

Unit 1.2: Communication and Internet Technologies

1.2.1 DATA TRANSMISSION

Data transmission: data transferred from one point to another

- Copper cable using electrical pulses
- Wirelessly using radio frequency
- Optical fibre using light
- Infrared

Serial transmission: when bits are sent one signal at a time over a single wire

- Used by USB (universal serial bus) cables
- Bits are transmitted sequentially
- Advantages:**
 - Cheap
 - Can transmit over long distances
 - Safe – collate the bits incrementally, no interference
- Disadvantages:**
 - Slow

Parallel transmission: bits are sent simultaneously over a number of parallel wires

- 8 wires = 1 byte
- Used when there is little chance of interference e.g. washing machines
- Integrated circuits (IC):** made of a semiconductor material silicon
 - Silicon layer assembles millions of tiny resistors, transistors and resistors sending data in parallel
- Advantages:**
 - Fast
- Disadvantages:**
 - More expensive
 - Limited to short distances
 - Less safe as errors can occur when collating the bits

Simplex transmission: data sent in one direction only

Half-duplex transmission: data is sent in both directions one direction at a time

- E.g. printer cables

Full-duplex transmission: data is sent in both directions at the same time

- E.g. internet cables

1.2.2 SECURITY ASPECTS

Malware (malicious software): any software written with malicious intent

- Damage files, limit hard disk space, consume internet bandwidth
- Spyware**: a software that covertly gathers information from your computer
 - E.g. collect usernames and passwords, credit card details, install more spyware on your machine to read your cookies and change your system preferences
- Adware**: responsible for the adverts that pop-up whilst using the computer – don't do harms
- Viruses**: small program which when executed, can replicate by inserting itself into other computer programs
 - Attach themselves to existing software programs and infect your computer when you run the programs
 - Email, memory stick, file sharing
 - E.g. botnets, DoS (denial of service) attacks
- Worms**: a standalone file that does not need a host program to attach itself to
- Trojans**: a non-self-replicating virus that masquerades as a harmless file you may open
- Ransomware**: used to lock your computer so you have to pay to regain access to your files

Reducing the risks

- Personal vigilance – don't open email attachments from unknown senders
- Anti-virus software**: detects viruses and usually deletes infected files
 - Commonly finds all other malware
 - Holds a dictionary of code snippets used in viruses that is kept up-to-date
 - Scans new files, downloads and external drives on your computer, looks for suspicious malicious code by comparison
- Firewall software**: acts as a filter between your trusted network and others, only allows certain data packets across that meet set filtering rules
 - Can be hardware, software or both
 - Used in routers

Hacking: unauthorised access to programs or data

- Black hat**: illegally hacking to steal data or other bad intentions
- White hat**: ethical hackers employed by companies to find holes in their security
- Grey hat**: look for holes in other systems and then contact companies for payment in return for fixing the problem

Cracking: illegally accessing program source code to change it

- Bypass security, unlock new features that would need subscription

INTRODUCTION TO THE INTERNET

Internet: a collection of inter-connected networks

- ISP (internet service provider)**: a company supplying connectivity to the internet
 - Offers email services, web hosting, VOIP facilities
- Browser software**: safari, firefox, google chrome
- Search engines**: processes billions of searches every day e.g. bing, baidu, google

- WWW (world wide web)**: information may be biased, inaccurate, out-of-date
 - Every ISP has its own data storage facility
 - Data is stored in server rooms
-

1.2.3 INTERNET PRINCIPLES OF OPERATION

Two devices are needed to connect your PC to the internet.

Modem (modulator/demodulator): connects your PC to your ISP

- Converts digital signals from the computer to analogue signals used by telephone lines, second modem at the receiving end converts the analogue signal back to digital

Router: a hardware device that allows you to connect several computers and other devices to a single internet connection, in a home network. Provides access to a local network

PC → Router → Modem → ISP → Internet

Protocols: set of rules about how messages are formatted and transmitted

- TCP (transmission control protocol)**: breaks up messages sent over the internet into small chunks called packets, packets are reassembled at the other end

- Detects errors and resends lost messages

- IP (internet protocol)**: routes the individual packets between sender and recipient

- HTTP (hypertext transfer protocol)**: used for accessing and receiving web pages in the form of HTML files on the internet

- The protocol requests the web server to upload the requested web page to the user's browser for viewing

- HTTPS (hypertext transfer protocol secure)**: encrypts the information so that it cannot be hacked

- SSL (secure socket layer)/TLS (transport layer security)

- Packet switching**:

- Every packet is given a header which contains:

- The IP address it is going to
 - The IP address it has come from
 - The sequence number of the packet
 - The number of packets in the whole communication

- IP address**: every computer connected to the internet has an IP address

- Public: belongs to the router on your LAN
 - Private: accessible only within the LAN
 - Changes depending on the router you are connected to

- Packets are sent across the internet via different routes and reassembled at the end

MAC (media access control) addressing: assigned to each Network Interface Card (NIC) by the manufacturer

- Your computer may have multiple MAC addresses

- Uses hexadecimal
- Every networked device in the world has a unique MAC address
- 2^{48} possible addresses
- MAC address never changes

URL (uniform resource locator): web address

- Unique
- http:// – scheme
- www.....com – host name
- /xxyyzz – path
- Domain names: e.g. .edu, .com, .org, .gov

-DNS (domain name system): allows you to type a web address such as google.com into your web browser

- Transfers web address into an IP address
- When a DNS server receives a request not in its database, it will pass the request on to another server until it reaches one with the matching name and IP address
 - Lower level DNS servers are owned by ISPs

Cookies: a small data file that a web server will put onto your computer when you visit a website

Role of a browser: user types in a URL into the browser's address bar, web browser forwards this request to the web server to access the web page. Web server acknowledges the request and sends the HTML source code for the web page to the user's computer, source code is rendered into a viewable web page