COS30015 IT Security

Live Lecture Week 5

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

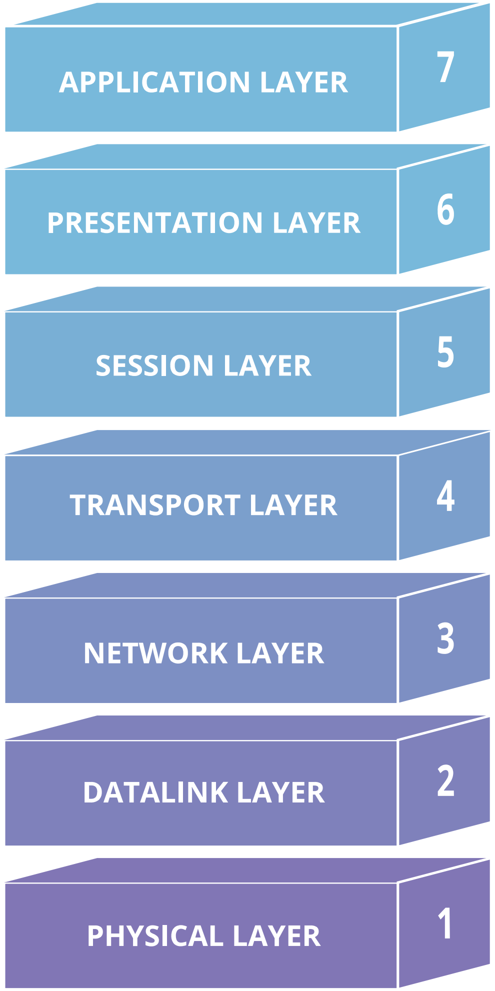
We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Network Basic

OSI Model



APPLICATION LAYER 7 — Human-computer interaction layer, where applications can access the network services

PRESENTATION LAYER 6 — Ensures that data is in a usable format and is where data encryption occurs

SESSION LAYER 5 — Maintains connections and is responsible for controlling ports and sessions

TRANSPORT LAYER 4 — Transmits data using transmission protocols including TCP and UDP

NETWORK LAYER 3 — Decides which physical path the data will take

DATALINK LAYER 2 — Defines the format of data on the network

PHYSICAL LAYER 1 — Transmits raw bit stream over the physical medium

(img source: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/)

https://www.youtube.com/watch?v=Ilk7UXzV_Qc

Network Tools

Ping
Traceroute/Tracert
ipconfig/ifconfig
Netstat
Packet Sniffing

Network Attacks

Network Attacks

- All layers of the OSI model are susceptible to attacks.
- Application layer:
  - viruses, worms, trojans
- Session layer:
  - null session attacks on Windows PCs
- Presentation layer
  - DNS DOS, DNS cache poisoning, Zone transfer
- Network layer
  - ARP cache poisoning, ARP spoofing
- Physical / Data link layers
  - Sniffing, playback attacks
- These and other layers have and will be attacked.

Common Attacks

- **Sniffing a NIC/hub/wifi broadcast.**
- Sniffing means capturing IP packets and displaying/analysing them.
- Common sniffing programs include Snort and Wireshark.
- Local NIC is set to Promiscuous Mode.
- Sniffing program records packets presented to NIC, including all packets passing through the hub.
- Switches are also susceptible to ARP cache poisoning and MAC flooding. Switches act like hubs when overloaded.

Common Attacks

- ARP cache poisoning.
- ARP maintains a table of MAC addresses and their equivalent IP addresses.
- ARP sends out queries: "Who has IP 239.254.2.15"
- Replies are added to the ARP table, and can come from any IP address at any time.

- How it works (MITM)
- Attacker attaches his PC to the network.
- sniffs to find target IP addresses.
- Sends a home-made ARP reply nominating his MAC as corresponding to the requested IP address.
- ARP adds the attackers MAC address to the ARP table.
- Future traffic to the target goes to the attacker.
- Attacker reads packets, doctors them and sends them on to the target who is none the wiser.

Common Attacks

- MAC flooding.
- Switches use ARP to map MAC addresses to IP addresses.
- When booted up, switches operate in hub mode while they learn the MAC addresses attached to each port.
- Switches have limited memory and computing power.
- When overloaded, they revert to Hub-mode and broadcast all packets to all interfaces.

- How it works
- Attacker attaches his PC to the network.
- Sends out multiple invalid ARP responses.
- Switch overloads and reverts to hub-mode (all lights start flashing).
- Attacker collects all packets from the network.

DoS (Denial of Service)

- DOS attacks are aimed at servers on the internet
- web servers (HTTP), name servers (DNS), FTP servers
- Can be launched at specific machines if the IP address is known.

- The goal is to Deny Service to legitimate customers/users.
- Customers go elsewhere
- Organisations lose money/trade/reputation

DoS (Denial of Service)

Ping of death

- an over-sized ping packet (>65535 bytes) is sent to a susceptible PC. Causes a re-boot on susceptible machines.

ICMP

- attacker sends a stream of ICMP echo request packets.

SYN Flooding

- a resource depletion attack
- attacker sends a stream of SYN packets (the first part of a TCP 3-way handshake).
- Each SYN packet consumes memory on the server while it sends the SYN_ACK packet and waits for the returning ACK packet.
- The attacker never sends the ACK packet.

DoS (Denial of Service)

UDP flood

- UDP packets are sent to random ports of the victim as fast as possible.
- The target machine will respond to each packet with a ICMP destination unreachable packet.

Teardrop

- A fragmented packet is sent to the attacker, but the parts have been corrupted and can not be put back together.
- Server consumes resources requesting retransmit.
- May crash the server.

Land attack

- Amplification attack
- A packet with a spoofed source IP address is sent to the victim. The return address is the same as the destination addresses, so the victim's machine ties it self in knots by answering back to itself.

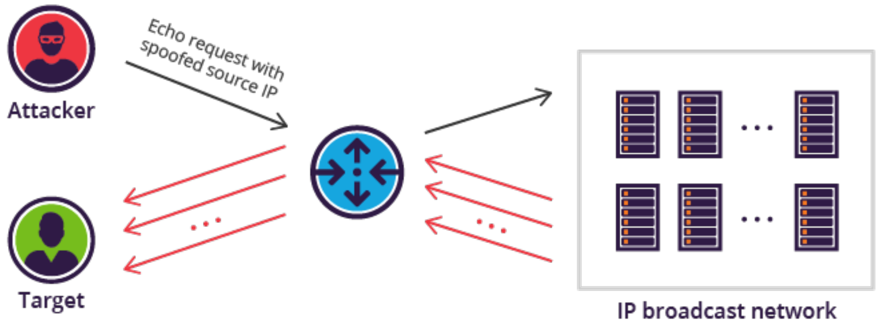
DDoS

- A Distributed DOS involves simultaneous attacks on a single site by 'zombie' machines infected with a 'bot'. Each bot is controlled by a 'bot-herder' originally through IRC channels and now through http. A bot-herder's 'bot-net' may range in size from a few hundred to millions of infected PCs.

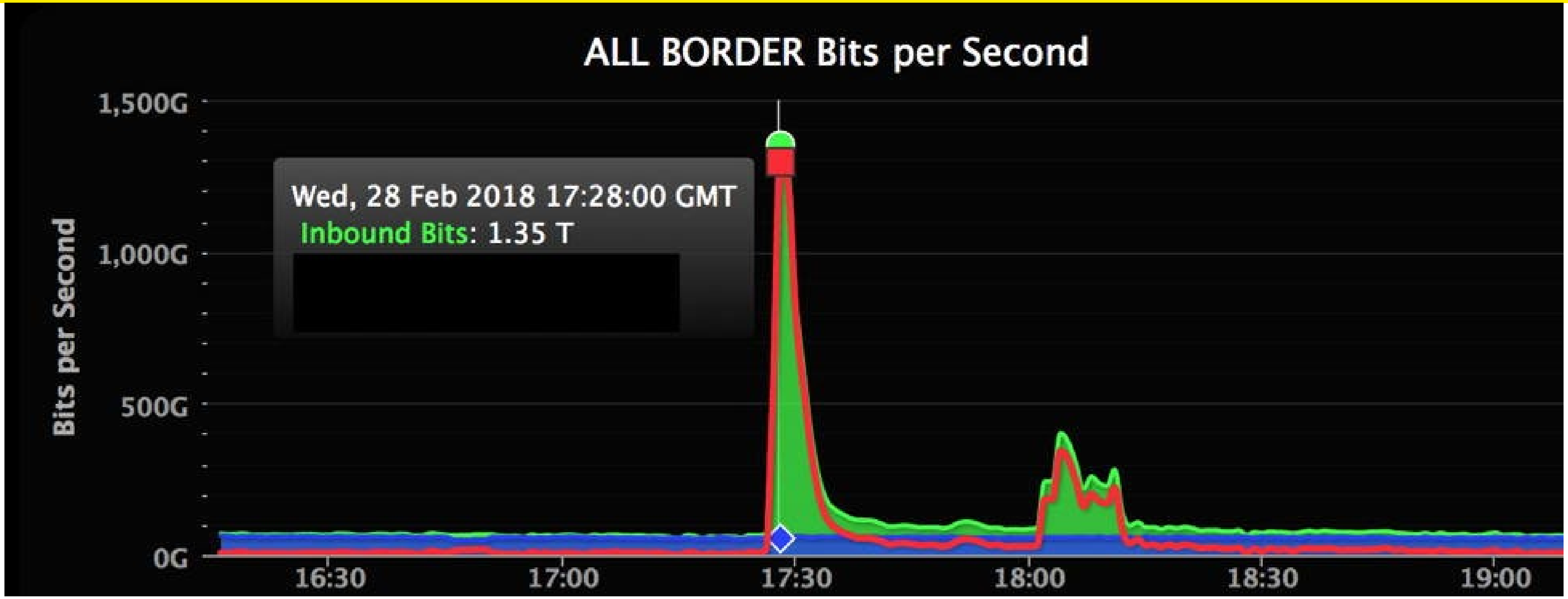
- Each bot is actually a small server program which has installed itself and is capable of launching DOS attacks, sending spam, infecting other machines, or all of the above.
- Spread by trojans (e-mail, web downloads) or by worms.

Smurf Attack (DDoS)

- Amplification attack
  - An attacker sends a ping (ICMP echo request) to the *broadcast* address of the victim's network.
  - This sends the ping to all IPs on the subnet. The original ping has a spoofed return IP address which is the address of the intended victim.
  - Each IP reached by the original ping replies to the victim.



DDoS attack example



GitHub DDoS attack, 2018

June 25, 2020

4

Re-Hash: The Largest DDoS Attacks in History

Amazon reported sustaining a 2.3 Tbps DDoS attack in 2020 – here’s what to know about the largest DDoS attacks on record & how they’re measured

Stopping DDoS

DDOS targets are chosen for a reason

- Find out who your enemies are.
- Are you a victim of extortion?
- Have you offended a script kiddie?
- Is there a political motive?

Options:

- Get a new IP address.
- Mitigation strategies: rate limiting, blackholing (not very effective)
- http://www.symantec.com/connect/articles/closing-floodgates-ddos-mitigation-techniques

Defence Strategies

Identify attack early

overprovision bandwidth

defend at the network perimeter

talk to your ISP

- filtering, rate-limiting
- port knocking

call a DDoS mitigation specialist

some services do not need to be protected

some services should not be on the Internet (use a private corporate network)

What's in this week's lab?

❑ Lecture Topic --- Network Security

❑ Lab Task --- Denial of Service Attack

Task List for Week 5

❑ Lecture Activity
  - ❑ Video-streaming lecture

❑ Complete this week’s Lab Task

❑ Draft for ASSIGNMENT 1. Then you still have one more week to finish the draft and maybe can refine it before submit!

❑ Suggest: external readings in Week 5 Module