure correctly
  - Hard to connect to the application layer



IPsec in ESP Tunnel mode

Imperial College London

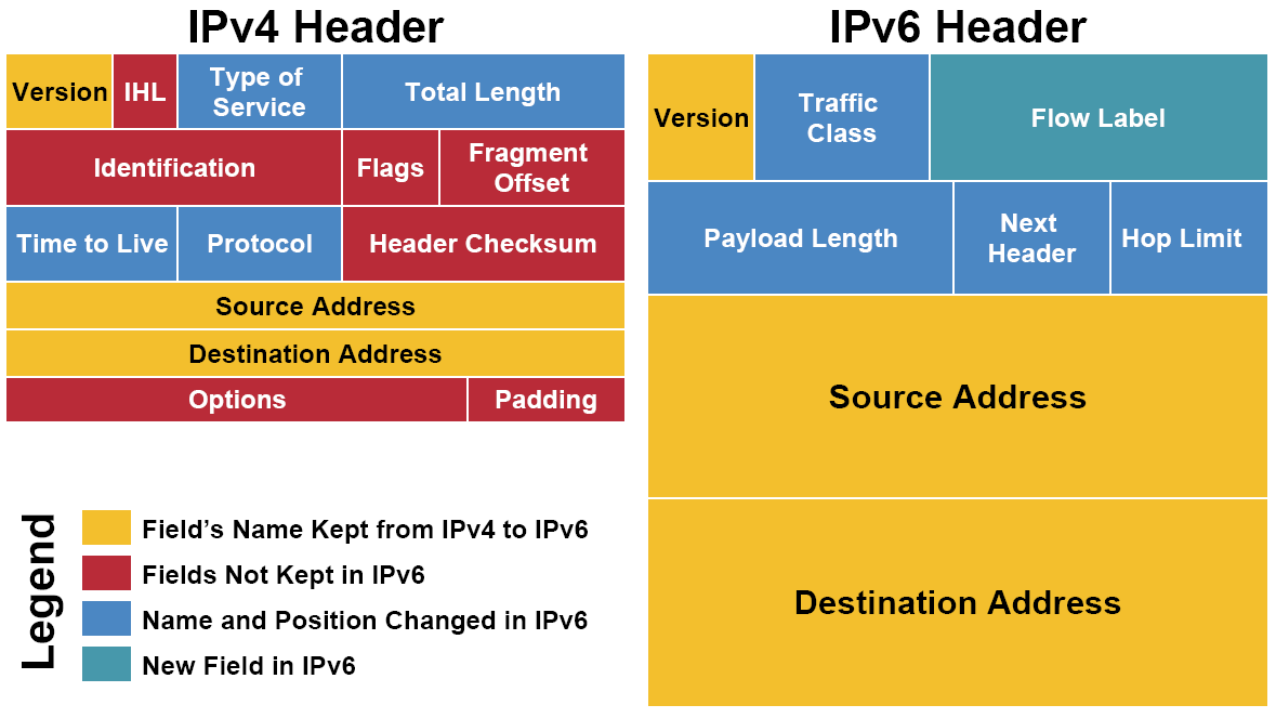


UNIXWIZ.NET

IPv6

Imperial College London

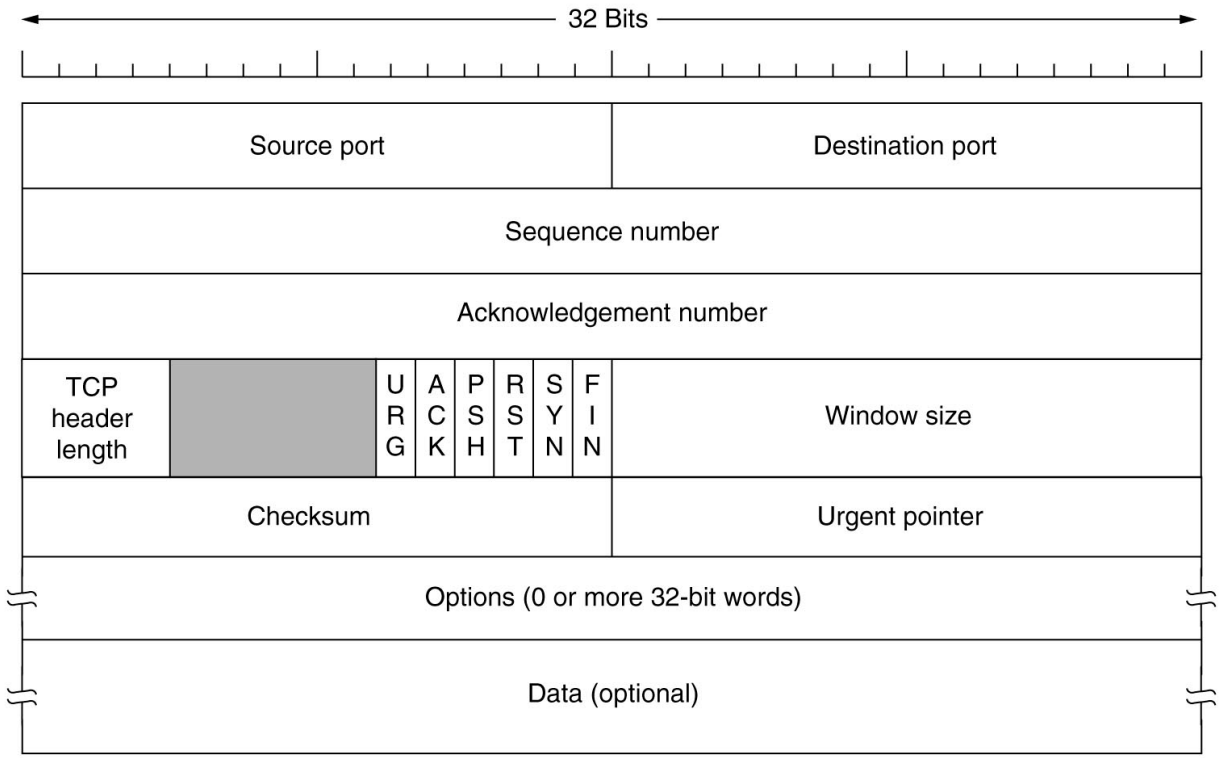
- IPv4: 155.198.140.14 is 32 bits: on 25/11/19 “we run out of IPv4 addresses”
- IPv6: 2001:0000:3238:DFE1:EA06:88FF:FECB:AF19 is 128 bits: no worries of exhaustion
- Comparison with IPv4
  - Address space is large enough that there is no more need for NAT
  - Fewer headers, enables better routing
  - Fragmentation only at the endpoints
    - (ICMP code signals failure due to packet size too big)
  - *Anycast addresses*: send packet to one IP in a range of IPs, assuming they provide the same service
  - Better support for IPSec



Transmission Control Protocol

Imperial College London

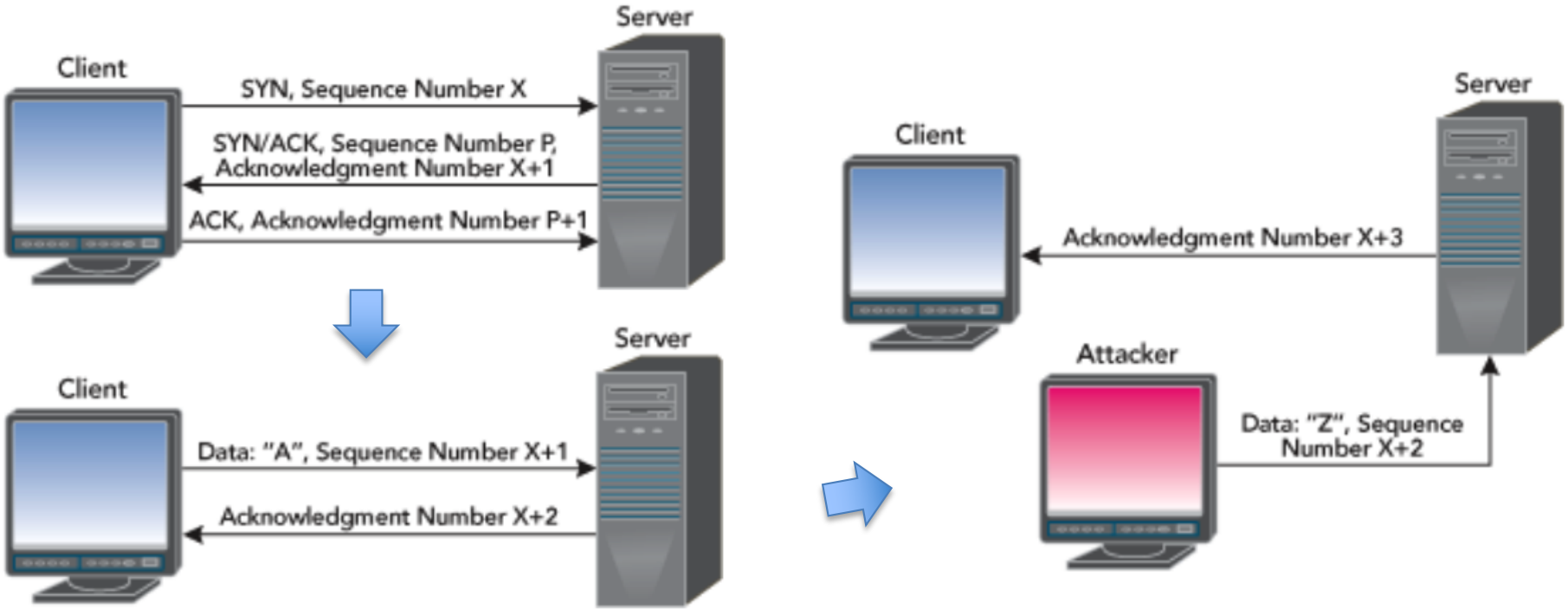
- TCP establishes a reliable connection to a service on the target destination port
  - Source port is chosen at random by OS, to receive responses
  - TCP adds sequence numbers and re-requests lost packets
  - Everything is delivered to the application, and in the right order
- TCP is the channel used to send HTTP data



TCP security issues

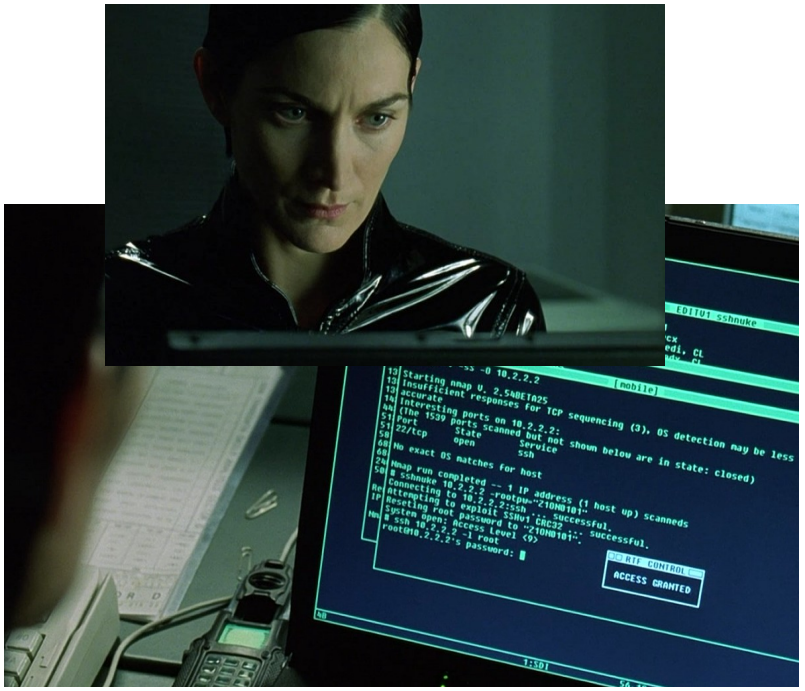
Imperial College London

- TCP state easily accessible
- Sequence numbers are predictable: previous number + bytes exchanged
- MITM attacker can read current sequence number and inject new packets
  - TCP session hijacking
- Off-path attacker can try and guess the right sequence number
  - Blind spoofing attack
  - See recommended reading: *Off-Path Hacking*
- Typical countermeasures
  - Time-delay, then discard race-condition packets
  - Use IDS, HTTPS



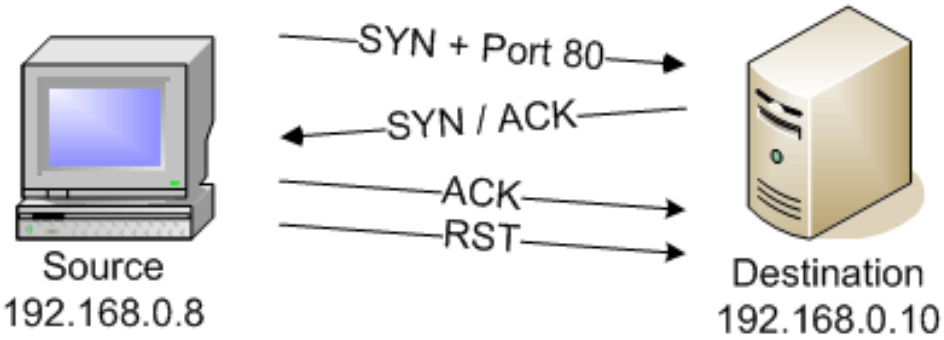
Port scanning

Imperial College London

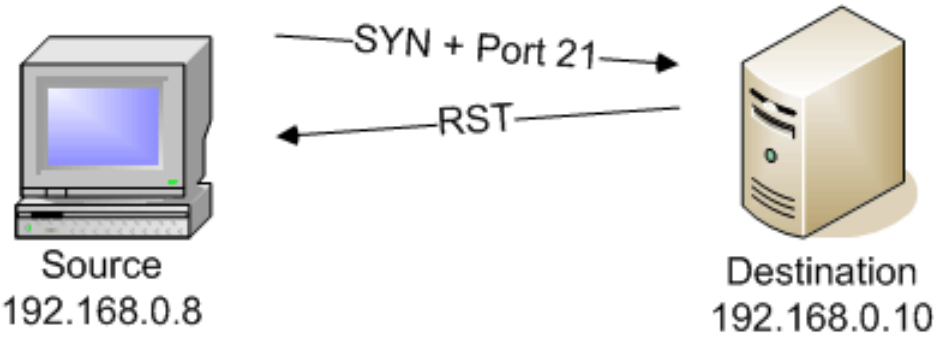


- (Unauthorised) port scanning **may be a crime**
  - Depending on the legal jurisdiction
- We will practice safely on VirtualBox with Nmap
- Different services/protocols require different kind of scans
- Examples
  - TCP `connect()` scan (below)
  - TCP idle scan (next slide)

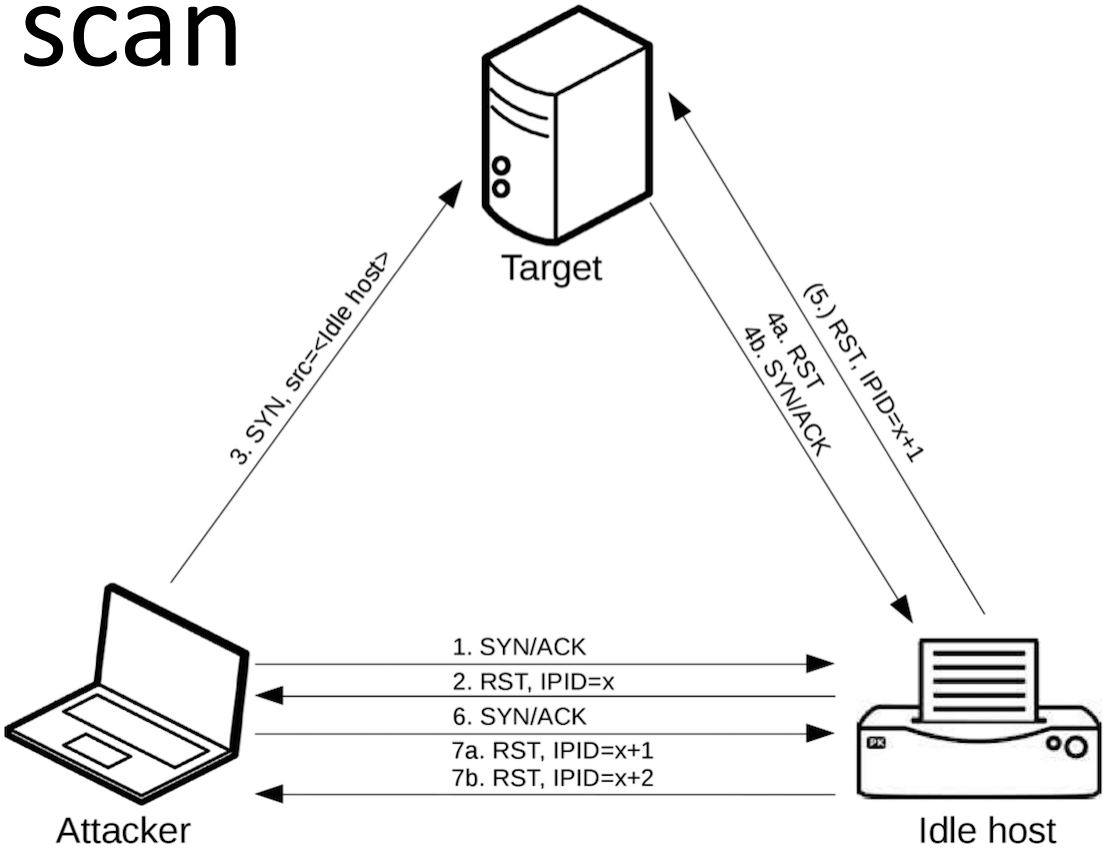
a) HTTP port is open



b) FTP port is closed



TCP idle scan

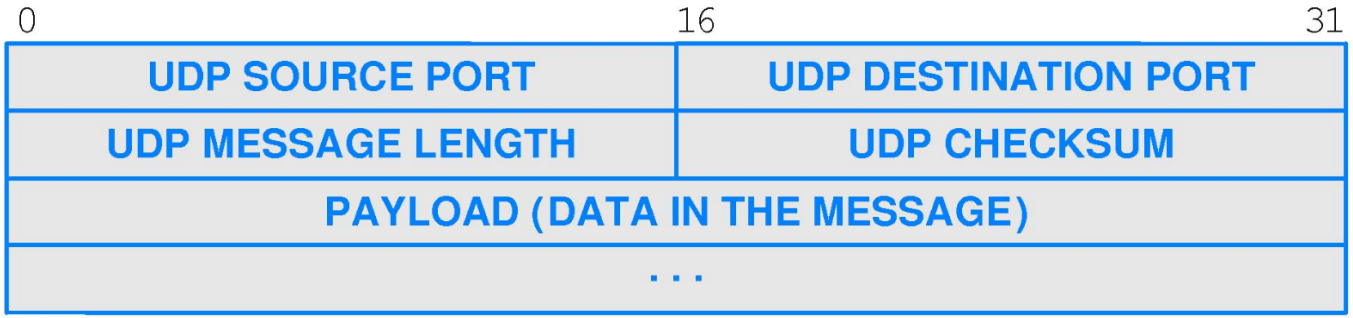


0. Identify an idle host (printer, ftp server, …)
1. & 2. Check available IPID on idle host
3. Spoof source IP when connecting to target
4. Idle host receives scan result it is not waiting for: 4a (closed) or 4b (open)
5. Only if scan result was 4b, idle host sends RST packet, incrementing IPID
6. & 7. Check new available IPID on idle host: x+1 port closed, x+2 port open

User Datagram Protocol

Imperial College London

- *Connectionless protocol*
  - Low overhead, low latency: faster than TCP
  - Can be used for broadcasting, multicasting packets
  - Up to the application layer to make sense of a stream of UDP packets
    - No guarantee data reaches destination: routers may drop UDP packets if there's a conflict
    - No integrity: checksum is optional
    - Packets may be received in different order than they are sent, receiver may also get duplicates
- Usage
  - Streaming media: voice and video
    - WebRTC (RTP) can use UDP or TCP
  - Network management: SNMP, DHCP, DNS
  - Applications that need low-level control on network packets



UDP scans

Imperial College London

- Many different protocols may be run on top of UDP
- Send generic UDP header with no payload to target ports
- If you receive a UDP response, the port is **open**
- If you receive an ICMP error the port is **closed** or **filtered** by a firewall
- If you timeout without a response
  - The port may be **open** and host a service that drops ill-formed packets
  - The port may be **filtered** by a firewall
  - Probe the port again using UDP packets with protocol-specific payloads
- UPD services are harder to scan
  - More time consuming
    - Timeouts for lack of response
    - May take several attempts to resolve **open|filtered** ports
  - Less precise
    - Some UDP custom protocols simply can't be probed

Key TCP/IP threats

Imperial College London

- Host and port scanning
  - Used by hackers during active information gathering
  - They will try to hide the requests within the normal variance of network traffic
- Port sweep
  - One attacker looks for a specific service on many machines
  - More sensitive than port scanning: likely that service is vulnerable (0-day, unpatched)
- Malicious traffic
  - Targeted attacks via network connections
  - Exploitation of networking stack implementation
  - Exfiltration of data
- Distributed Denial of Service (DDoS)
  - Flood a target with extremely high volume of network traffic
  - Attacker can use a botnet
    - Achieve large volume
    - Diversify behaviour to avoid detection
    - Spread attack traffic to preventing takedown

Port knocking

Imperial College London

- Technique to hide a service from port scanning
  1. Sequential or random scan only finds closed ports
  2. Client shares a secret with server that identifies specific ports to probe in a fixed order (3,1,2,4); server replies to last probe (4) with random port (n) where the service will be provided
  3. Client connect to service on the random port
- Can be used legitimately, or to hide backdoors