COMP3052.SEC Computer Security

Session 08: Network Security

Acknowledgements

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...
- Thank you to (amongst others):
  - Michel Valstar, Milena Radenkovic, Mike Pound, Dave Towey, …

This Session

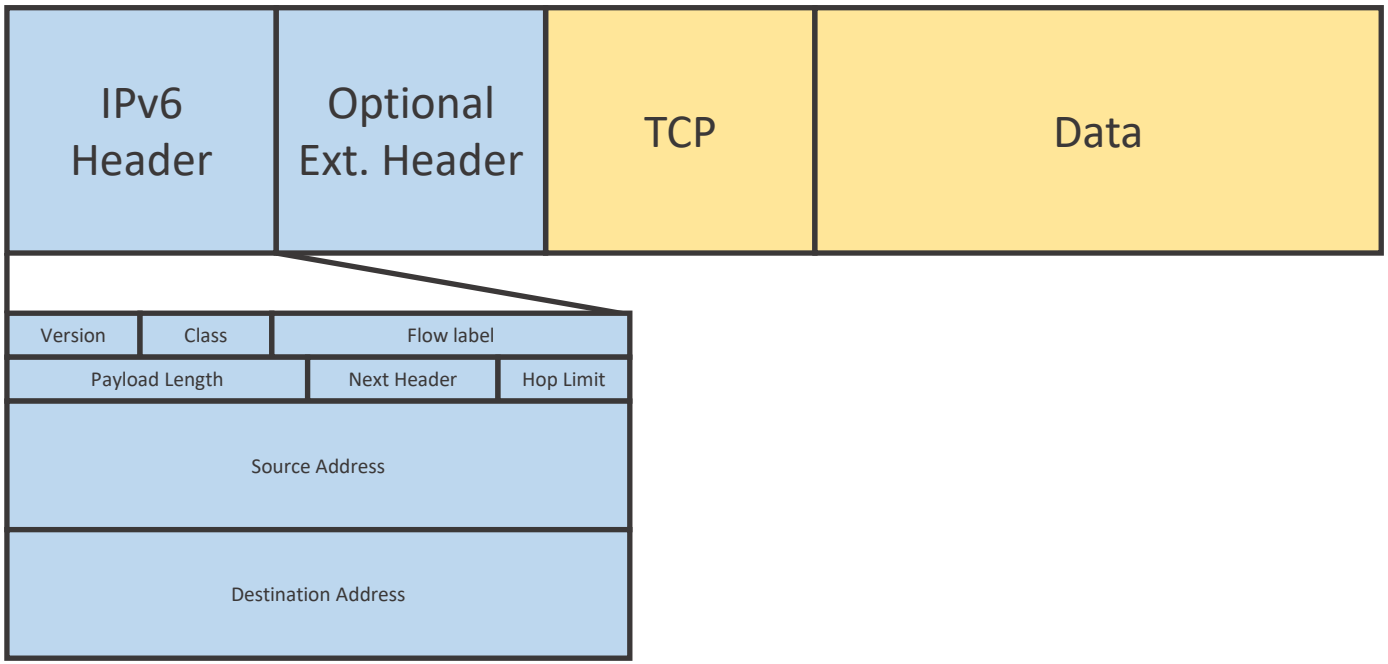
- TCP/IP
- IPSec
- ARP Cache Poisoning
- DNS Spoofing
- Denial of Service Attacks

Two Threat Models

- Passive attackers
  - Eavesdropping / wiretapping / sniffing
  - Traffic analysis
- Active attackers
  - Spoofing attacks (phishing, email)
  - Squatting attacks

TCP/IP - Nesting Headers

- Each protocol carries the protocol in the layer above by appending headers to it



IP Security

- IP is connectionless and stateless
  - Best effort service
  - No delivery guarantee
  - No order guarantee

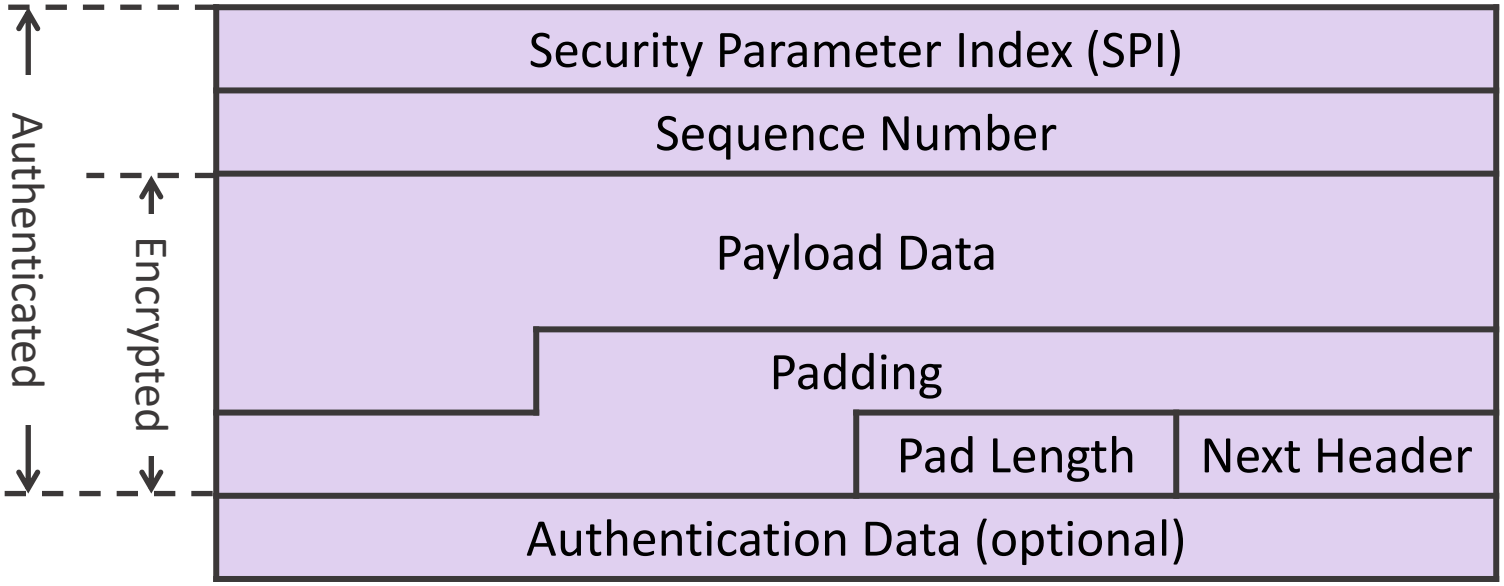
  } Provided by TCP
- IPv4 No guaranteed security support
- IPv6 security support is guaranteed - IPSec

IPSec

- Optional in IPv4, mandatory support in IPv6
- Two major security mechanisms
  - IP Authentication Header (AH)
  - IP Encapsulating Security Payload (ESP)
- Does not contain any mechanisms to prevent traffic analysis

Encapsulating Security Payload (ESP)

- Includes an additional header within the IP packet that describes what encryption and authentication is in use



Transport vs Tunnel Modes

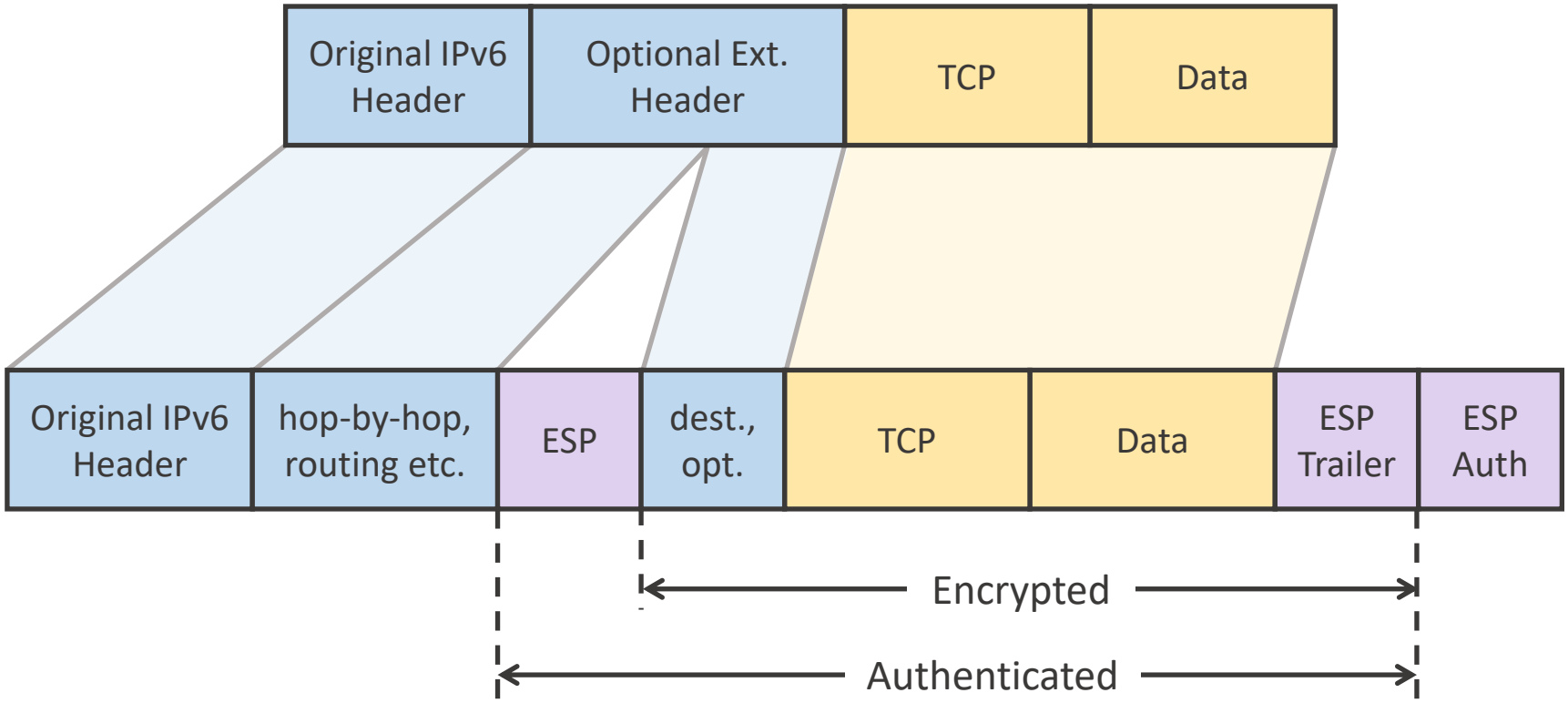
- Transport mode simply encrypts packets, providing host-to-host encryption but using the original header
- Prevents contents being read, but doesn't stop traffic analysis or manipulation of the header

Transport vs Tunnel Modes

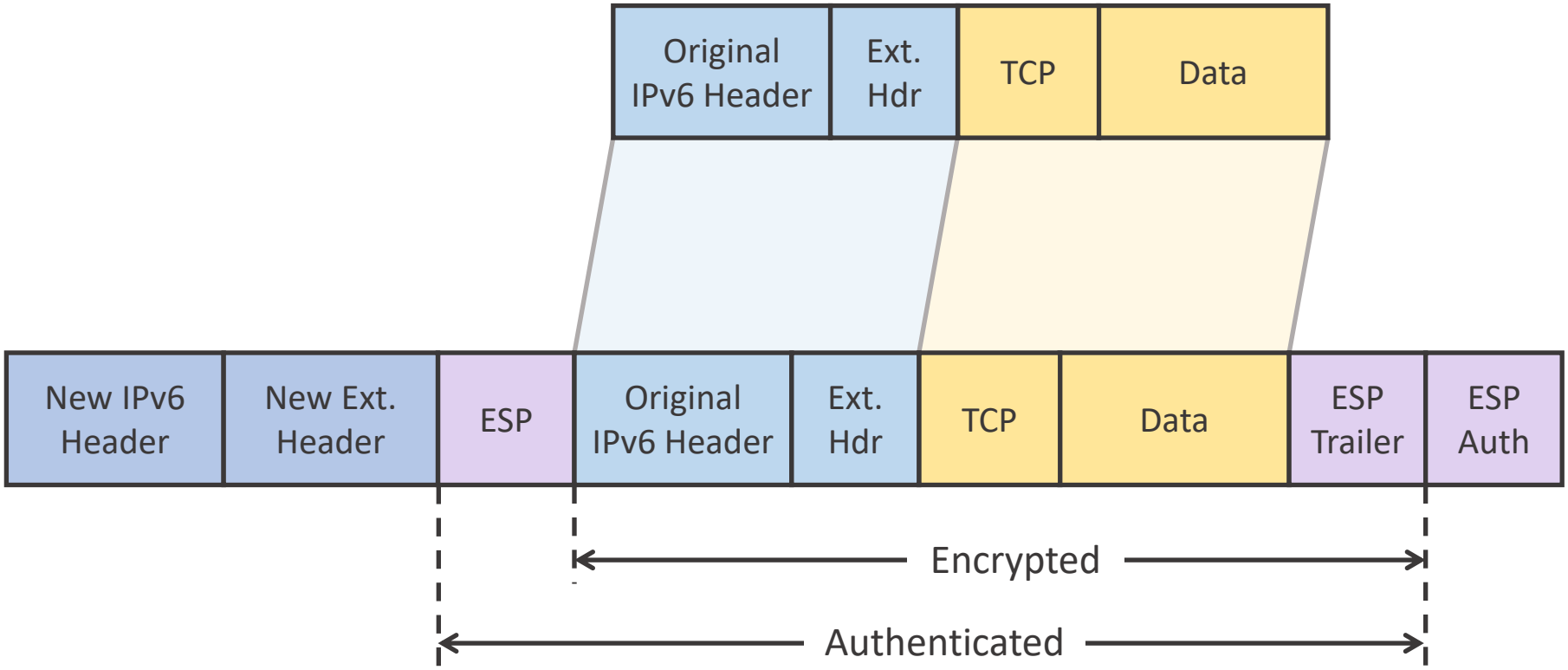
- Tunnel mode (usually gateway-to-gateway) protects some segment of a channel with encryption
- Provides some resistance to traffic analysis, and completely protects manipulation of the payload
- VPNs are commonly implemented this way

ESP in Transport Mode

- ESP uses either Transport or Tunnel modes

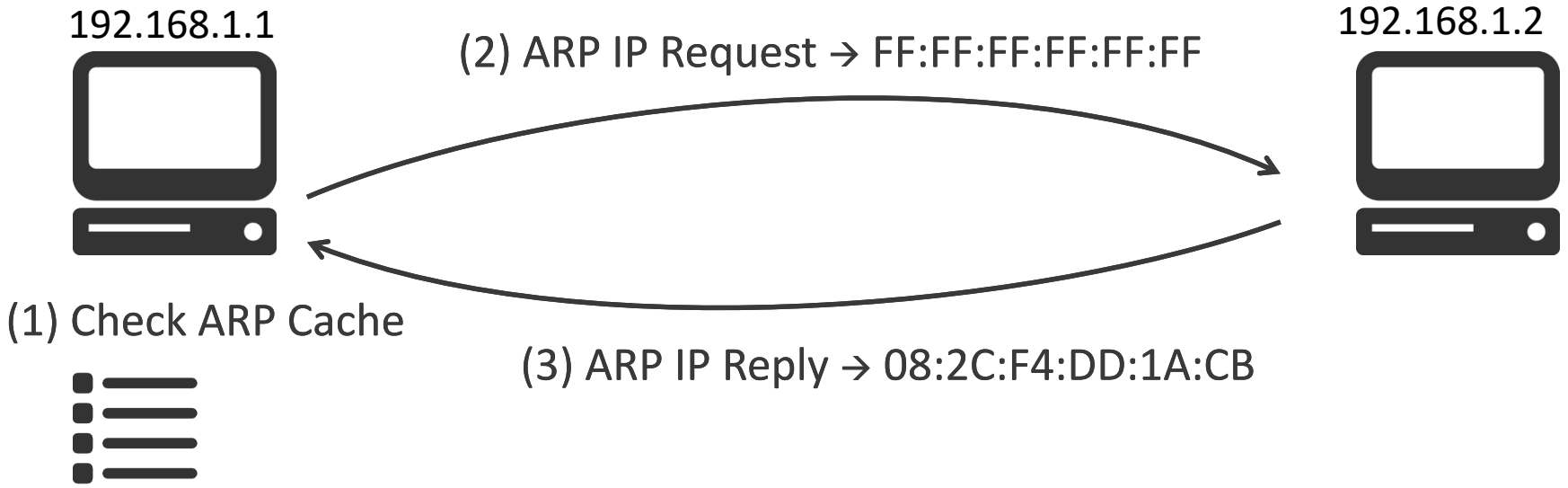


ESP in Tunnel Mode



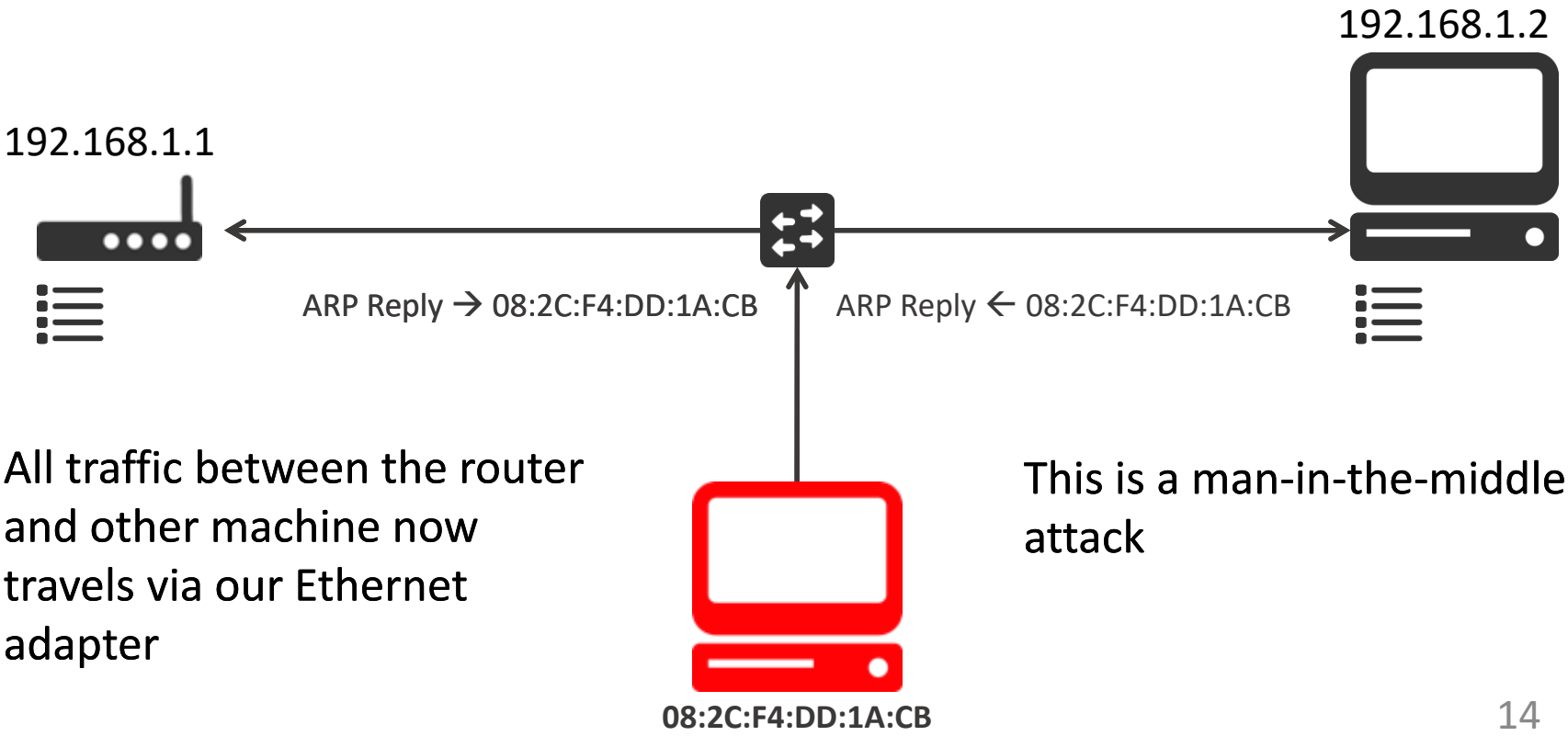
Address Resolution Protocol (ARP)

- ARP is a protocol used (in IPv4) to obtain physical MAC addresses for given IPs
  - It is used prior to constructing IP and TCP packets for communication
  - Network layer

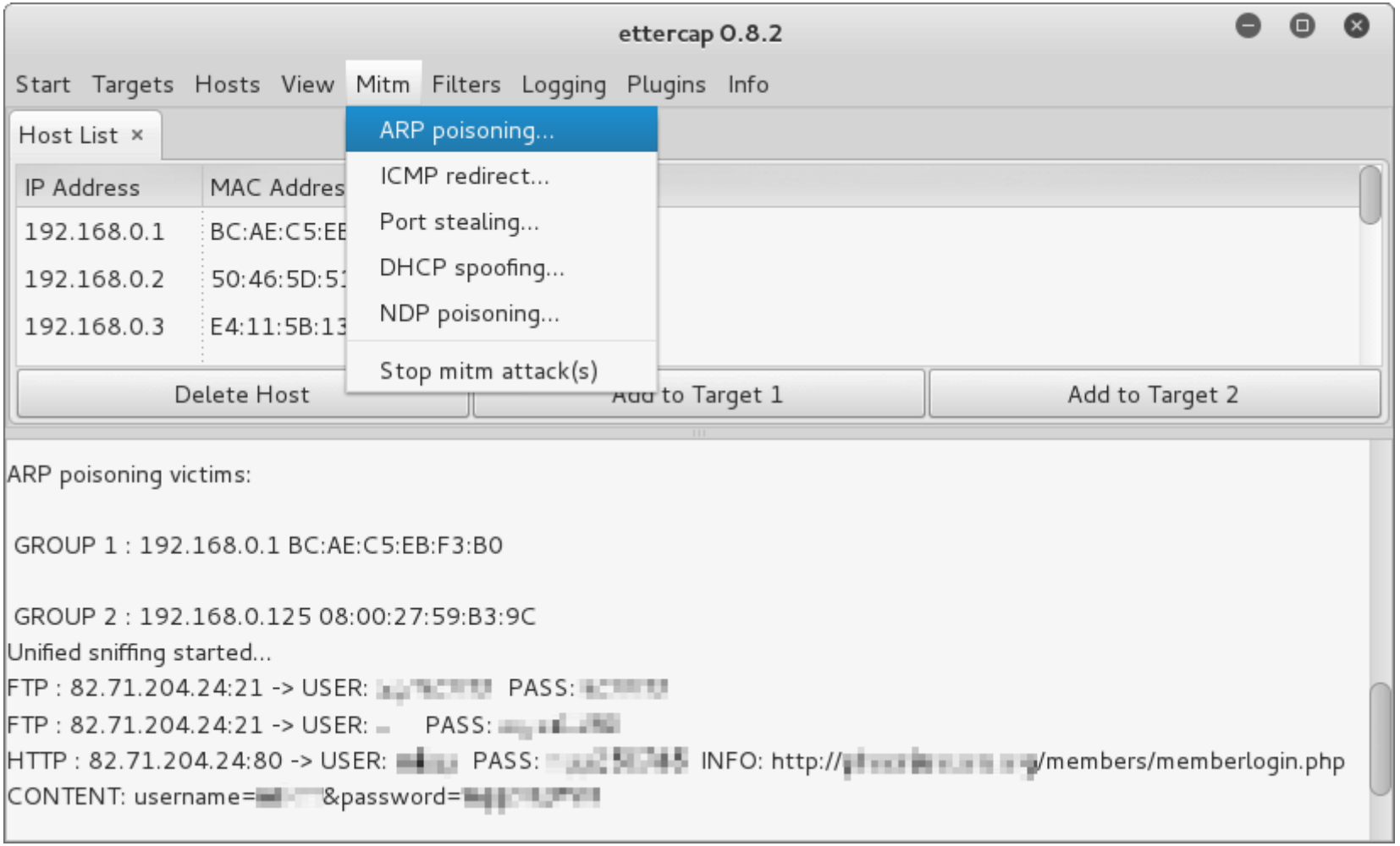


ARP Cache Poisoning

- We can simply send an unrequested ARP reply, and overwrite the MAC address in a host's ARP cache with our own



ARP Cache Poisoning

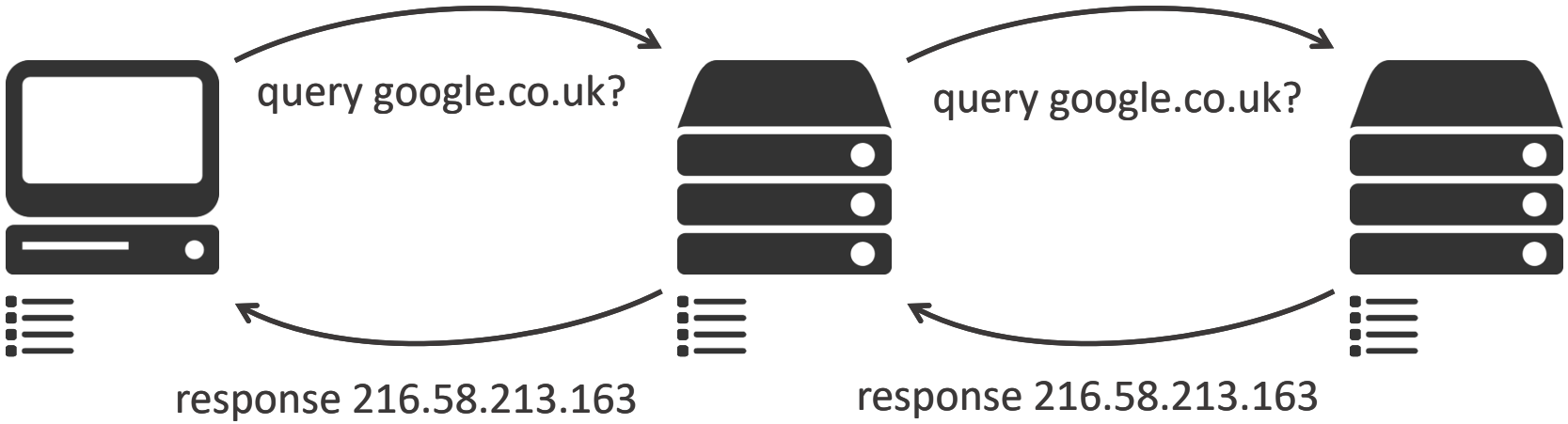


ARP Protection

- Some OSs ignore unsolicited ARP requests, or can be configured to use ARP differently
- Some software, such as intrusion detection packages, will include ARP spoofing detection
  - Maintain a log of current MAC:IP assignments and ARP requests / replies
  - Allows us to spot suspicious messages such as unsolicited ARP replies

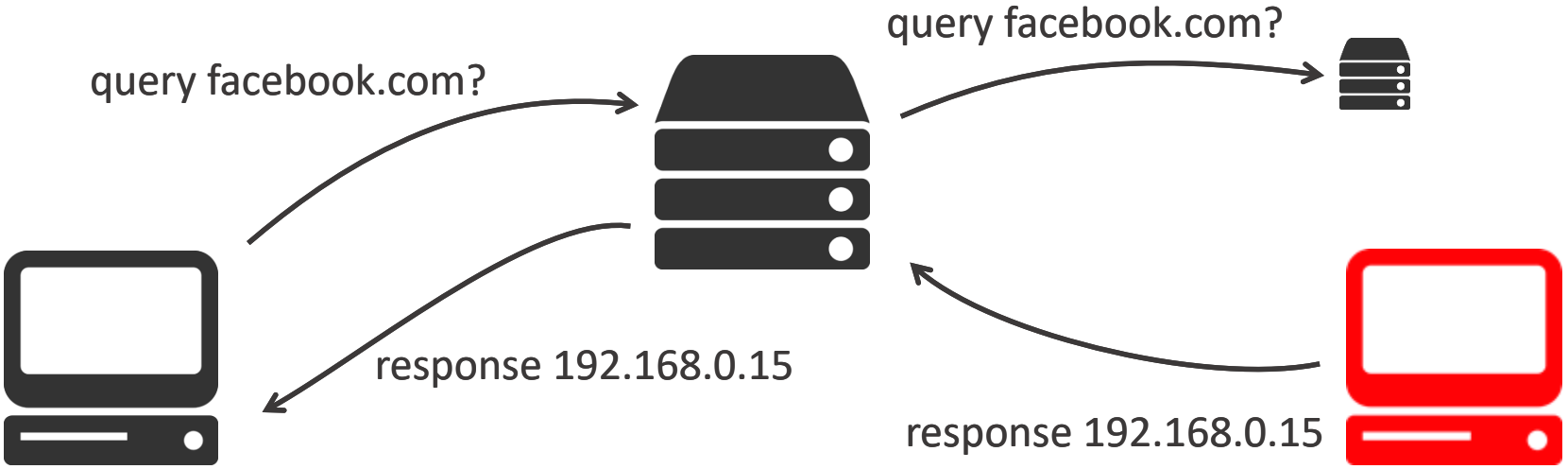
Domain Name System (DNS)

- DNS translates domain names into IP addresses
  - E.g. nottingham.ac.uk → 128.243.80.167
- DNS packets are UDP
  - Stateless, on the transport layer
- DNS resolvers will cache the IPs for a while



DNS Spoofing

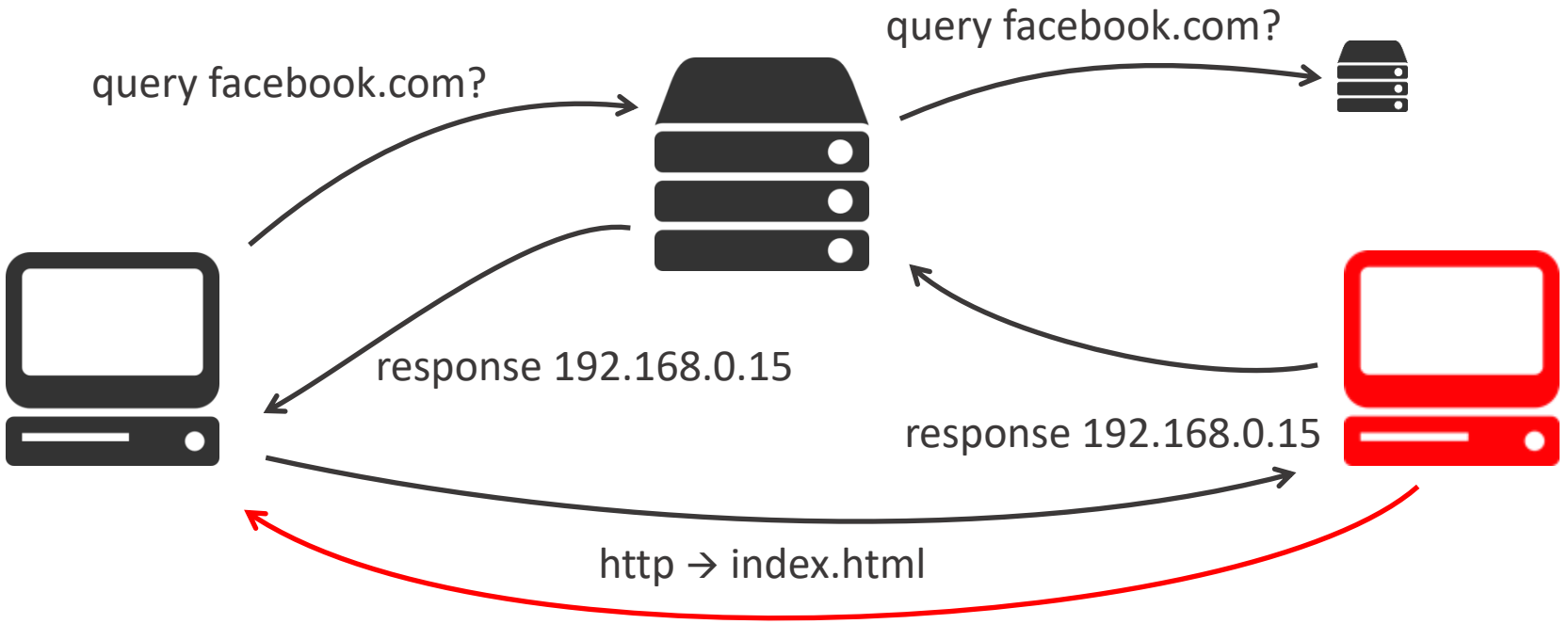
- If we can poison the cache of a nameserver people are using, we can replace a website lookup with our IP



- Can be achieved through prior ARP cache poisoning, a reply flood or a Kaminsky attack

DNS Spoofing

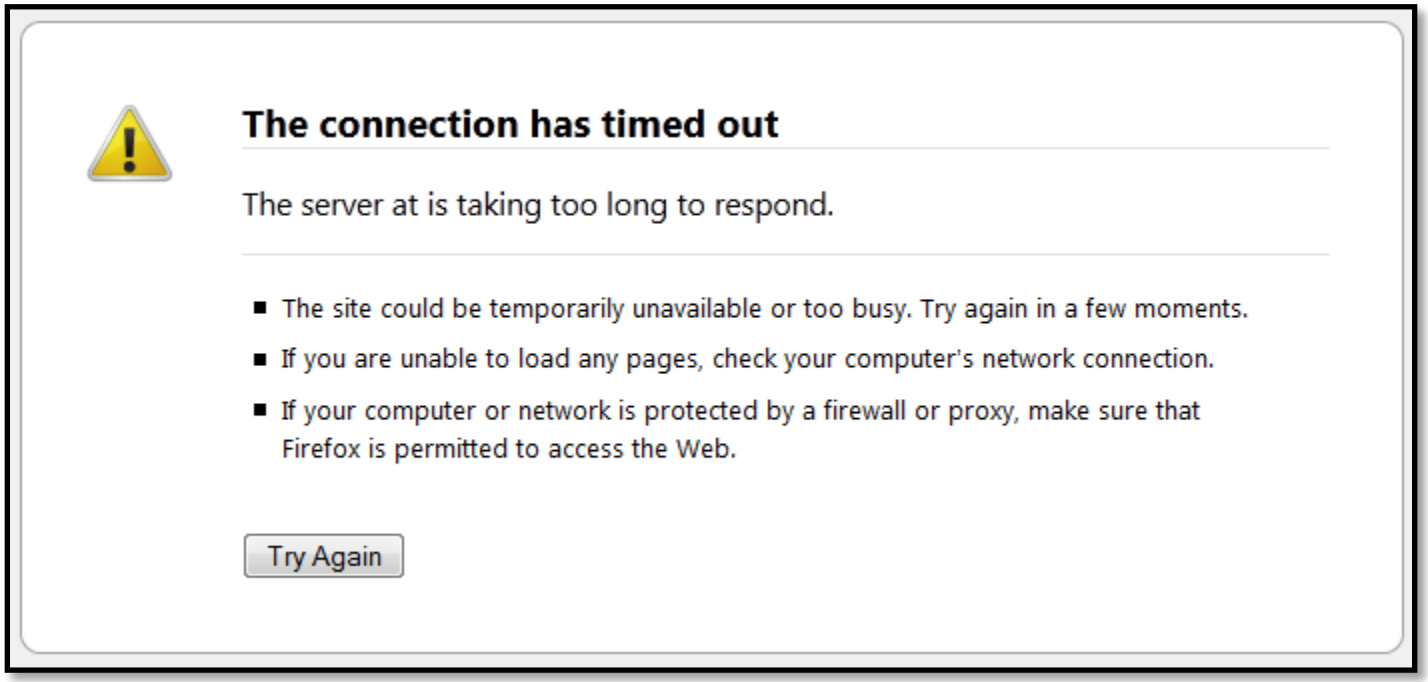
- If we can poison the cache of a nameserver people are using, we can replace a website lookup with our IP



index.html{ <html><head><script src="cryptowall.js"/></head>
<body onload="ransom()"/></html> }

DNS Protection

- Random query numbers help protect against spoof replies
- Since the Kaminsky attack, most resolvers now randomise the source port too
- DNSSEC aims to tackle DNS exploits by authenticating the name server and providing integrity for the messages



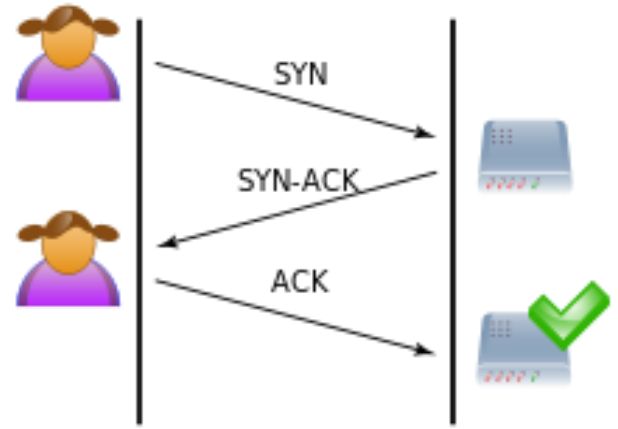
Denial of Service

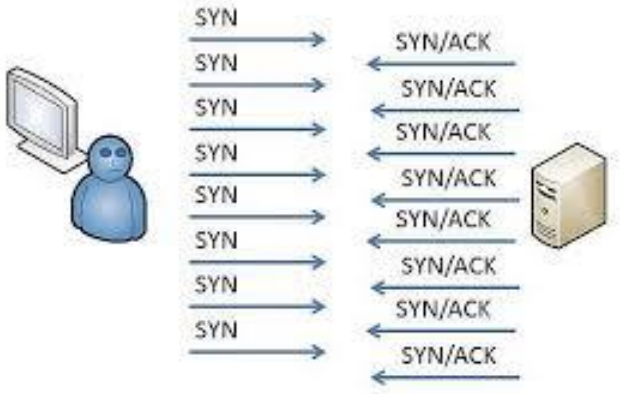
Denial of Service Attacks

- A denial of service attack is an attempt to make a machine or network resource unavailable to its authorised / intended users
- This will usually involve flooding a machine with enough requests that it can't serve its legitimate purpose
  - E.g. Ping flood
- A distributed denial of service occurs where there is more than one attacking machine

Simple Attack Example

- TCP Syn Flooding
  - Attacker initiates a genuine connection but then immediately breaks it
  - Attacker never finishes 3-way handshake
  - Victim is busy with the timeout
  - Attacker initiates large number of syn requests
  - Victim reaches its half-open connection limit
  - Denial of service

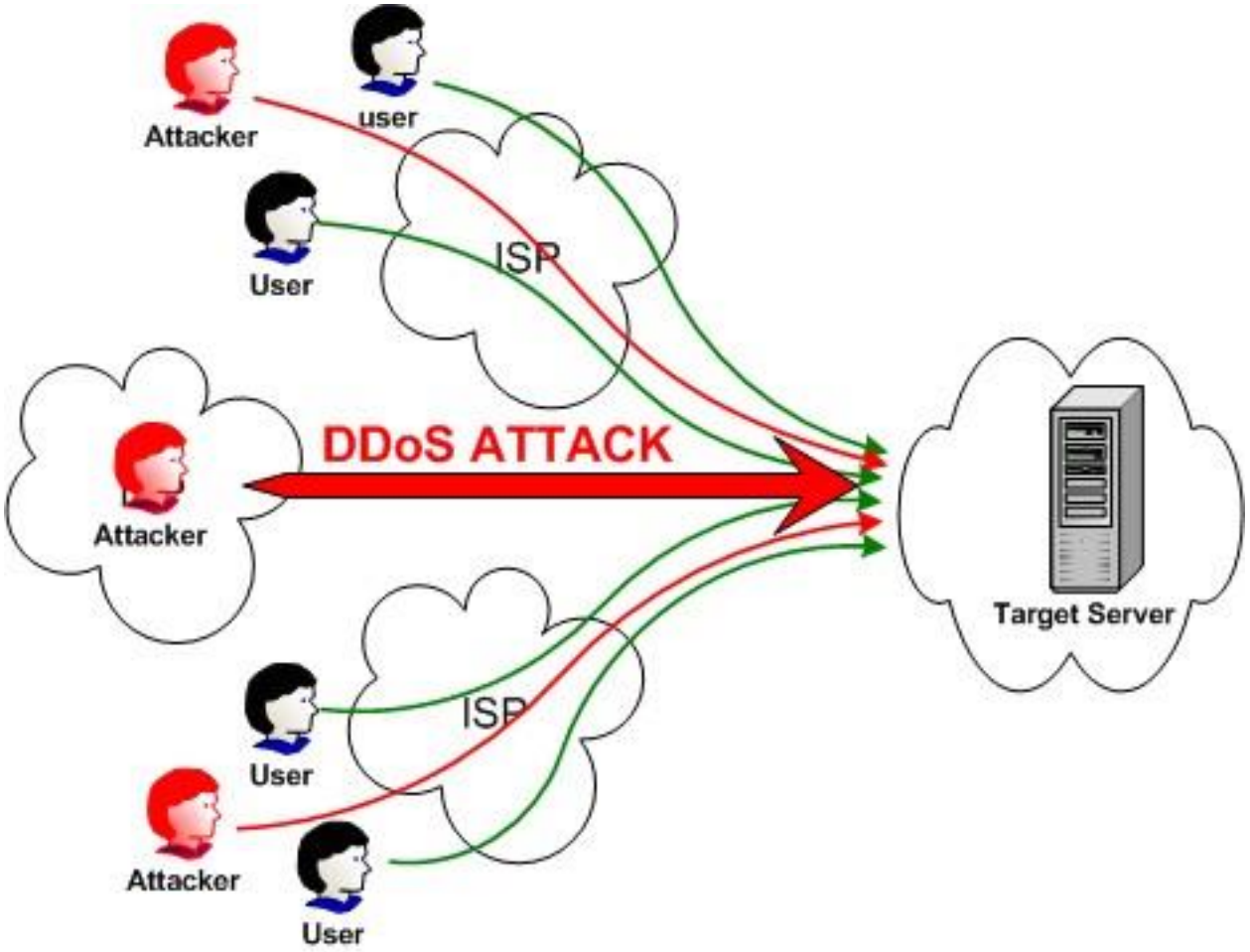




Low and Slow

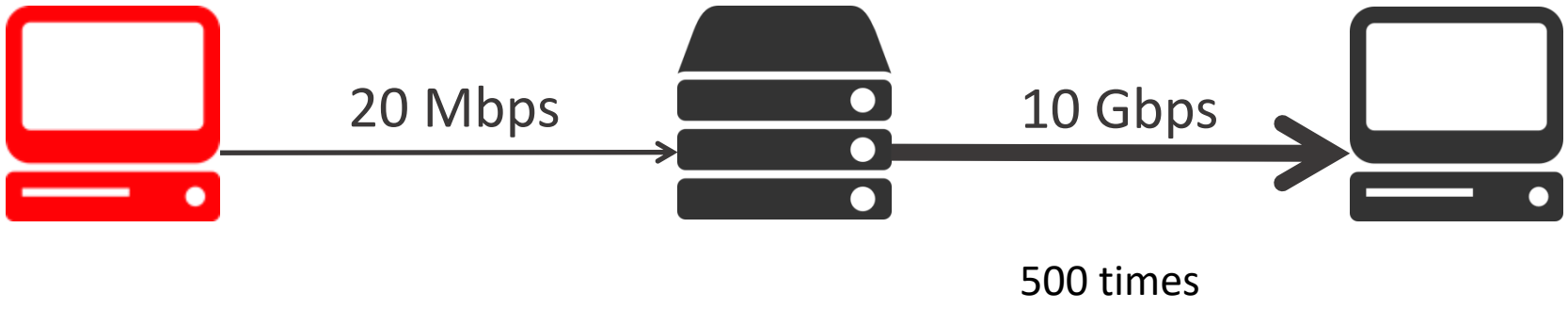
- Slowloris
  - Open numerous connections to a server
  - Begin an HTTP request, but never actually finish it
- R-U-Dead-Yet?
  - Similar to slowloris
  - Begin an extremely long HTTP POST, send tiny amounts at a time

Distributed Denial of Service (DDoS) Attack Example



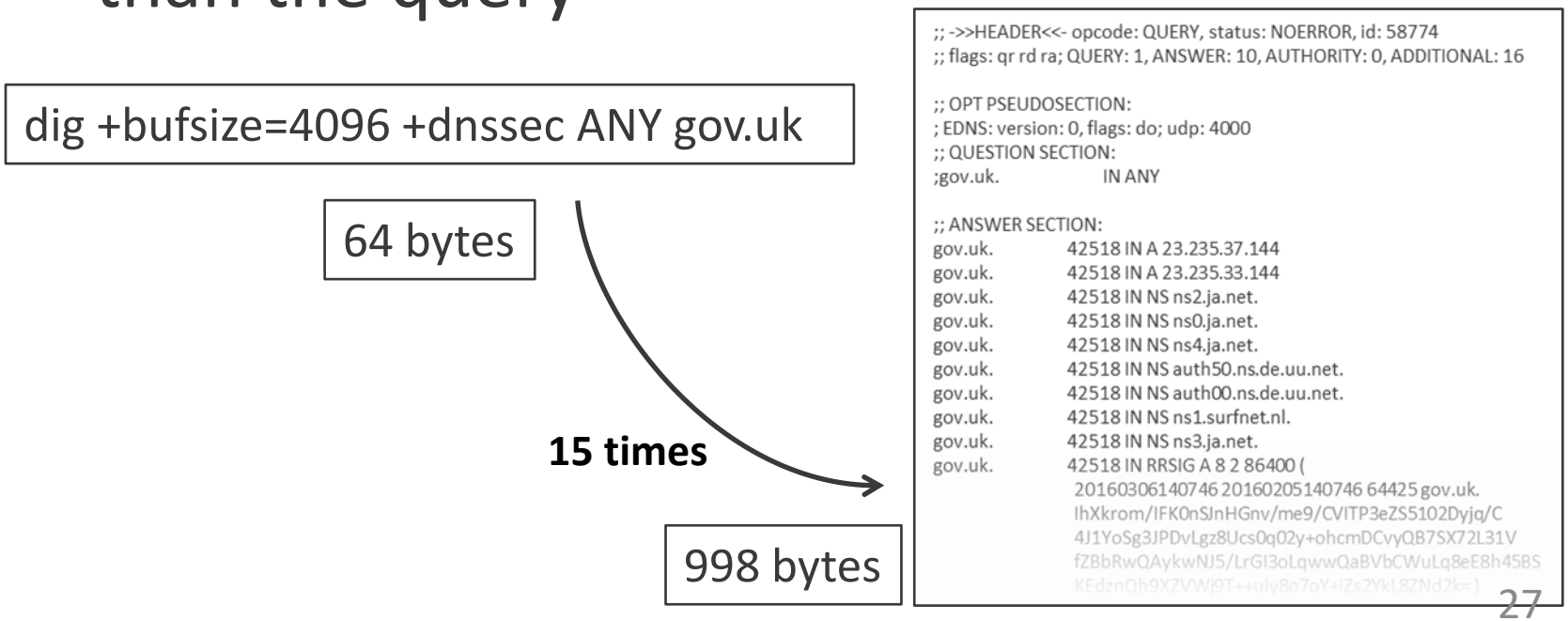
Amplification Attacks

- Regular attacks are attacker's bandwidth vs attacker's target's
- Amplification attacks utilise some aspect of a network protocol to increase the bandwidth of an attack



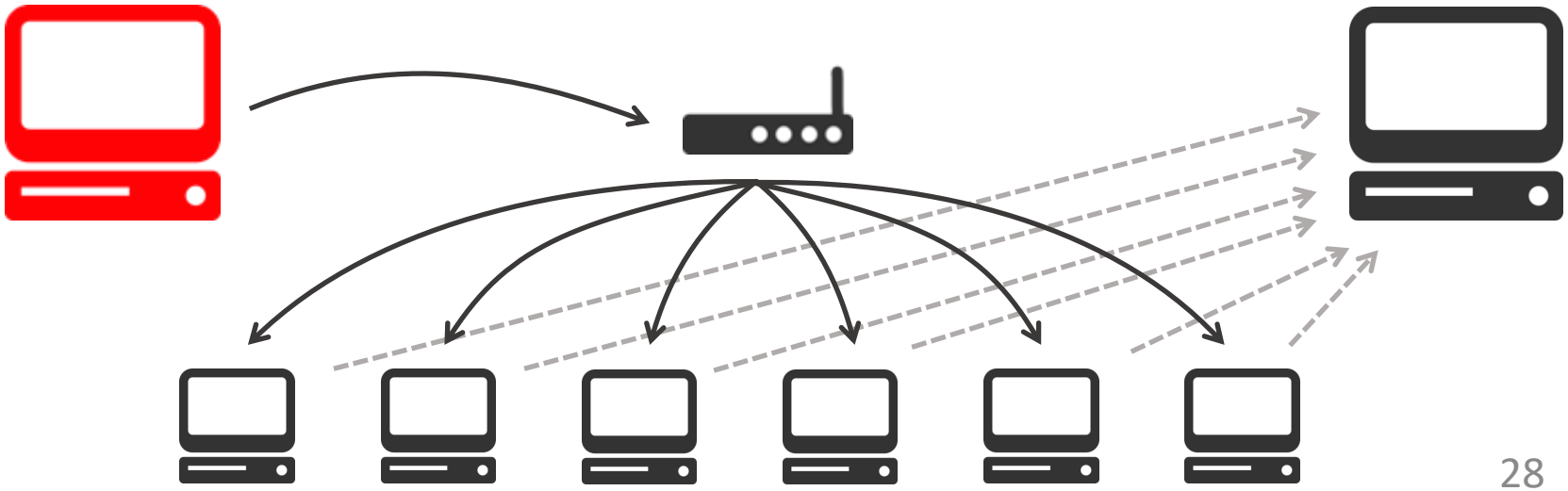
DNS Amplification

- Recursive resolvers respond to DNS queries then return a response
- This response can be many times larger than the query



Smurf and Fraggle Attacks

- Smurf attacks broadcast an ICMP Ping request to a router, but with a spoofed IP belonging to the victim
- A Fraggle attack is identical in principle, using UDP echo packets



Summary

- TCP/IP
- IPSec
- ARP Cache Poisoning
- DNS Spoofing
- Denial of Service Attacks

Gollman Chapter 16 (& 17?)