Section 5 - Networks and Web Technologies

- Structure of the Internet and Internet Communication
- Network Security and Threats

Structure of the Internet and Internet Communication

The Internet

The internet is a network of networks set up to allow computers to communicate with each other globally. It is accessed via Internet Service Providers (ISPs), which usually provide routers for families and businesses to access the internet.

URLs

URLs are made up of:

- Method (http://, https://, etc)
- Host (www, mail, etc)
- Domain name (google, microsoft, etc)
- Second level domain (co, org, etc) (not always necessary) (there can be more levels, but this is uncommon)
- Top level domain (uk, ps, etc) (necessary)
- Location (e.g. webpage.html)
- Resource (e.g. #element)

> https://www.domainname.com/folder/subfolder/webpage.html#element

Domain names identify the areas or domains that internet resources reside in. Thees are structured into a hierarchy of smaller domains and written as strings separated by full stops as dictated by the rules of the Domain Name System (DNS).

Internet registrars hold records of all existing website names and details of domains that are available for sale. They resell domain names.

Internet registries own worldwide databases that hold records of all domain names currently issued to individuals and companies with their details. They also allocate IP addresses and keep track of which address(es) a domain name is associated with as part of the DNS.

Domain Name System

The Domain Name System (DNS) is a "hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol networks" (source).

Domain names are made up of:

- A website name.
- Company second level domain (2LD) (not always necessary) (there can be more levels, but this is uncommon)
- Company top level domain (TLD).

To be a fully qualified domain name (FQDN), there must also be a host.

- Host (e.g. www, mail)

> https://www.bhf.org.uk
>
> https://www.bookstack.asadhussain.net

IP Addresses

An Internet Protocol (IP) address is a unique address that is assigned to a network device. It indicates where a packet of data is to be sent or has been sent from. Routers use the IP address to direct data packets accordingly.

Networks

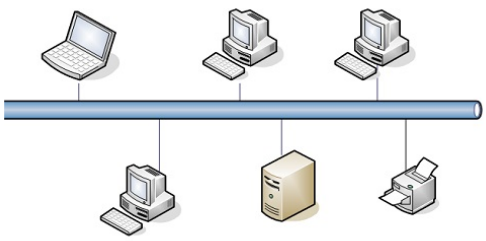
- A Local Area Network (LAN) consists of multiple devices connected over a small geographical area. Companies/individuals own and use their own hardware for a LAN, e.g. copper cables and ISP routers.
- A Wide Area Network (WAN) consists of multiple LANs connected over a large geographical area. Usually used by companies, this type of network usually requires renting infrastructure to connect LANs.

Network Topologies for LANs

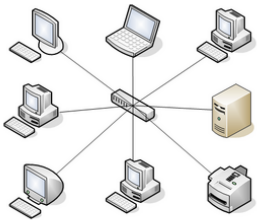
Topology	Description	Advantages	Disadvantages

(1) Physical bus	All devices are connected to a single cable.	Inexpensive to set up due to not a lot of cables required.	Single point of failure (main wire). With more traffic, performance degrades due to data collisions. Since every device has access to the cable, there is low security as all traffic can be seen.
(2) Star	All devices are connected to a central node, usually a switch, which routes data.	If one cable fails, other devices can still connect. Consistent performance, even under high load. No problems with data collisions. The system is more secure due to only one path between a device and the switch. Easy to add nodes to the network.	Costly due to more cables required. Single point of failure (central node).
(3) Partial/Full mesh	All devices are connected to each other, and access each other via these connections.	More reliable due to more interconnected nodes. - if one fails, another route can be taken via other nodes. With wireless, no cabling costs, so cheaper. Easy to add new nodes. Faster communication due to no need for a switch.	Physical implementations are expensive due to lots of cables.

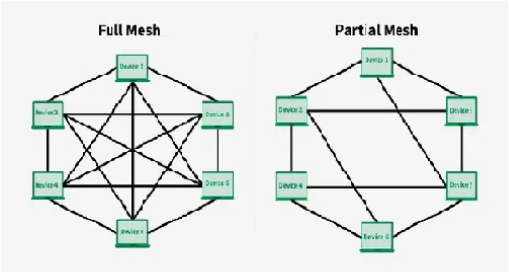
(1)



(2)



(3)



Network Security and Threats

Threats

Viruses

A virus is a piece of malicious software that has the ability to self-replicate. It exists in a host file, usually an executable file of some sort. It inserts its malicious code in other executable files to spread. A virus can be: spyware, which captures user data and sends them to a hacker; ransomware, which encrypts user data and demands payment for decryption.

A worm is another type of virus that doesn't require a host - it is self sustaining. It simply replicates itself and sends itself to other devices on a network or can hijack your email and send itself to your contacts.
E.g. the ILOVEYOU worm was a VBS script that destroyed every file on a user's computer, stole passwords, installed a backdoor, and used one's email to send itself to other people. The file was hidden as a TXT file named "LOVE-LETTER-FOR-YOU.TXT.vbs", but Windows hides file extensions by default, so users didn't know it was a script and expected the file to open in a text editor.

Trojans

A trojan presents itself as a legitimate file. Once run, it executes a payload, which may have different purposes based on its creator. The typical purpose of a trojan's payload is to install a backdoor in a computer, which is a route by which hackers can access a computer and perform more malicious tasks, such as spying on you or stealing your passwords.

System Vulnerabilities

Out-of-date software can have security flaws that can be exploited by hackers to gain access to a system. It thus makes it very important to keep software up-to-date.

It can also be just due to bad coding practices. An example of an exploit is SQL injection, where SQL statements are added to input boxes in a website, which can lead to the execution of these statements, allowing hackers to bypass login or just dump tables of data for the hacker to view.

Social Engineering

Social engineering involves the manipulation of people to gain unauthorised access to their/a system. This can be as trivial as peeking over their shoulder to see them type their password into their computer, or (as seen above in the ILOVEYOU worm) hiding the fact that a file is an executable script and making people think it's genuine enough to be opened.

An example is phishing, which is usually an email or website that impersonates a legitimate company like Google or Microsoft.

Pharming is the redirection of users to a fake copy of a trusted website, usually by alteration of DNS records or host files. This allows the collection of data like emails and passwords.

Data Interception

This is the unauthorised access of data while it is being transmitted over a network. If not encrypted, it can be read by a hacker. In a man-in-the-middle attack, the hacker is a proxy between the victim and the network, and can manipulate inbound and outbound data. E.g. the victim can be directed to a phishing login page for their email.

DoS and DDoS Attacks

DoS (denial of service) attacks involve sending massive numbers of requests to a server/network, causing bandwidth to be consumed, slowing down the network to the point of access to a provided service being denied.

DDoS (distributed denial of service) attacks involve multiple infected computers, usually infected from a virus, sending massive numbers of requests instead of just one. The increased number of requests makes DDoS attacks much more devastating than DoS attacks. A collection of infected computers used in DDoS attacks is called a botnet.

Security Measures

Firewalls

A firewall monitors and controls incoming and outgoing network traffic. It serves as a barrier between a computer and a network. It can be used to restrict access to specific applications and websites, controlling which resources can connect to or be accessed via the network. It can protect against:

- Hackers
- Malware
- DoS and DDoS attacks

A firewall uses packet filtering.

- Static (stateless) filtering involves examination of source and destination: IPs; protocols; and port numbers, all found in a packet header. Unauthorised requests are blocked based on a set of rules, which the above 3 pieces of information are compared with to authorise or reject requests.
- Dynamic filtering (stateful) involves the live analysis of packets going between two verified clients. Any detected anomalies are flagged based on temporary and adaptive rules for the session, and packets can be rejected or the connection can be dropped.

Proxy Server

A proxy server acts as an intermediary between a user's device and the internet, forwarding requests and returning responses on the user's behalf. This helps hide the user's IP address and allows organisations to monitor and control network traffic. It can protect against:

- Malware
- Hackers
- Phishing

A proxy server also maintains cached data for visited websites, speeding up website loading times. Network requests can also be filtered, so proxy servers are used in institutions like school to block access to blacklisted websites.

Encryption

Encryption scrambles data using a key to make it unreadable. Attackers cannot understand it if intercepted during transmission. It can protect against:

- Data interception
- Device/Data theft

Anti-Malware Software

Anti-malware software scans files and programs and compares them to a database of known malware signatures to identify them as malicious. It can quarantine, block, and remove suspicious files to prevent them from harming the system. They protect against malware such as:

- Viruses
- Worms
- Trojans
- Spyware
- Ransomware