School of Computing
FACULTY OF ENGINEERING & PHYSICAL SCIENCES

UNIVERSITY OF LEEDS

COMP3911 Secure Computing

8: TCP/IP Networking Threats

Nick Efford

https://comp3911.info

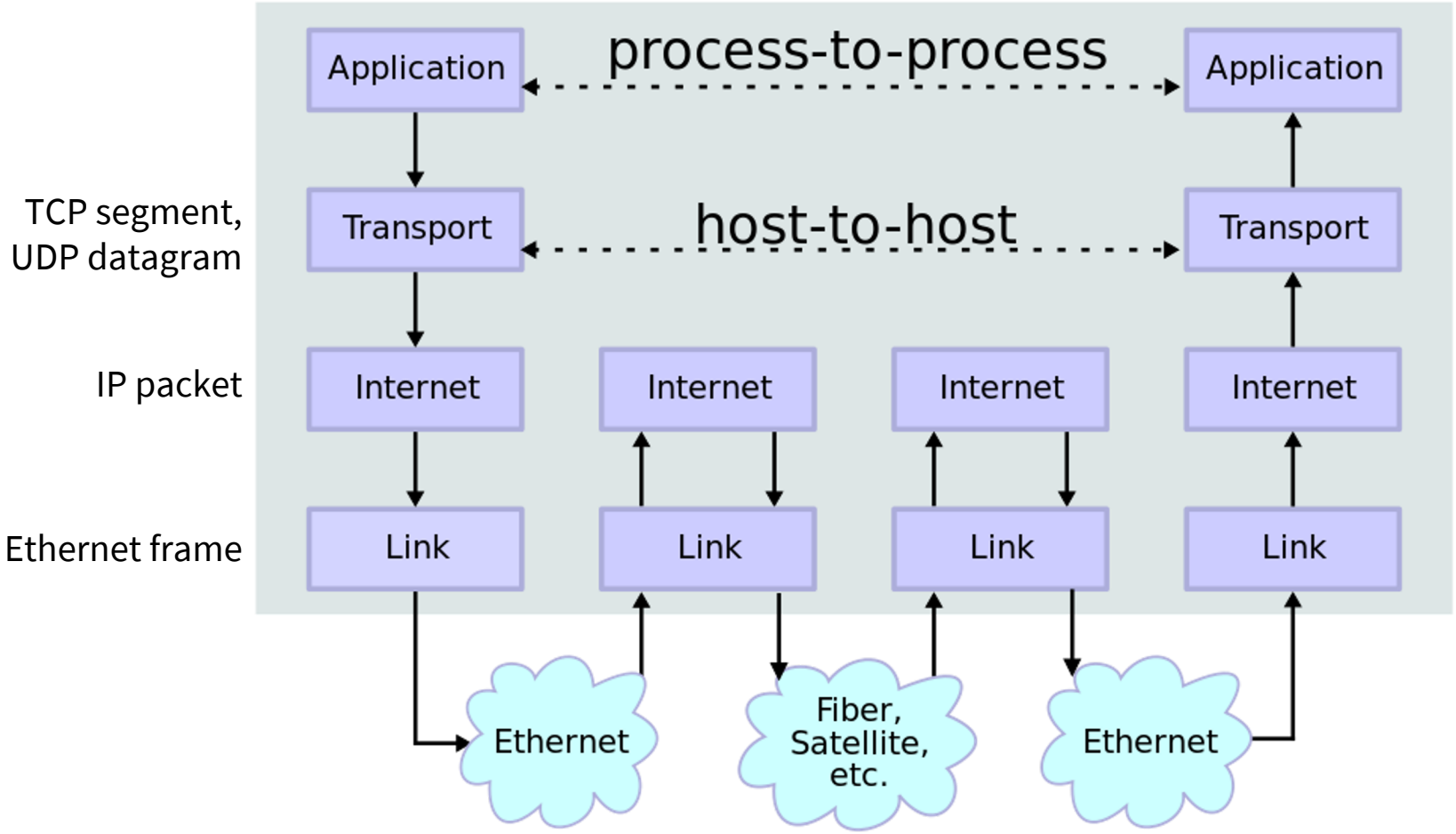
Objectives

UNIVERSITY OF LEEDS

- To review the layered network model and relevant protocols operating in the Internet and Transport layers
- To consider how those protocols can be exploited to probe and attack systems

Network Protocol Stack

UNIVERSITY OF LEEDS



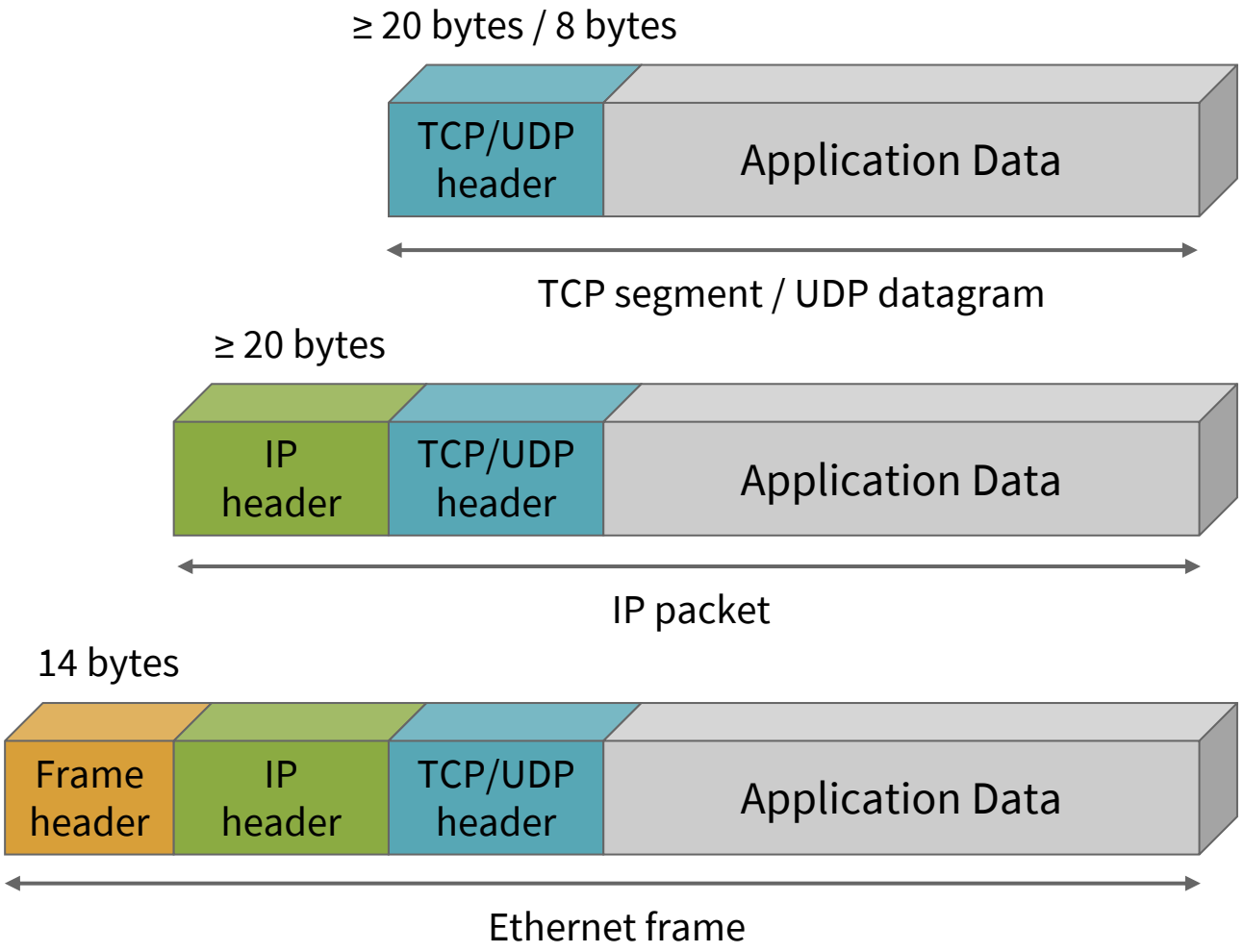
IP Packet Payloads

UNIVERSITY OF LEEDS

- Transmission Control Protocol (TCP)
  - Provides reliable bytestream connection
  - Uses **sequence numbers** to order segments
  - Retransmits segments where necessary
- User Datagram Protocol (UDP)
  - No promise of reliable delivery
- Internet Control Message Protocol (ICMP)
  - Control of routing
  - Error reporting

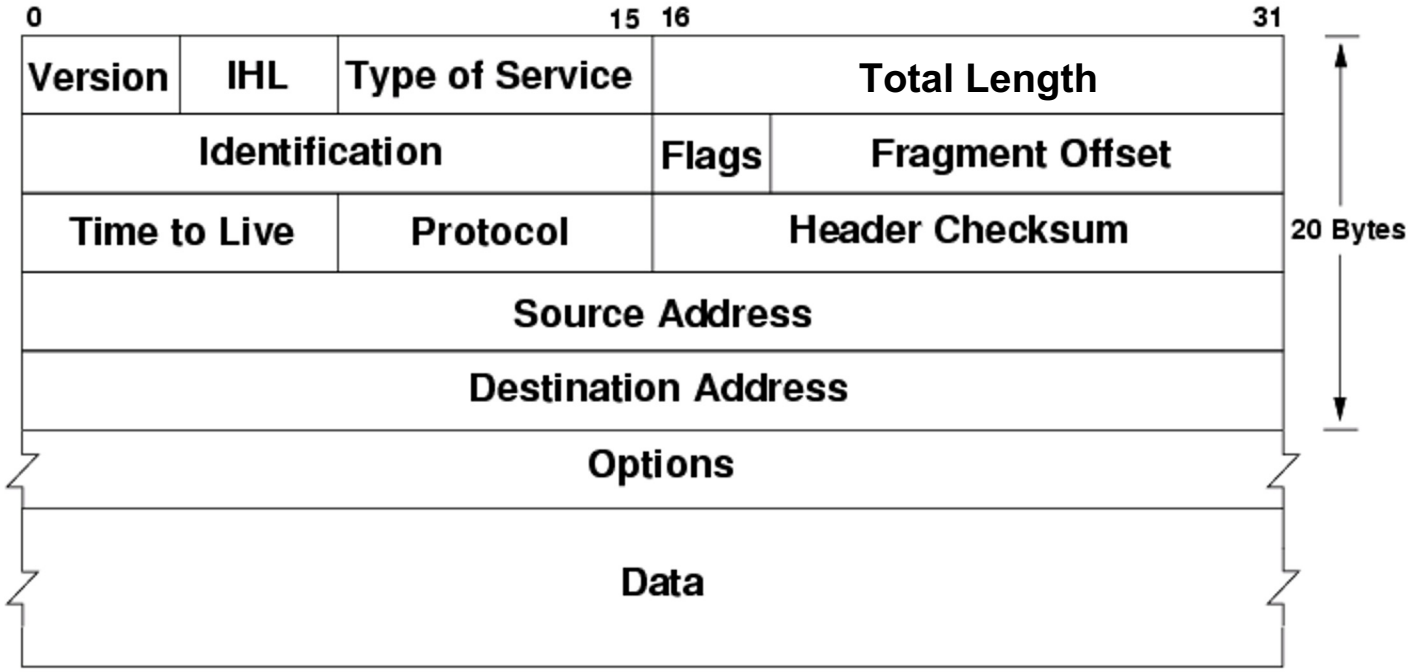
TCP & UDP Data Packaging

UNIVERSITY OF LEEDS



IPv4 Header

UNIVERSITY OF LEEDS



Protocol field identifies payload: TCP, UDP or ICMP

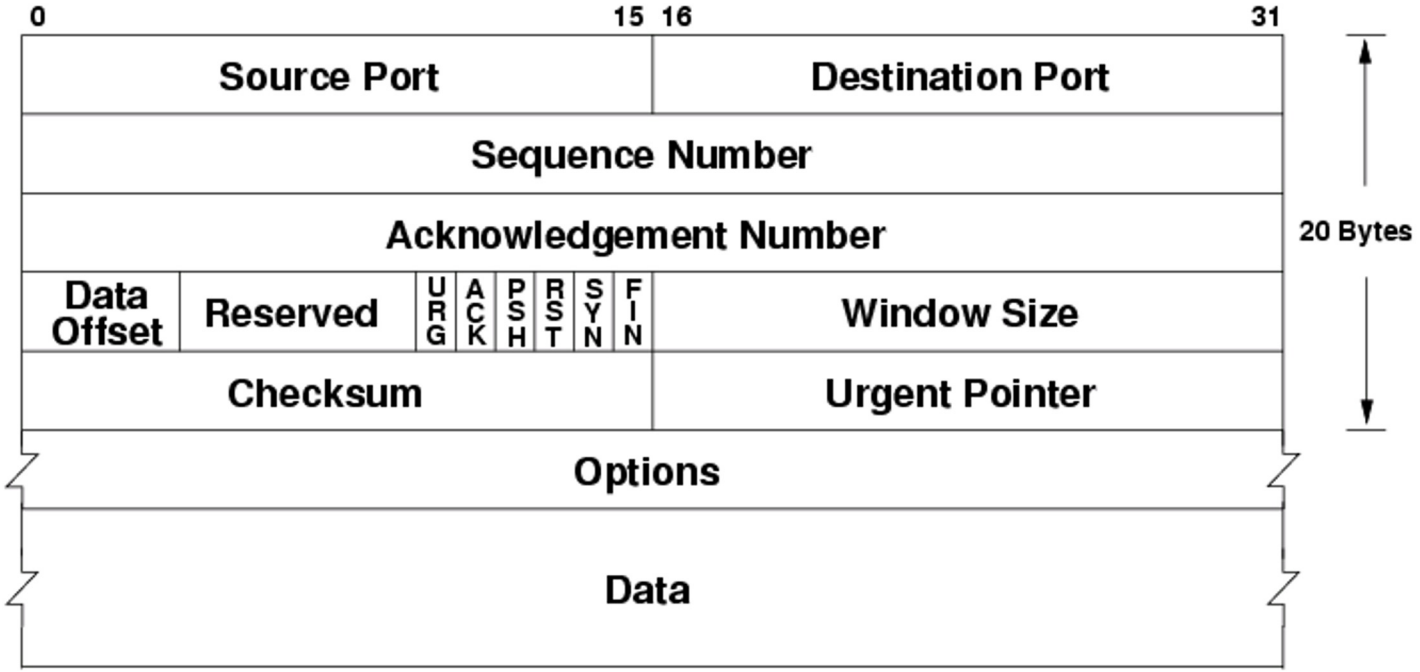
Fragmentation

UNIVERSITY OF LEEDS

- Occurs when IP packet needs to traverse a network with MTU smaller than packet size
- Reassembly is possible because
  - All fragments from same packet have same ID
  - Each fragment stores its offset into the original, unfragmented packet
  - Each fragment knows if more fragments follow it
- Attacker might *deliberately* break a malicious packet into fragments – e.g., to try to fool an IDS

TCP Header

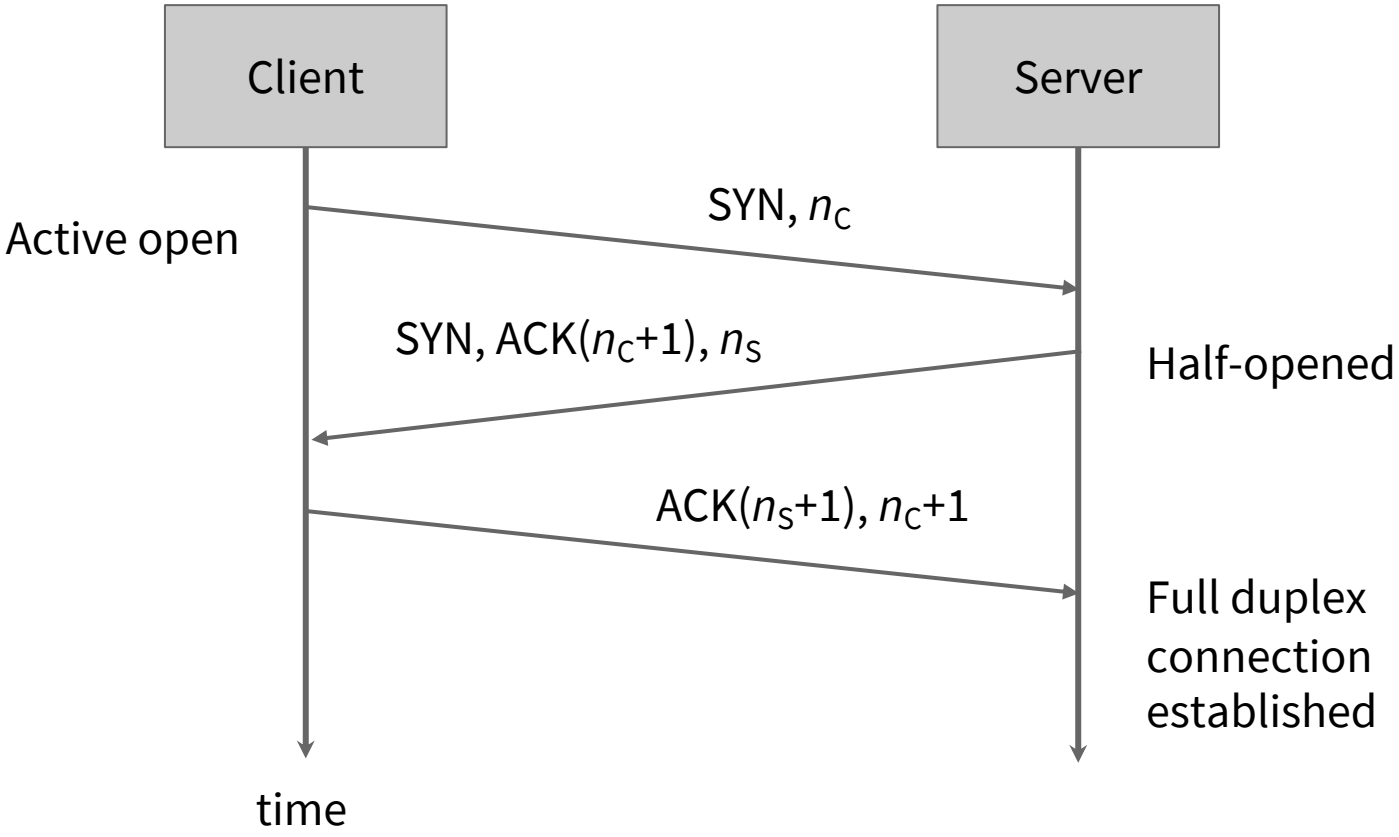
UNIVERSITY OF LEEDS



6 reserved bits can be used by attackers as a **covert communications channel** – though this requires installation of a **rootkit** on victim's machine, and a large number of small segments must be exchanged for it to be effective…

TCP Handshaking

UNIVERSITY OF LEEDS



Security Perspective

UNIVERSITY OF LEEDS

- Protocols were not designed with security in mind
- No guarantees of confidentiality, authenticity, integrity
- Protocols are easily abused
  - To conduct network reconnaissance
  - To actively attack victims

Intelligence Gathering

UNIVERSITY OF LEEDS

ICMP echo requests (‘ping sweep’)

- Live hosts will issue ICMP echo replies
- ‘Host unreachable’ reply from router if no host
- Typically blocked by networks

TCP scans

- Full connection (noisy)
- Half-open connection (‘SYN scan’)
  - Open ports respond with SYN-ACK, closed with RST
  - Attacker tears down with RST, so logs tend to show lots of SYNs and RSTs

Stealthier TCP Scanning

UNIVERSITY OF LEEDS

ACK scan

- Not blocked by older stateless firewalls
- Open and closed ports respond with RST; filtered ports give no response
- Logs: many ACKs without corresponding SYNs

FIN scan

- Not blocked by older stateless firewalls
- RST from closed ports, ignored by open ports
- Logs: many FINs without corresponding SYNs / ACKs

Intelligence Gathering Tools

UNIVERSITY OF LEEDS

- `traceroute` sends UDP or ICMP echo packets with increasing TTL, to map paths taken by packets
  - Identifies firewall and external router
  - Identifies hosts on same network
- **Nmap** supports a range of different scanning techniques and can perform **OS fingerprinting**
  - Uses database of TCP/IP stack idiosyncrasies
  - Estimates how easily sequence numbers can be predicted (for session hijacking)

Types of Attack

UNIVERSITY OF LEEDS

- Spoofing of identity
- Packet sniffing
- Session hijacking
- Denial of service (DoS)

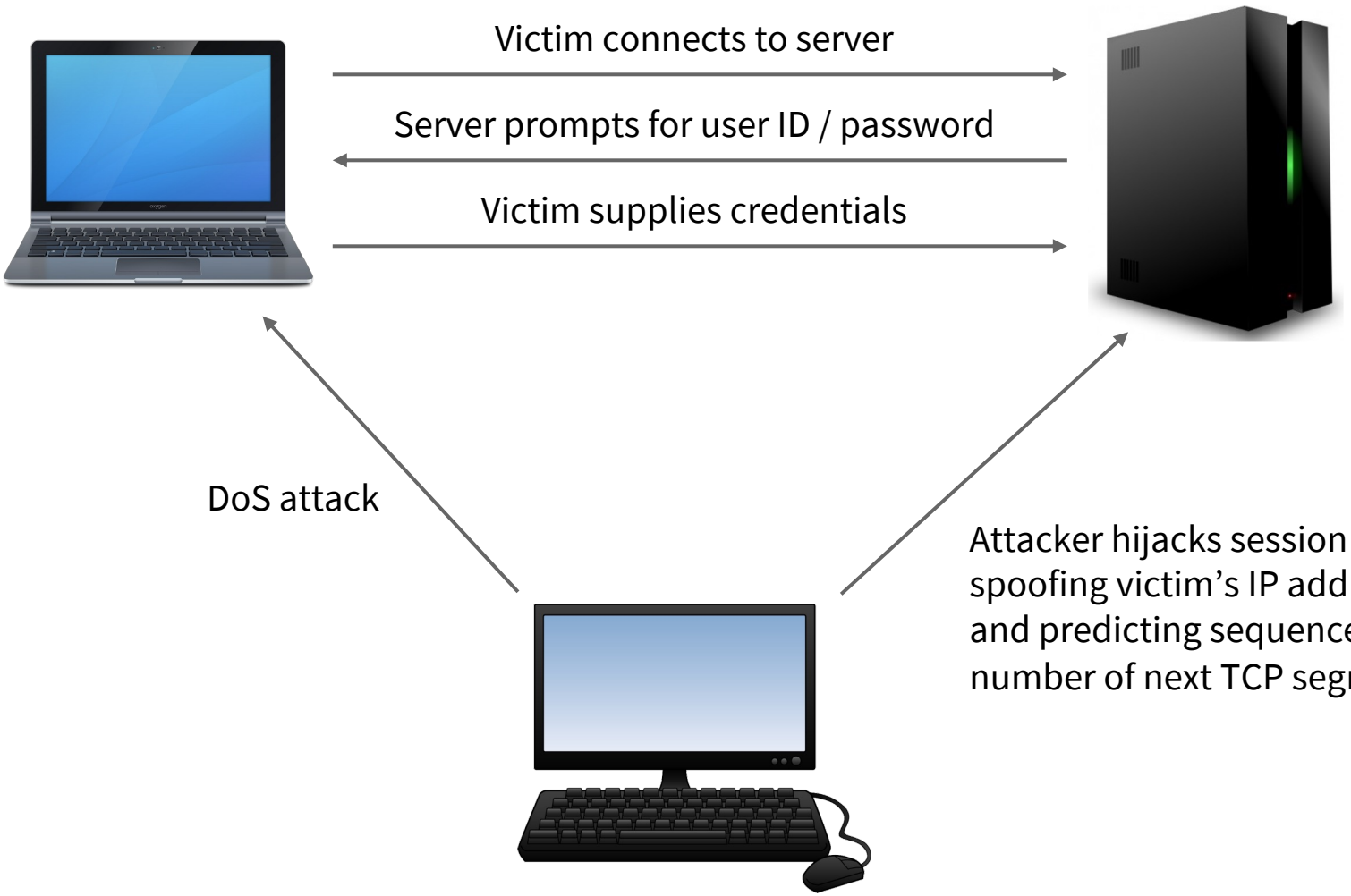
Spoofing of Identity

UNIVERSITY OF LEEDS

- Changing the source IP address in header is trivial…
- BUT this means attacker is ‘flying blind’; packets are sent to, but not received from, victim!
- Attacker could try **source routing**: packets will be routed through addresses specified by the attacker, on their way to the (spoofed) source
  - Frequently blocked!
- …or they could just attack from a compromised host

Session Hijacking

UNIVERSITY OF LEEDS



Denial of Service Attacks

UNIVERSITY OF LEEDS

- Goal is to render a server unavailable to clients
- Many different ways of achieving this
  - Exploiting weaknesses in protocols themselves or in their implementations
  - Overwhelming server with sheer volume – typically by directing a large **botnet** of compromised hosts to bombard it with traffic simultaneously (DDoS)

Past Examples

UNIVERSITY OF LEEDS

Ping of Death

- Used an ICMP echo request with fragment offset in the enclosing IP header set to maximum value and fragment size greater than 8 bytes
- Reassembled packet exceeds the $2^{16}-1$ byte size limit and could overrun memory buffers

Teardrop

- Similar idea: create fragments with overlapping offsets
- When fragments were reassembled, some systems would crash or reboot

Slowloris

UNIVERSITY OF LEEDS

- Notably used to target Iranian government web sites during the 2009 presidential elections
- Allows one machine to take down a web server
- Works by opening many HTTP connections to the server, sending partial requests that never complete
  - … eventually tying up connection pool of server

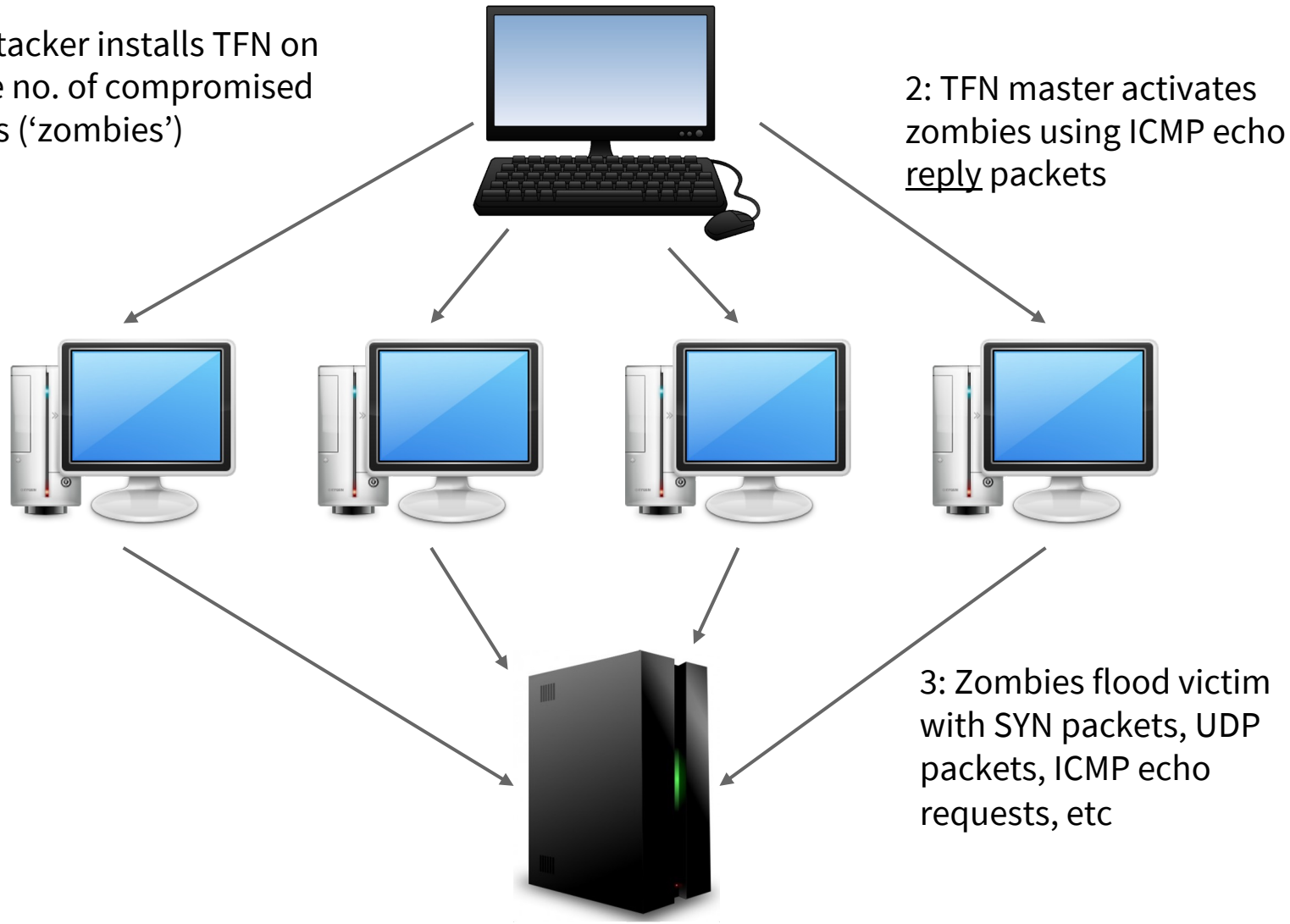
SYN Floods

UNIVERSITY OF LEEDS

- Attacker generates bogus packets, with SYN flag set and spoofed source IP address
- Victim is swamped with these packets (1000s per sec)
- Queue of half-open connections maintained by TCP/IP stack is quickly filled…
- … preventing further connections to victim
- Can be resisted using **SYN cookies**

DDoS in 1999: TFN

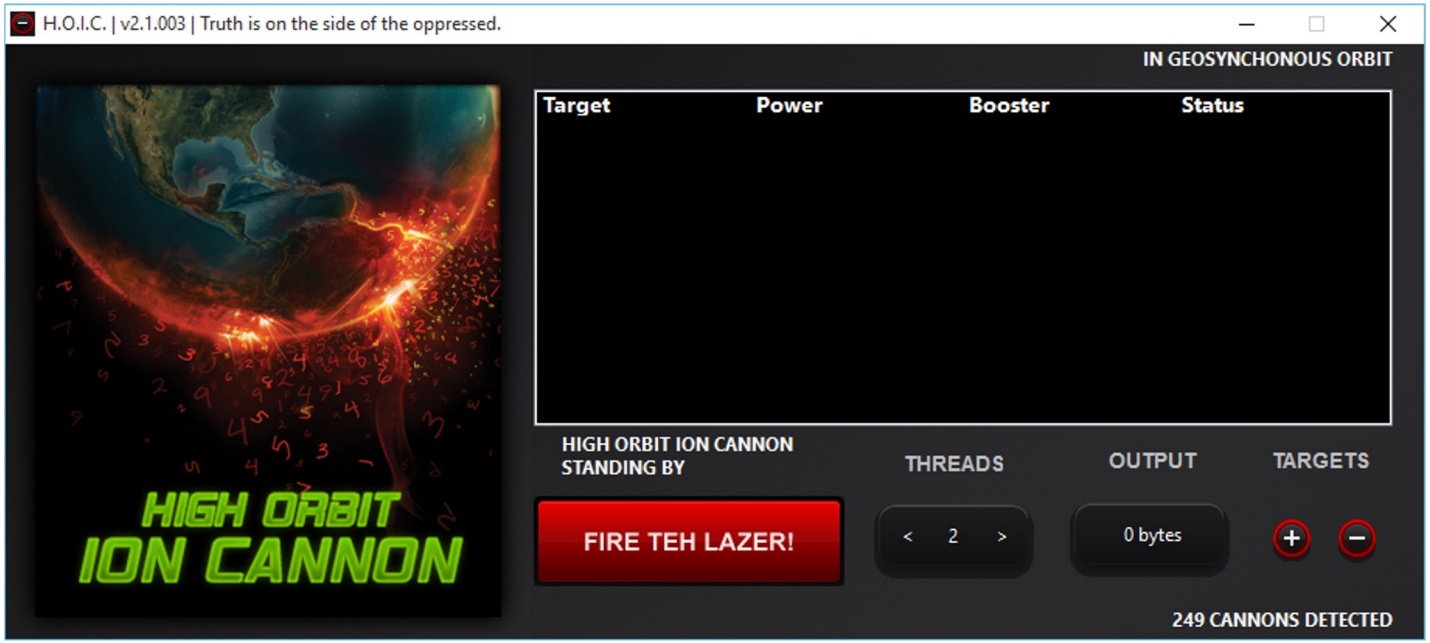
UNIVERSITY OF LEEDS



DDoS by Consent

UNIVERSITY OF LEEDS

- Coordinated group of users run the same software deliberately to DDoS a target site
- Example: High Orbit Ion Cannon, used by Anonymous



DDoS with Internet of Things

UNIVERSITY OF LEEDS

- IoT ⇒ billions of devices on the network…
- Mostly with poor security (at the moment)…
- Therefore easily recruited to botnets!
- Most famous example: September 2016 DDoS of ‘Krebs on Security’ blog (achieving **620 Gbps**)
  - Mirai software is available on GitHub!

Mirai Botnet

UNIVERSITY OF LEEDS

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-pass
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=4
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-

Used 68 factory-default / hard-coded username and password pairs to compromise 380,000 devices

Summary

UNIVERSITY OF LEEDS

We have

- Reviewed features of the TCP/IP stack that make it vulnerable to attack
- Discussed how attackers can do network reconnaissance using ICMP, UDP or TCP-based scans
- Seen how it is possible to spoof identity or even hijack an active TCP session
- Considered various examples of DoS & DDoS

Follow-Up / Further Reading

UNIVERSITY OF LEEDS

- Nmap, the network mapper
- Exercise 13 & Exercise 14
- Blog: “I scanned the whole country of Austria…”
- “Large DDoS attacks over 50 Gbps have quadrupled between 2015 and 2017” (Help Net Security)
- Slowloris: info and sample attack code
- Mirai IoT botnet source code
- “Reaper botnet could be more devastating than Mirai” (Graham Cluley)