Motherboard
The motherboard is a printed circuit board found in all computers. It allows the processor and other computer hardware to function and communicate with each other. One of the major functions of a typical motherboard is to act as a kind of 'hub' that other computer devices connect to. A typical motherboard consists of a sheet of non-conductive material, such as hard plastic. Thin layers of copper or aluminium are printed onto this sheet. These form the circuits between the various components. In addition to circuits, a motherboard contains several sockets and slots to connect the other components.

Random access memory (RAM)
Random access memory (RAM) is an internal chip where data is temporarily stored when running applications. This memory can be written to and read from. Since its contents are lost when power to the computer is turned off, it is often referred to as a volatile or temporary memory.
RAM stores the data, files or part of the operating system currently in use.

Read-only memory (ROM)
Read-only memory (ROM) is a memory used to store information that needs to be permanent. It is often used to contain, for example, configuration data for a computer system. These chips cannot be altered and can only be read from (hence their name).
One of the main advantages is that the information stored on the ROM chip is not lost even when power is turned off to the computer. They are often referred to as non-volatile memories.

INTERNAL COMPUTER HARDWARE

Video card
A video card allows the computer to send graphical information to a video display device such as a monitor, television or projector. It usually connects to the motherboard (see above). Video cards are usually made up of:

- a processing unit
- memory unit (usually RAM)
- a cooling mechanism (often in the form of a heat sink since these cards generate much heat)
- connections to a display unit (monitor, television or projector).

Sound card
A sound card is an integrated circuit board that provides a computer with the ability to produce sounds. These sounds can be heard by the user either through speakers or headphones.
Sound cards also allow a user to record sound input from a microphone connected to the computer, and to manipulate sounds stored on a disk.
Sound cards use two basic methods to translate digital data into analogue signals (needed for speakers):

- **FM synthesis** mimics different musical instruments according to built-in formulas
- **wavetable synthesis** relies on recordings of actual instruments to produce sound.

Internal hard disk drive/solid state drive (HDD/SSD)
These two devices are covered in considerably more depth in later chapters of this book. Basically, hard disk drives (HDD) are magnetic in nature and are one of the main methods for storing data, files (text, photos and music) and most of the system and application software. More modern computers (and all tablets) use newer storage systems that make use of solid state drive (SSD) technology and are replacing HDD in many cases. Their function is the same as HDD.

Figure 1.3 Internal computer hardware

The next generation of smartphones will use touch screens with OLED (organic light-emitting diode) technology. The touch screens are coated with a crystalline layer that allows the phones to be partially solar powered, but this also allows them to use Li-Fi (similar to Wi-Fi except communication uses visible light rather than radio waves). Communication using Li-Fi is considerably faster than Wi-Fi (it has a much higher data transfer rate); it is also more secure (it stops internet 'piggybacking', unauthorised use of the internet connection) and can also be used on flights since it doesn't use radio waves.

The technology works by switching LED bulbs off and on in nanoseconds (10^{-9} of a second) which is too quick for the human eye to detect. Light on represents the binary value 1, while light off represents the value 0. This is the basis behind the method used for communication.

Advantages of smartphones:

- they are very small in size and lightweight – therefore very easy to carry round and have on your person at all times (this is more difficult with laptops since they are much bulkier and also much heavier)
- can use them to make phone calls as well as connect to the internet while on the move
- because they use Wi-Fi and mobile phone networks, they can be used almost anywhere (this is not the case with laptops or PCs, although tablets also use the same technology)
- they have hundreds of Apps (such as camera facility, MP3/4 players, and so on) – again this is similar to tablets, but it is an advantage compared to laptops
- they have a reasonable battery life compared to laptops.

Disadvantages of smartphones:

- the small screens make pages difficult to read and small keyboards make typing things in more difficult and slower (laptops and PCs have much bigger screens and much larger keyboards) – this disadvantage is becoming less of a problem as smartphone screens get larger on newer phablets
- web browsing and photography can drain the battery quickly
- memory size in most phones isn't very large when compared to laptops and PCs – although it is comparable with tablets
- not all website features are compatible with smartphone operating systems
- because of their small size, it is much easier to lose a smartphone (or for it to be stolen) than laptops or PCs
- the data transfer rate using mobile phone networks is slower than with Wi-Fi – this makes streaming of video or music, for example, less than satisfactory at times.

1.4.5 Smartwatches

Smartwatches essentially allow users to wear a mini-computer on their wrists. They offer the same functions as a smartphone and make use of OLED technology (see Chapter 2). As with smartphones, they use touch-screen technology but also have the ability to link to smartphones using Bluetooth technology.

1.5 Impact of emerging technologies

Some of the latest technologies were mentioned in Section 1.4. This section reviews briefly the impact of the following new technologies:

- artificial intelligence (AI) biometrics
- vision enhancement
- robotics
- quantum cryptography
- computer-assisted translation (CAT)
- 3-D and holographic imaging
- virtual reality.

New technologies are being developed at a remarkable rate, so the reader is advised that the above list could be out of date very quickly. A quick review on the internet is advised every six months or so to ensure that the reader is up to date with all the latest technologies.

1.5.1 Artificial intelligence (AI) biometrics

A known problem with biometric technology is that many fingerprint identification systems falsely reject a person's fingerprints – when the scanned fingerprints are checked against the database no matches are found.

Artificial intelligence (AI) biometrics overcomes this problem using **dynamic profiling** – the system learns by using AI about a person's fingerprints on every scan. This means a person doesn't have to worry about getting their finger in exactly the right place every time on the scanner. The system learns from the different alignments and is therefore still able to match the fingerprints to those stored on a database.

Facial-recognition systems have the same problem. A human being is still able to recognise a face even if the person has grown facial hair, now wears glasses or has aged. Computerised facial-recognition systems are confused by such **soft biometric** changes. New systems use AI to learn from scanning a number of faces and can pick out these soft biometric features. This means the system can still recognise faces and cross-reference these attributes with corresponding images stored on the database.

Other AI biometric technologies are being developed, so these security systems become increasingly more reliable.

1.5.2 Vision enhancement

Low-vision enhancement systems (LVES) use video technology through a headset connected to a computer. The system allows images to be projected inside the headset in front of the eyes. This effectively brings the objects closer for examination by the user of the system.

Night vision enhancement (NVE) amplifies infrared light and visible light so that an image can still be seen in apparent darkness. For example, the military use this technology to carry out surveillance at night. The dim light source is captured and passed through an **image intensifier tube**, which converts the light into electrons. These electrons pass through another tube where they are amplified to produce several times the original number of electrons. A screen at the end of the tube is coated in phosphor dots that glow when electrons collide with them – this results in an image that is considerably clearer than the original.

1.5.3 Robotics

Robotics has been around for many years, mostly in the manufacturing industry. They are used in car factories to weld car bodies, spray body panels and fit items such as windscreens. No human intervention is required. However, there are areas outside manufacturing where robotics is evolving rapidly, and we could see robots appearing in many areas of our lives in a relatively short space of time.

One application is the use of **drones**. These are unmanned flying devices that are used by both the military and civilians. The military have used drones in reconnaissance missions for a number of years. Civilian uses include surveying the landscape in 3-D for use with GPS, investigating weather phenomena (for example, flying into hurricanes or other weather conditions that would be dangerous for manned surveillance), or search and rescue/fire fighting in natural disasters. All of these are currently under evaluation and many more applications could evolve over the coming years.

Another application is the use of robots in surgical procedures. Robotic surgery allows surgeons to perform complex procedures with more precision, flexibility and control than standard surgical techniques. With this technique, surgeons use robotics equipped with a camera arm and several interactive mechanical arms – these have joints that work like a human's wrist.

1.5.4 Quantum cryptography

Cryptography is the science of making a message unintelligible to any unauthorised user (a hacker). This technique is often referred to as **encryption**. There are many methods of cryptography in existence but all of them have a limited life as computers become faster and faster at number crunching. A consequence of this is that, over the next few years, a hacker is increasingly likely to decipher encrypted messages unless computer designers can further strengthen security systems.

Quantum cryptography is based on the use of photons (light) and their physical quantum properties to produce a virtually unbreakable cryptography system. This helps protect the security of data being transmitted over fibre-optic cables. The technology relies on the fact that photons oscillate in various directions and produce a sequence of random bits (0s and 1s) across the optical network. It is based on the laws of physics rather than mathematics (which is how current cryptography methods work). How this works in detail is beyond the scope of this book.

1.5.5 Computer-assisted translation (CAT)

Existing online language translators have a very limited use.

Consider the insect called a fruit fly, which particularly enjoys eating bananas. What if we typed in the phrase: 'fruit flies like a banana'. This could be translated into German using a free online translator as '*fruchtfliegen wie eine banane*'. The statement in German only refers to the banana-shaped flight path of a piece of fruit thrown through the air! Imagine a whole page being translated that is full of such double meanings of words and phrases.

Computer-assisted translation (CAT) goes some way to overcome these issues. CAT is a type of language translator that uses specific software to help in the translation process. In particular, CAT uses two tools:

- terminology databases – linguistic databases that grow and 'learn' from translations being carried out
- translation memories – these automatically insert known translations for certain words, phrases or sentences.

All CAT software needs some post-editing by the user to remove errors from the translation process. While not perfect, they are certainly more accurate than existing free online translators.

1.5.6 3-D and holographic imaging

Holography is a technology that allows 3-D images (known as holograms) to be produced. The technology involves the use of:

- a source of laser light
- interference of light
- light diffraction, and
- light intensity recording.

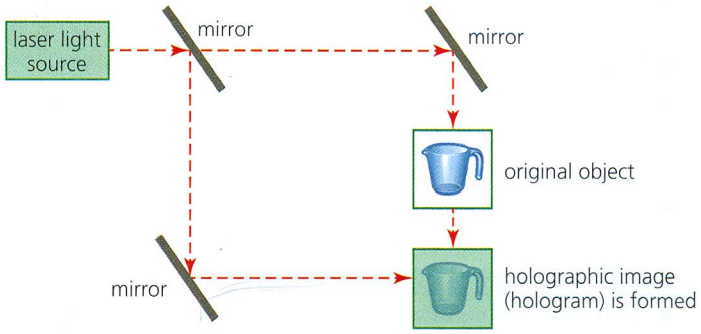


Figure 1.8 Formation of a hologram

As a holographic image is rotated, it appears to move in the same way as the original object, thus appearing to be in three dimensions (3-D). The hologram is produced by first splitting a laser beam. Half of the light (known as the **object beam**) is reflected off the object on to a photographic plate. The other half of the light (known as the **reference beam**) is reflected off a mirror and on to the same photographic plate. The holographic image is produced where the two light beams meet on the photographic plate.

Holograms have the following applications:

- engineering design (CAD)
- architecture (ability to rotate design through 360 degrees)
- simulations
- medical imaging (see inside organs in 3-D – links into tomography, which is the same technology behind 3-D printers)
- cinema (special effects)
- gaming (special effects)
- advertising
- holographic televisions (expected by around 2025, these should give a full 3-D experience without the need for special glasses)
- holographic computer memories (a new type of optical storage – a crystal the size of a sugar cube can hold up to 1 TB of data)
- optical computers (these will operate at speeds that are trillions of times faster than-current technology computers).

1.5.7 Virtual reality

Virtual reality is an artificial environment created by software. The user makes use of data goggles, sensor suits, data gloves or helmets to get a feeling of reality (that is, the feeling of 'being there'). The technology is used in training (for example, in a nuclear reactor where the user can see all the walls, pipes, vessels and valves as if they were inside the reactor, so that they can be trained safely to deal with certain events), education (for example, to explore the inside of a building such as a castle in a history lesson) or in games (where the user can interact as if they were there, such as a driving simulator where the road ahead is output on to a visor in a helmet strapped to the user's head).

Virtual reality is used in all of the following areas:

- military applications (for example, training to use a new tank)
- education (for example, looking inside an ancient building as part of a history lesson)
- healthcare (for example, as a diagnostic tool)
- entertainment (for example, games where gloves, goggles or helmets are worn to give realism to the scenario and even to give images or sound to make it seem very real)
- fashion (for example, to do fashion shows before doing the real thing to see the clothes on people, check out the venue and so on)
- heritage (for example, showing monuments such as Stonehenge)
- business (for example, training courses and role-playing scenarios for staff)
- real estate (for example, allowing people to 'look around' houses that are for sale)
- engineering (for example, seeing how new designs will look)
- sport (for example, a golfer trying to improve their swing can use this technology and get feedback to improve their game)
- media (for example, special effects in films such as *The Matrix*)
- scientific visualisation (for example, looking at molecular structures in chemistry).

Disadvantages

- If the magnetic stripe gets damaged (for example, due to exposure to a strong magnetic field) the data is lost.
- Doesn't work at a distance (card needs to be in close contact with the reader).
- Since the information is not human readable, this can be a disadvantage in some applications.

Contactless card readers

Contactless debit or credit cards allow customers to pay for items worth up to $25 without entering their PIN. All contactless cards have a small chip that emits radio waves embedded in them. The card is held within a few centimetres of the payment terminal to pay for an item; the terminal picks up the signal from the chip and allows the transaction to be processed.

The steps taken are:

1. Customers look out for the contactless symbol on the payment terminal.
2. The shop assistant enters the amount for payment.
3. The card reader informs the customer to present their contactless card.
4. The customer holds their card in front of the card reader.
5. The terminal display will indicate that the card has been read.

Advantages

- Faster transaction (typical transaction takes 15 seconds as opposed to 30 seconds using a magnetic stripe reader).
- The system uses 128-bit encryption to protect data.
- Customers do not have to worry about typing errors (such as incorrectly typing in a PIN).
- Retailers no longer have access to the customer's credit/debit card information.
- The chip in the contactless credit card responds to the payment terminal reader with a unique number used for that transaction only; it does not simply transmit the consumer's account number; this number is also encrypted.

Disadvantages

- They are more expensive than normal credit/debit cards.
- A thief with a suitable reader could monitor your contactless card transaction while standing at the counter with you, or just behind you (the third point above reduces this risk considerably however: because you don't have to type in a PIN, somebody standing behind you couldn't steal your PIN and use it).
- Can take money twice if the customer uses it as a chip and PIN card (one is contactless and the other is chip and PIN).
- Transactions are usually limited to a small maximum value (e.g. $25).
- Transactions have been carried out without the card holder being aware of this while they were just standing in the payment queue.

Chip and PIN readers

Chip and PIN readers are similar to smart card readers but are used at EFTPOS terminals. The device has a slot into which the card is placed and the chip is read; the PIN is entered using the keypad. The reader also has a small screen which

gives instructions to the operator. They are similar to the contactless system, except for two points:

- the customer has to key in their PIN to make a transaction
- the cards do not make use of RF technology.

Uses

- Where payments are made using cards (restaurants, supermarkets, travel agents, etc.).

Advantages

- More secure system (PIN typed in must match up with PIN stored on chip).
- More robust system than magnetic stripe cards.

Disadvantages

- Fraud – need to be careful to ensure PIN isn't read by somebody else while typing it in.

2.2.2 Radio frequency identification (RFID) readers

This technology has already been mentioned in the description of contactless credit/debit card transactions.

Radio frequency identification (RFID) readers use radio waves to read and capture information stored on a **tag**. The tag can be read from a distance of several metres, which is one of its advantages over the barcode system. The RFID tag is made up of two components:

- a microchip that stores and processes information
- an antenna that is used to receive and transmit data/information.

The tags can be passive or battery powered. Passive tags use the reader's radio wave energy to relay the information; battery-powered tags use a small embedded battery to power the RFID.

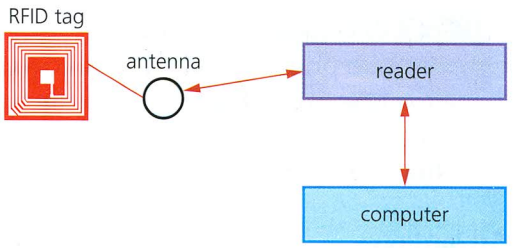


Figure 2.3 Radio frequency identification readers (RFIDs)

Uses

- Livestock tracking (so that the whereabouts of each animal on a farm is known; it also identifies which farm owns the animal).
- Retail (it is similar to barcodes but doesn't require any scanning; details, such as price, can be stored on the tag and then automatically read at a checkout – a big advantage is that several tags can be read at the same time, thus speeding up the checkout process).
- Admission passes (for example, in theme parks RFID cards eliminate the need to scan or swipe people before 'rides', reducing the waiting time; it also allows the tracking of people in the theme park and certain information, such as height or age, can be stored to prevent entry to certain rides on safety grounds).
- Libraries (books can be tracked in and out automatically by readers at the library entrance; no need to scan barcodes or magnetic stripe cards, making the process quicker and more accurate).

Table 2.2 Comparison of OCR and OMR

OCR	OMR
Because this method reads handwriting, it is possible for customers to extend their answers to questions	Since this involves shading in lozenges to answer set questions, the information obtained is limited to the choices offered in each question
This method can read handwriting – but poor handwriting may cause reading errors	OMR relies on simply detecting where marks have been made on a page; the position of the marks is compared to a template stored in memory
OCR is used for converting printed documents to an editable electronic format	OMR simply reads the position of marks, so it is ideal for multiple-choice exam papers
OCR requires a complex recognition system	This method requires complex (and expensive) forms to be completed; but the recognition system is simpler than OCR
Fewer 'how to fill in' instructions are needed for forms designed to be completed and then read by OCR	While this method requires more 'how to fill in' instructions, it is easier and faster for customers to complete OMR forms than to complete OCR forms
While OCR is more accurate than data entered into a computer by keyboard, there are still problems recognising all types of handwriting, leading to inaccuracies	OMR is essentially a more accurate method for reading data than OCR

2.2.6 Barcode readers

Barcode readers are used to read information in the form of a barcode.

The readers are usually in the form of a barcode scanner and are often built into POS terminals in supermarkets. **Hand-held scanners or wands** (as shown in the photograph) are also very common for reading barcodes if portability is required (for example, if the barcodes are on large or fixed objects).

Uses

- Used in supermarkets and other shops where the goods are marked with a barcode; the barcodes are used to give information about the product which enables automatic stock control, itemised billing, etc. to take place.
- Used in libraries to keep track of books on loan.
- Used as a safety function in many companies to ensure that electrical equipment is checked on a regular basis (barcodes are placed on an item to identify it and a database holds all the information related to that barcode so it is possible to interrogate the system as part of a safety audit).

Advantages

- Much faster than keying in data manually and fewer mistakes will be made.
- If used as a way of recording data, they can improve safety.
- They allow automatic stock control.
- They are a tried and trusted technology.

Disadvantages

- Relatively expensive system to administer.
- Not foolproof (barcodes can be swapped around on items).
- Can be more easily damaged than RFID tags or magnetic strips.

Quick response (QR) codes

...her type of barcode is the **quick response (QR) code**. This is made up of a ...r of filled in dark squares on a light background. For example, the following QR code contains the message: 'Cambridge IGCSE ICT textbook Chapter 2'.

- LEDs give a whiter light, which sharpens the image and makes the colours appear more vivid; CCFL had a slightly yellowish tint
- LEDs produce a brighter light, which improves the colour definition
- monitors using LED technology are much thinner than monitors using CCFL technology
- LEDs last almost indefinitely; this makes the technology more reliable and makes for a more consistent product
- LEDs consume very little power, which means they produce less heat as well as using less energy.

What of the future?

Future LED technology will make use of **organic light emitting diodes (OLEDs)**. These use organic materials (made up of carbon compounds) to create semi-conductors that are very flexible.

Organic films are sandwiched between two charged electrodes (one is a metallic **cathode** and the other a glass **anode**). When an electric field is applied to the electrodes they give off light. This means that no form of backlighting is required, which allows for very thin screens. It also means that there is no longer a need to use LCD technology, since OLED is a self-contained system.

As can be seen in the photo, OLEDs allow screens to be curved, which ensures a good picture from any angle.

But the important aspect of the technology is how thin this makes the screen. It will be possible, using OLED technology, to bend screens to any shape. If this is adopted by mobile phone manufacturers, it will be possible to develop phones that can wrap around your wrist – much like a watch strap (see smartwatches earlier).

Imagine screens so thin that they can be folded up and placed in your pocket until they are needed. Or how about using folding OLED displays attached to fabrics creating 'smart' clothing (this could be used on outdoor survival clothing where an integrated circuit, mobile phone, GPS receiver and OLED display could all be sewn into the clothing)?

Science fiction becomes science fact – yet again.

Advantages of using OLED compared to existing LED and LCD monitors/screens:

- the plastic, organic layers of an OLED are thinner, lighter and more flexible than the crystal structures used in LEDs or LCDs
- the light-emitting layers of an OLED are lighter; OLED layers can be made from plastic rather than the glass as used in LED and LCD screens
- OLEDs give a brighter light than LEDs
- OLEDs do not require backlighting like LCD screens – OLEDs generate their own light
- since OLEDs require no backlighting, they use much less power than LCD screens (most of the LCD power is used to do the backlighting); this is very important in battery-operated devices such as mobile phones
- since OLEDs are essentially plastics, they can be made into large, thin sheets (this means they could be used on large advertising boards in airports, subways, and so on)
- OLEDs have a very large field of view, about 170 degrees, which makes them ideal for use in television sets and for advertising screens.

layer using powdered stone until the final object was formed. The subtractive method would involve carving the statue out of solid stone (that is, removing the stone not required) until the final item was produced. Similarly, **CNC** (computer controlled machine – a type of lathe) removes metal to form an object; 3-D printing would produce the same item by building up the object from layers of powdered metal.

- **Direct 3-D printing** uses inkjet technology; a print head can move left to right as in a normal printer. However, the print head can also move up and down to build up the layers of an object – each layer being less than a tenth of a millimetre (< 0.1 mm).
- Binder 3-D printing is similar to direct 3-D printing but this method uses two passes for each of the layers: the first pass sprays dry powder then, on the second pass, a binder (a type of glue) is sprayed to form a solid layer.
- Newer technologies are using lasers and UV light to harden liquid polymers; this further increases the diversity of products that can be made.

The steps in the process of producing an object using 3-D printers is summarised in Figure 2.4.

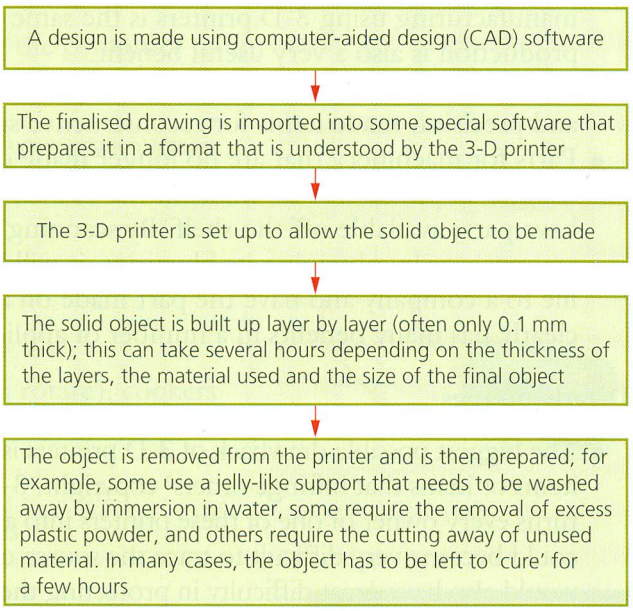


Figure 2.4 Creating a solid object using 3-D printers

3-D printing is regarded as being possibly the next 'industrial revolution' since it will change the manufacturing methods in many industries. The following list is just a glimpse into what we know can be made using these printers; in the years that follow, this list will probably fill an entire book:

- prosthetic limbs can be made to fit exactly on to the injured body part
- making items to allow precision reconstructive surgery (for example, facial reconstruction following an accident); the parts made by this technique are more precise in their design as they can be made from exact scanning of the skull
- in aerospace, manufacturers are looking at making wings and other aeroplane parts using 3-D technology; the bonus will be lightweight, precision parts
- fashion and art – 3-D printing allows new creative ideas to be developed
- making parts for items no longer in production, for example, parts for a vintage car.

These are just a few of the exciting applications that make use of this new technology.

Exercise 2d

Use the internet to research some new and innovative 3-D printing applications.

Advantages

- The manufacturing of items has become much easier than ever before. It is now theoretically possible to manufacture any product a user wants using only a 3-D printer. This has led the way for customised products, as it allows a user to create their own designs in 3-D and have them printed in solid form.

Data packets

The data is carried in the packet according to which protocol (set of rules) is used. Packets of data usually contain the following information:

- some form of header to identify the data packets
- the sender's IP address
- the receiver's IP address
- how many data packets make up the whole 'message'
- the identity number of each packet.

This information allows the router to route a packet across a network to its correct destination and allows the data packets to be reassembled in their correct order according to identity number at the receiving station.

When a router receives a packet of data, it checks the destination IP address against the stored routing table. The routing table stores the MAC address of the device, the assigned IP address and the lease time the IP address is assigned for. The bits forming the destination IP address in the data packet are used to point to the correct route. The packet is sent to a number of routers until it reaches its final destination.

Note: MAC addresses and IP addresses are discussed in more detail later.

Other hardware

Gateway

A **gateway** is a network point (or **node**) that acts as an entrance to another network. It is a key point for data on its way to or from other networks. All networks will have boundaries so that all communication within the network is conducted using devices such as switches or routers. If a network node needs to communicate outside its network, it needs to use a gateway.

Network interface card (NIC)

A **network interface card (NIC)** is needed to allow a device to connect to a network (for example, the internet). It is usually part of the device hardware and frequently contains the MAC address generated at the manufacturing stage.

Network cables

Even though many computer systems use Wi-Fi, **network cables** are still used because they have the following advantages over Wi-Fi:

- faster data transfer rates
- can be more secure than wireless networks.

The cables can be either copper or fibre optics – the latter offers higher data transfer rates and also better security (see notes on quantum cryptography).

4.1.2 Internet protocol (IP) and media access control (MAC) addresses

Each device on the internet is given a unique address known as its **internet protocol (IP) address**. This is a 32-bit number that is usually written in the form:

109.108.158.1

A home computer is given an IP address when it connects to the internet. This is assigned by the ISP and is unique for that particular internet session. The only IP addresses that remain fairly unchanged are the web servers. An IP address can be used instead of typing in the full URL; for example, http://109.108.158.1 would take you straight to the device containing web page corresponding to this address.

Bluetooth creates a secure **wireless personal area network (WPAN)** based on key encryption.

Table 4.1 summarises some of the differences between Wi-Fi and Bluetooth.

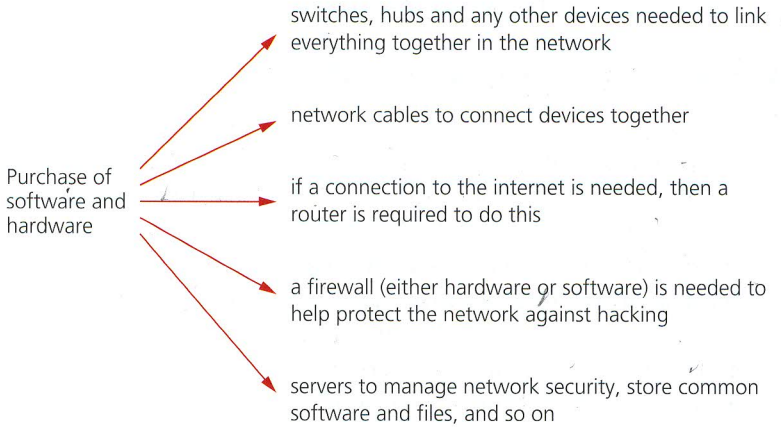
Table 4.1 Differences between Wi-Fi and Bluetooth

Feature	Bluetooth	Wi-Fi
Transmission frequency used	2.4 GHz	2.4, 3.6, 5.0 GHz
Data transfer rate (maximum)	25 Mbits/second (~3.1 Mbytes/second)	250 Mbits/second (~31 Mbytes/second)
Maximum effective range (metres)	30 m	100 m (but can be obstructed by walls etc., reducing effective range to only a few metres)
Maximum number of devices connected	Up to 7	Depends on the router used (can be one device or many devices)
Type of data transmission security	Key matching encryption	WEP (wireless equivalent privacy) and WPA (Wi-Fi protected access) are the most common security systems

4.1.4 How to set up and configure a small network

Suppose you were asked to set up and configure a small network of 10 computers. You would need to consider the following points:

Apart from all the hardware and software, you would also have to think about doing the following:



- setting up an IP account if internet access is required
- setting up the system (or buying appropriate hardware correctly configured) to allow for wireless connectivity
- configuring all the hardware and software so that they work correctly together
- if internet is required, ensuring that a high-speed broadband connection exists
- putting all the common software onto a server and also making sure that a network licence has been acquired so that all network users can make use of the software
- setting up privileges so that each user can only access their own area or common shared area
- setting up a network-manager-level of privilege do that they can monitor network usage, change passwords, etc.

Exercise 4a

Find out any other hardware or tasks that need to be carried out when setting up a small network. Ask questions such as 'would Wi-Fi or Bluetooth be the best type of connectivity?', 'Should PCs or laptops be used?', and so on.

4.1.5 Internet, intranets and extranets

The main features of the internet, intranets and extranets, and the differences between them, are covered at length in Chapter 10. Read Chapter 10 if you wish to cover this topic in some depth before carrying on with the rest of this chapter.

4.1.6 Local area networks (LANs) and wide area networks (WANs)

Local area networks (LANs)

These systems are usually within one building, or certainly not very far away from each other geographically. A typical LAN will consist of a number of computers and devices (for example, printers) that are connected to **hubs** or **switches**. One of the hubs or switches will usually be connected to a **router** and a **modem**

4.2.4 Data protection acts

Most countries have some form of **data protection act (DPA)**. These are designed to protect individuals and to prevent incorrect or inaccurate data being stored.

Essentially DPAs are set up to protect the rights of the individual about whom data is obtained, stored and processed (i.e., collection, use, disclosure, destruction and holding of data). Any such act applies to both computerised and paper records.

Many data protection acts are based on eight principles, as outlined in Figure 4.10.

In many countries, failure to abide by these simple rules can lead to a heavy fine or even imprisonment to anyone who holds data about individuals.

There are general guidelines about how to stop data being obtained unlawfully:

- don't leave personal information lying around on a desk when not attended
- lock filing cabinets at the end of the day or when the room is unoccupied
- do not leave data on a computer monitor if it is unattended; log off from the computer if away from your desk for any length of time
- use passwords and user ids, which should be kept secure; passwords should be difficult to guess/break and should be changed frequently (see earlier notes on passwords)
- make sure that anything sent in an email or fax (including attachments) is not of a sensitive nature.

All of the above are in addition to other security safeguards discussed elsewhere in this book.

1. Data must be fairly and lawfully processed.
2. Data can only be processed for the stated purpose.
3. Data must be adequate, relevant and not excessive.
4. Data must be accurate.
5. Data must not be kept longer than necessary.
6. Data must be processed in accordance with the data subject's rights.
7. Data must be kept secure.
8. Data must not be transferred to another country unless they also have adequate protection.

Figure 4.10 Main principles of data protection acts

4.2.5 Network communication

Faxes and emails

There are two basic ways of sending a fax (abbreviation for facsimile – a copy):

- a physical fax (a dedicated machine connected to a telephone line; it requires the number of the recipient to be dialled before the document is copied and then sent electronically)
- electronic faxing (this requires a network, such as the internet, for the fax to be sent).

Physical fax machines

Fax machines have been used for many years to send and receive paper documents.

A standard fax machine allows documents to be sent to another fax machine using a normal telephone line. The user places the document in the fax machine tray, lifts the receiver and dials the fax number of the recipient and then presses <send>. At the receiving end, the document is printed on another fax machine. It can be quite a slow way to send a document if the fax line is busy or if there are several pages to send.

However, a more modern way is **electronic faxing** (or online faxing) which makes use of computer technology and the internet. Electronic faxing has the following advantages over the more traditional method described above:

- costs are reduced as there is no need to buy a fax machine, ink/toner or paper
- transfers using electronic methods are encrypted, improving security
- transmissions are sent to an email account, which is password protected
- there is no issue of a 'busy signal' preventing the fax being sent.

At this point you may be wondering what is the difference between an electronic fax and an email? The simple answer is not a lot. The only real difference is that online faxing is always associated with an email address *and* a fax number. The fax number is similar to the traditional fax number and needs to be known by the sender. Having this number allows a user to send fax messages to the recipient. Once a fax is received, the online fax service provider sends an email with the fax message attached in a tiff or pdf format. The sender of the fax can either use an email account or log into any online account to send the fax.

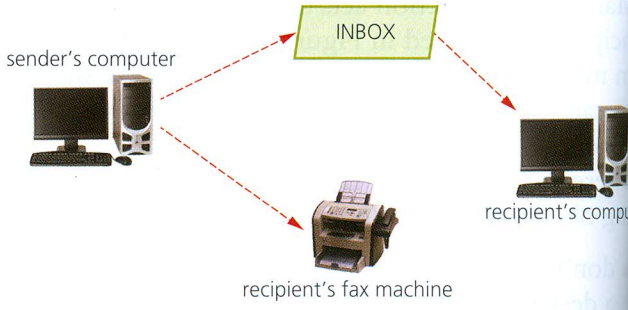
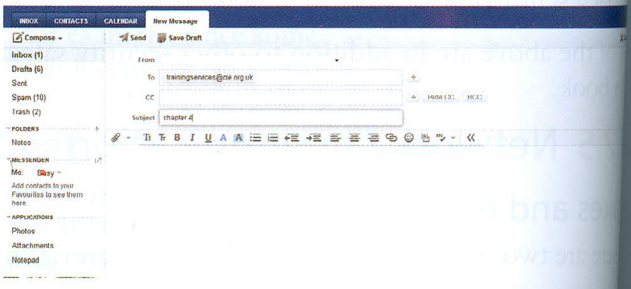


Figure 4.11 Sending an electronic fax

It is important to realise that it is possible to send a fax from your computer to another device connected to the internet *or* to a traditional fax machine, where the document will be printed out in the normal way.

Emails

Electronic mail (email) is discussed in many parts of this book. Emails are particularly useful when sending attachments (for example, documents, videos, music, and so on). Emails can be sent to, or sent from, any device connected to the internet. When sending attachments it is usually important to have a good, stable internet connection – particularly when sending or receiving large files. The basic difference between emails and electronic faxes was described above; all the advantages and disadvantages of emails apply to electronic faxing when it is sent from computer to computer.



Emails require an account with an ISP. When sending an email, it is necessary to include the email address (which **must** be exact), a subject line and any attachments if required.

The recipient simply has to log on to their account and read the emails in their inbox.

It is now worth comparing emails with traditional, physical faxes (as indicated above, there are few differences between electronic faxes and emails so they won't be part of this comparison).

As the name suggests, they can be used to make phone calls from any location within the cellular network; this has advantages over the more conventional landline system:

- there is no need to look for an operational public telephone in an emergency
- it is possible to conduct business or personal phone calls on the move
- it is easier to keep in contact with co-workers at the office no matter where you are.

They allow text messaging:

- this is quicker and less expensive than making phone calls
- also text messages can be sent at any time of the day even if the recipient's phone is switched off
- they employ predictive texting where the system completes a word from the first few letters keyed in e.g. key in 'preci' and the phone completes the word as 'precious'; predictive texting also allows the system to remember frequently used words – together they increase typing speed.

Mobile phones allow access to the internet on the move using either the cellular network or a Wi-Fi 'hot spot'.

6.1.7 Internet telephony

One of the most common forms of internet telephony (i.e. having a telephone conversation via the internet) is **Voice over internet Protocol (VoIP)**.

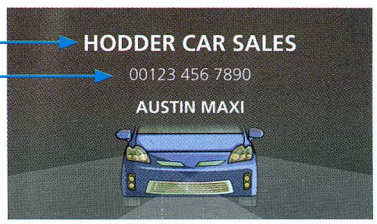
Voice over internet protocol (VoIP) is a method used to talk to people using the internet. VoIP converts sound (picked up by the computer microphone or special VoIP telephone plugged into the USB port of the computer) into discrete digital packets which can be sent to their destination via the internet. One of the big advantages is that it is either free (if the talking is done computer to computer i.e. both computers have VoIP telephones or use their built in/plugged in microphones and speakers) or at a local rate to anywhere in the world (when VoIP is used to communicate with a mobile or land line telephone rather than another computer). Obviously, to work in real time this system requires a broadband ISP. The main problems are usually sound quality (echo and 'weird sounds' are both common faults). Security is also a main concern with VoIP, as it is with other internet technologies.

One of the big advantages of using VoIP is that a webcam can also be used so that it becomes a type of video chat. Whilst this doesn't have the sophistication of a video conference, it is much cheaper (no need for special software and additional hardware items – VoIP uses built-in microphones, speakers and webcams). Usually the video quality is not very good, but this can be improved by using a more expensive webcam connected to one of the computer's USB ports.

6.1.8 Business cards and letterheads

Many IT companies offer to produce business cards and letterheads to any design. The user connects to an appropriate website and they will be given a number of business card templates. The user chooses a template and keys in data such as:

- name of company
- contact details
- image wanted on the business card.



6.4.4 Glasshouse environment control

Five different sensors could be used here to control the glasshouse environment; namely, humidity, moisture, temperature, pH and light. To simplify this problem the control mechanisms are shown in Figure 6.7.

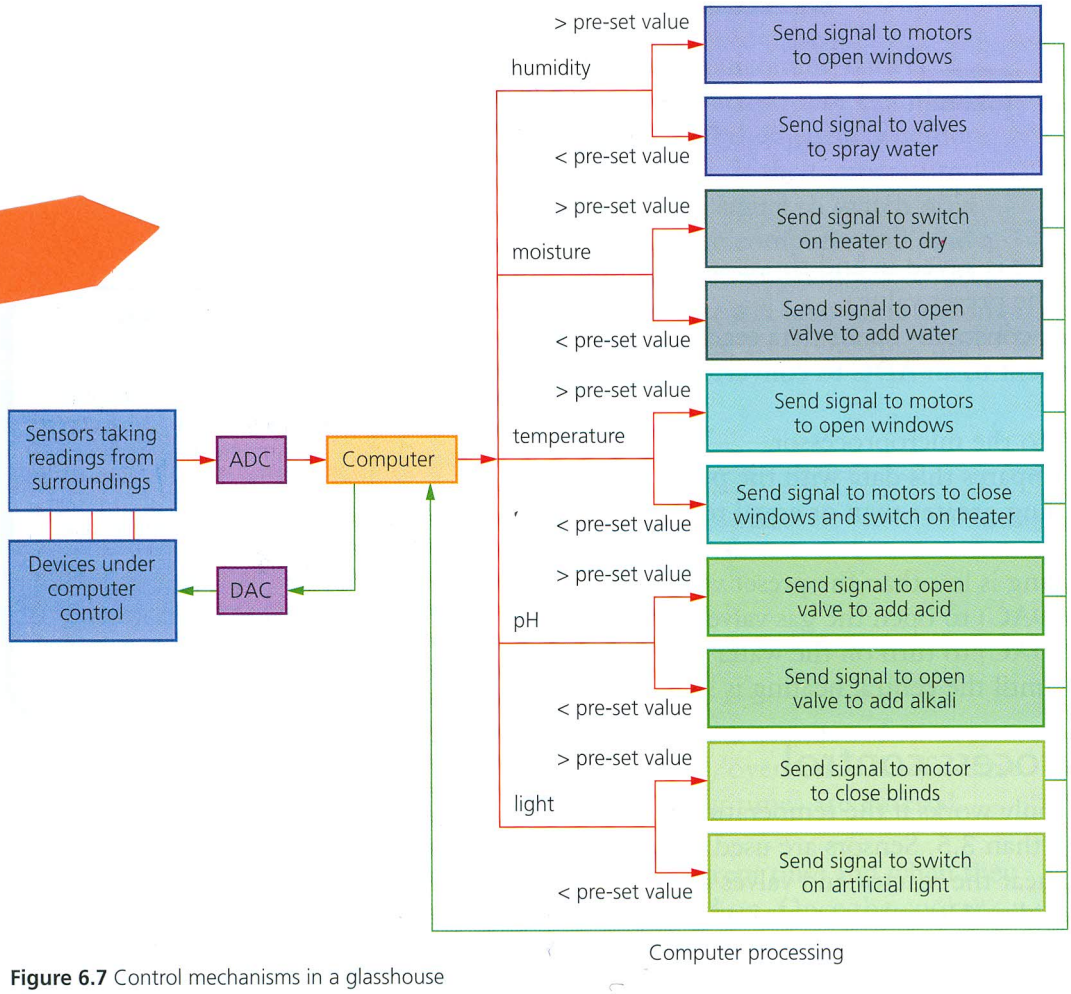


Figure 6.7 Control mechanisms in a glasshouse

Because of the number of sensors, this is clearly quite a complex problem. Let us consider the humidity sensor only. This sends a signal to an ADC which then sends a digital signal to the computer. This compares the input with stored (preset) values and decides what action needs to be taken (follow the orange lines in the diagram above). If humidity is greater than (>) the preset value, the computer sends a signal to a DAC to operate the motors to open windows thus reducing the humidity. If it is less than (<) the preset value, the computer sends a signal to open valves to spray water into the air (follow the green lines in the diagram above). If the reading is the same as the preset value, then no action is taken (this isn't shown in the diagram since it could follow either direction). The control process continues as long as the system is switched on. Similar arguments can be used for all five sensors.

The table on the next page gives a list of possible sensors that might be used in various applications which involve measurement or control.

6.6 Manufacturing applications

Manufacturing uses ICT (i.e. automation) in a number of areas to improve productivity, reduce costs, improve consistency and to make factories safer and more environmentally friendly.

One of the most common forms of automation is the use of robots.

Robotics

Robots are used in many areas of manufacturing, from heavy work right through to delicate operations. Examples include: paint spraying of car bodies, welding bodywork on cars, manufacturing of microchips, manufacturing electrical goods and automatic warehouses.

Control of robots is either through embedded (built-in) microprocessors or linked to a computer system. Programming of the robot to do a series of tasks is generally done in two ways:

1 The robot is programmed with a sequence of instructions which allow it to carry out the series of tasks (e.g. spraying a car body with paint).

2 Alternatively, a human operator manually carries out the series of tasks; this can be done in two ways. In our example, we will assume an object is being painted using a robot arm.

i The robot arm is guided by a worker when spraying the object; each movement of the arm is stored as an instruction in the computer.

OR

ii The worker straps sensors to his own arm and sprays the object; each movement is stored as a set of instructions in a computer; the sensors send back information such as position relative to the object, arm rotation, and so on – this information forms part of the instructions stored in the computer.

Whichever method is used, once the instructions have been saved, each series of tasks can then be carried out by a robot arm automatically. Each instruction will be carried out identically every time (e.g. assembling parts in a television) giving a consistent product.

Robots are often equipped with sensors so they can gather important information about their surroundings and also preventing them from doing 'stupid things' e.g. stopping a robot spraying a car if no car is present, or stop the spraying operation if the supply of paint has run out, etc.

Robots are very good at repetitive tasks. However, if there are many different tasks (e.g. making specialist glassware for some scientific work) then it is often better to still use human operators.

Figure 6.8 Robot arm equipped with a spray gun 'end effector'. Different end effectors allow the robot arm to carry out many different tasks

and date on the database. This would give a very comprehensive record of when the student attended the school and the number of hours they attended. It would also be a more secure method in the event of, for example, a fire. The school would now be able to account for every student currently showing as being present on the school premises. Using the paper-based system, a student could register then just go home – with this ID card system, the student's attendance would be known at all times.

There are further subtleties that could be used such as (1) use of a PIN to stop another student swiping in with the wrong card (2) use of GPS tracking (see Section 6.16.1) so the exact whereabouts of a student would be known; this would require the addition of a chip in the ID card so that the tracking system could identify them (this is the basis of RFID which was discussed in Chapter 2). At the end of a term (or school year), the database could be interrogated and it would give an accurate attendance record for the student.

Method 2

A second method could make use of biometrics. Each student would have their fingerprints taken. Their personal details (as in method 1) plus fingerprints would be stored on a database. When a student entered the school premises, they would be asked to put their hand on a scanner which would read their fingerprints. Since each student would have unique fingerprints, this system would be very secure. As with method 1, the date and time of entering or leaving the school would be accurately recorded on the database.

Advantages

- Fingerprints are unique, so it would be impossible for a student to sign in pretending to be someone else (with magnetic cards, a student could give his card to a friend and ask them to sign in for him) – this gives more accurate data and improved security.
- ID cards could easily be lost – fingerprints are 'part of you' so can't be lost.
- ID cards could be affected by magnetic fields (e.g. by being placed close to a mobile phone) which would stop them working.
- It is much easier to 'clone' (i.e. make copies of) ID cards than it would be to copy fingerprints (not impossible but very difficult).

Disadvantages

- It would take a long time to collect the initial fingerprints for every student in the school.
- The equipment needed to take and read fingerprints is more expensive than magnetic stripe reading equipment.
- If a student cuts a finger, the fingerprint may not be identified by the system (which would prevent entry to the school).
- There are 'invasion of privacy' issues and some parents may object to having the fingerprints of their children stored on a database.

6.7.2 Student performance

Teachers could make considerable use of spreadsheets to monitor the performance of their students. This was discussed in Section 5.1. Essentially, spreadsheets could record the test results of each student over a term/year. This would allow a teacher easily to see how they were performing against other

Databases also allow a quick and easy search for patient records – this could be very important in an emergency, for example, when accessing the patient's medical history could mean the difference between life and death. It also means that medication can be prescribed without issuing paper prescriptions – an email could be sent to the pharmacy.

The sort of data which would be required on a patient database is as follows:

- a unique identification number
- name and address
- date of birth
- gender (male or female)
- medical history (e.g. recent medicine/treatment)
- blood group
- any known allergies
- doctor
- any current treatment
- any current diagnosis
- important additional information such as X-rays, CT scans, and so on.

6.11.2 Monitoring patients

Note: See also Section 6.3.

By connecting a patient to a computer system, it is possible to carry out 24-hour monitoring of the patient. The computer can monitor:

- heart rate
- respiration (breathing rate)
- brain activity
- blood/body temperature
- blood pressure
- blood sugar levels
- oxygen levels in the blood.

This is not an exhaustive list, by any means.

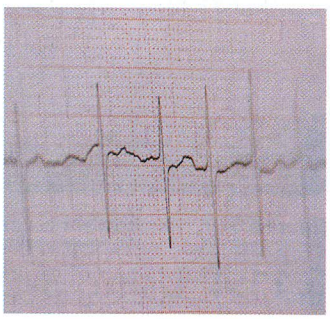


Figure 6.11 Heart beat trace

The results are shown on a monitor in the form of a digital read-out and/or graphical read-out.

Digital read-outs give the nurse or doctor an immediate value; graphical representations are used to show trends over a period of time. Both methods supply different information. There is often sound output as well in the form of beeps to indicate that the machine is working. It also indicates, for example, the heart rate and gives a warning if the patient's condition suddenly deteriorates. All of these outputs give the nurses and doctors useful information.

As discussed in Section 6.3, the system relies on sensors attached to patients and to a computer system that interprets the sensor data and converts it into a format useful to the nurses and doctors. Using sensors and computers has many advantages over taking readings manually:

- it is more accurate; using a computer system almost removes any chance of error
- they can operate 24/7 and don't require any breaks or get tired
- they never forget to take readings – a nurse could be too busy for example
- readings can be taken more frequently using computer systems
- they are capable of responding much faster to any change in the patient's condition

Some 3-D printers produce hard nylon objects which are used in certain pre-surgical planning. If a patient has suffered a bone break, for example, surgeons can physically test and position screws and plates in the '3-D bone nylon image' prior to the surgery taking place. This reduces the chance of any errors when the actual procedure is carried out.

Prosthetics

3-D printers are now being used to print out prosthetics (false arms, hands and legs). Whilst state-of-the-art myoelectric prosthetics cost tens of thousands of dollars, the price for 3-D printing a prosthetic arm or hand can be as little as $100.

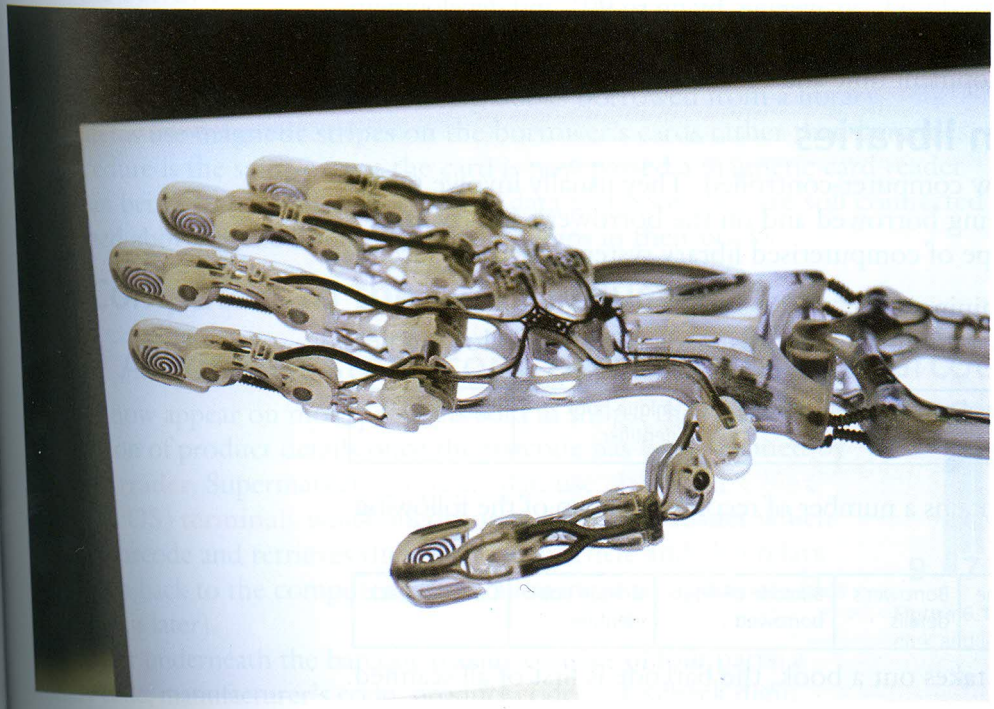


Figure 6.13 This image shows a prosthetic arm produced by a 3-D printer. Whilst the technology may not be cutting-edge, it can be life-changing to an amputee.

There is still much research needed in this field. However, the results to date are very encouraging with many more people from poorer countries now having a chance to replace missing limbs at a fraction of the cost compared to existing methods.

Tissue engineering

Recent advances have allowed the 3-D printing of bio-compatible materials, cells and supporting structures. This has improved the viability of the function of cells within a 3-D printed object. 3-D bio-printing is a very complex process and requires the input from biologists, medical engineers, physicists and other engineers. It has already been used successfully to produce multilayered skin tissue, bone tissue, heart/artery grafts and tracheal splints.

The procedure involves making biological materials by diffusing cells into a bio-compatible scaffold. The bio-printed tissue is then put into an incubator and the cell structure held within the scaffold grows to form actual cellular tissue.

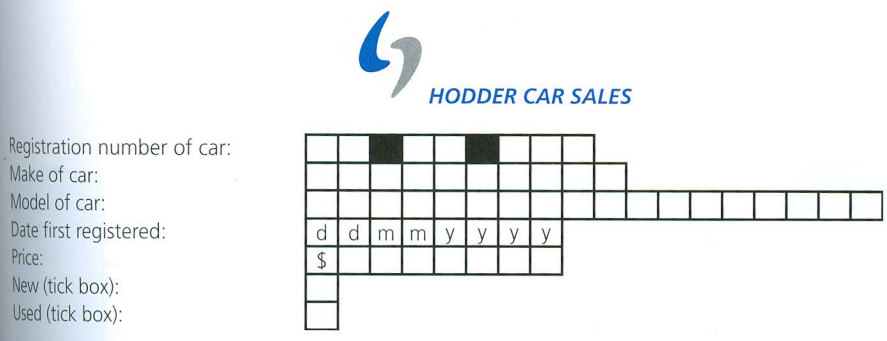


Figure 7.6 Paper-based data capture form

A computer-based data capture form is slightly different. These often have the following features:

- use of text boxes to capture key data clearly
- use of on-screen help when completing the form
- use of drop-down/combo boxes where there are limited choices
- use of radio buttons and tick boxes, requiring a single click of a mouse to select
- automatic validation of data as it is entered
- control buttons (such as next form, clear entry, save, etc.)
- double entry boxes (with verification rules) to check correctness of key data (for example, when keying in an email address).

In the car sales example shown above, the following differences could be used with a computer-based data capture form:

- **registration number**: same as paper-based form
- **make of car**: make use of a drop-down box as there is a limited number of manufacturers
- **model of car**: same as paper-based form
- **date first registered**: use of drop-down boxes for day, month and year
- **price**: use boxes as shown but include a validation check
- **new or used**: use of tick box or radio button to indicate option
- **other features**: a back and forward button (to complete details of all cars), and a save button when form is complete for each car.

Exercise 7b

Design a computer-based data capture form using the fields given above. Remember that it has to be completed online, so it should include radio buttons, drop-down boxes and so on. It should look a little different to the paper-based form shown in Figure 7.6.

7.2.2 Screen displays and printed reports

The output from any system needs careful consideration since this is part of any user interface and is also the result of some form of processing. Screen outputs should be designed:

- to make sure the size of all the output fields is correct
- so that any instructions/descriptions are clear
- so that the full screen is utilised (avoiding large areas of 'nothing')
- so that colours and fonts (size and type) make the output clear.

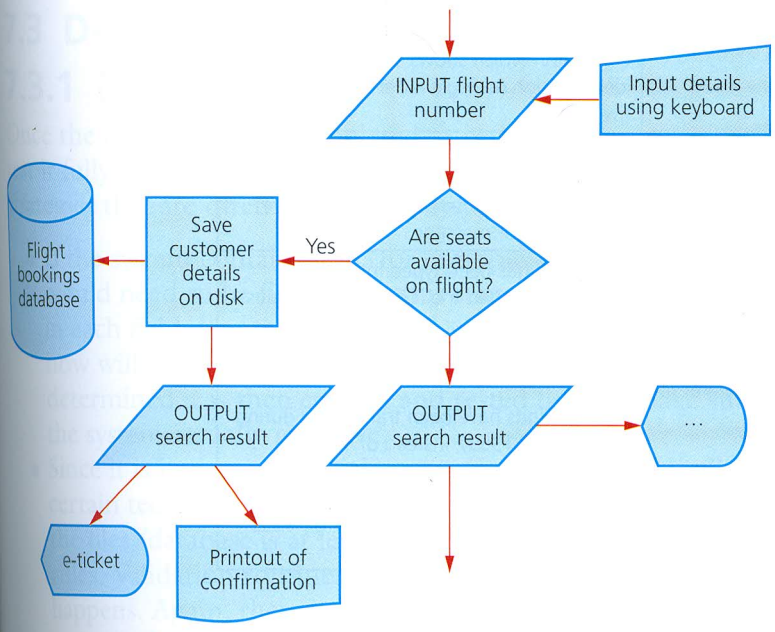


Figure 7.9 Sample system flowchart

7.2.4 Verification

Verification is a way of preventing errors when data is copied from one medium to another (for example, from paper to disk/CD). There are two common ways that verification checks are carried out.

- **Double entry**: in this method, data is entered **twice**, using two people, and is then compared (either after data entry or during the data-entry process).
- **Visual check**: this is the checking for errors by the person who is entering the data; they compare the entered data with the original document (i.e., what is on the screen is compared to the data on the original paper documents – note that this is **not** the same as proofreading).

7.2.5 Validation

Validation is a process where data is checked to see if it satisfies certain criteria when input into a computer; for example, to see if the data falls within accepted boundaries. A number of validation techniques exist; Table 7.2 highlights some of the more common checks used when writing computer software.

Table 7.2 Validation checks

Validation check	Description	Example(s) and comments
Range check	checks whether data is within given/ acceptable values	e.g. to check if a person's age is > 0 but is also < 150
Look-up check	this checks whether the data entered exists and is stored in a table of data	e.g. check is 'senior manager' exists as on option in the query such as: 'PLEASE ENTER YOUR JOB TITLE'
Length check	checks if the input data contains the required number of characters	e.g. if a field needs six digits then inputting a five-digit or seven-digit number, for example, should cause an error message
Character/type check	checks that the input data doesn't contain invalid characters	e.g. a person's name shouldn't contain any numbers, but a person's height should only contain digits

ontinued...

- make sure you exercise every hour or so to prevent the health risks outlined Table 8.1 from becoming a real issue
- carry out an 'ergonomic assessment' on your work station (there are numerous online questionnaires that will enable you to check whether your work station is set up properly for your own health and safety); it may require you to buy new chairs or computer hardware to minimise the impact of sitting in front of screens or typing for long periods at a time.

8.2 E-safety

First of all, what is the definition of **e-safety**? It refers to safety when using the internet, i.e. keeping personal data safe and applies to any of the following devices:

- mobile phone
- computer or tablet
- games console
- wireless technology.

Personal data refers to any data concerning a living person who can be identified either from the data itself or from the data in conjunction with other information (for example, 'Peter Smith has blue hair and lives at 40 Green Street' would very clearly identify this individual).

Examples of personal data include:

- name
- address
- date of birth
- medical history
- banking details.

Some personal data is often referred to as **sensitive personal data** and includes:

- ethnic origin
- political views
- religion
- sexual orientation
- criminal activity.

Exercise 8a

Do some research and find out why it is important that personal data is kept confidential. Present your notes as an article to discuss with the rest of the class.

E-safety also refers to the benefits, risks and responsibilities when using ICT. The following list is by no means exhaustive but gives some idea of the e-safety issues that can be encountered by users of ICT hardware:

- don't give out **any** personal information to people who are unknown to you; this is especially true online where it isn't possible to physically meet people so that their motives can be fully assessed. Remember that anyone can say anything they want online and it is very difficult to determine whether they are genuine or not
- don't send people photos of yourself – either online or via a mobile phone – unless the person is known to you (it is very easy for somebody to pass

8.3.2 Phishing

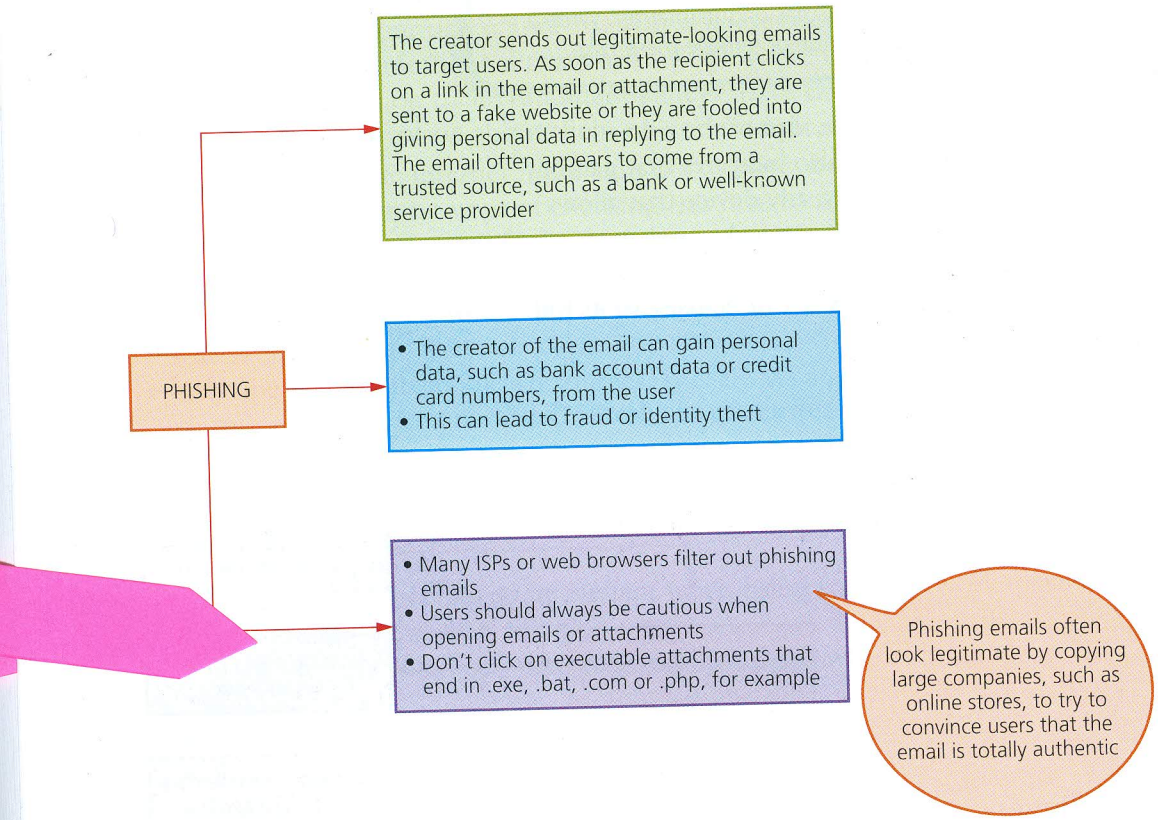


Figure 8.3 Phishing

Malicious use refers to, for example, deletion, fraud, identity theft and selling on personal data. A good example of a phishing attack is when a user is sent an email saying they have ordered an item from an online store. They will be asked to click on a link to see the order details. The link takes the user to a page that shows a product code from a well-known company. A message such as: 'if this order wasn't made by you, please fill out the following form to cancel your order in the next 24 hours' is given. The form will ask for details such as credit card number, user's address and so on. Some of the key clues are that links, such as how to 'contact us', don't work.

Smishing – short for SMS phishing – uses the SMS system of mobile phones to send out fake text messages. It is very similar to phishing as described earlier. These scams often contain a URL or telephone number embedded in the text message. The recipient will be asked to log on to the website or make a telephone call. If they do, they will be asked to supply personal details such as credit/debit card numbers or passwords. As with phishing attacks, the text message will appear to come from a legitimate source and will make a claim, for example, that they have won a prize or that they need to contact their bank urgently. Most people believe that only computers are liable to security threats; mobile phones aren't at risk. This makes smishing a particularly dangerous security threat to many people.

Vishing (voice mail phishing) is another variation of phishing. This uses a voice mail message to trick the user into calling the telephone number contained in the message. As with all phishing attacks, the user will be asked to supply personal data thinking they are talking to a legitimate company.

- Look out for check boxes that are already selected when items are bought online; companies sometimes add a check box (which is already selected) to indicate that you have agreed to sell or give your email address to third party users; make sure that this check box is 'unticked' so that your email address can't be shared.
- Do not sign up to commercial mailing lists.
- Do not reply to an email or unsubscribe from a mailing list that you did not explicitly sign up to in the first place.

8.3.7 Moderated and unmoderated forums

A **moderated forum** refers to an online discussion forum in which all the posts are checked by an administrator before they are allowed to be posted. Many users prefer this type of forum, compared to an unmoderated one, as the moderator can not only prevent spam, but can also filter out any posts that are inappropriate, rude or offensive, or even those that wander off the main topic.

The internet is essentially an **unmoderated forum**. No one 'owns' the internet, and it is essentially not policed (this is discussed in more depth in Chapter 9). The only real safeguards are a voluntary cooperation between the users and the network operators. However, most social forums or networking groups on the internet have a set of rules or protocols that members are requested to follow or they will be deleted.

8.3.8 Cookies

Cookies are small files or code that are stored on a user's computer. They are sent by a web server to a user's computer. Each cookie is effectively a small look-up table containing pairs of (key, data) values; for example (surname, Jones) and (music, rock). Once the cookie has been read by the code on the web server or user's computer, the data can be retrieved and used to customise the web page for each individual. These are often referred to as user preferences. For example, when a user buys a book online, the cookies remember the type of book the user chose and the web page will then show a message such as: 'Customers who bought *Cambridge IGCSE ICT* also bought *Cambridge IGCSE Computer Science*'.

The data gathered by cookies forms an **anonymous user profile** and doesn't contain personal data such as passwords or credit/debit card numbers. Cookies are a very efficient way of carrying data from one website session to another, or even between sessions on related websites. They remove the need to store massive amounts of data on the web server itself. Storing the data on the web server without using cookies would also make it very difficult to retrieve a user's data without requiring the user to login every time they visit the website.

Use of secure servers is always advised. A secure web server is one that supports any of the major security protocols, such as SSL/TLS, that encrypt and decrypt messages to protect them against third party eavesdropping. Making purchases from a secure web server ensures that a user's payment or personal information can be translated into a secret code that's difficult to break.

8.4 Additional security of data online

This section discusses additional ways of keeping data secure when accessing external systems, such as the internet. We will consider:

- firewalls
- security protocols
- encryption
- authentication.

- using spam filters to remove suspicious emails to a 'junk folder' or even to block the email entirely
- running anti-virus and anti-spam software at all times on your computer to protect against emails from unknown or malicious sources.

Emails are said to be vulnerable to both **passive** and **active** attacks. Passive attacks include the release of email material to other users without your consent. Active attacks involve the modification of your messages or even denial of service (i.e., overloading your system by sending thousands of emails, which basically 'clogs up' your computer and makes internet access almost impossible). Active attacks can also involve viruses or phishing attacks (these are covered elsewhere in the book).

Netiquette

Netiquette is a shortened form of the phrase inter**net** et**iquette**, which refers to the need to respect other users' views and display common courtesy when posting views in online discussion groups or when sending out emails. It is very important to consider what you write always since the reader can't see your facial expressions or body language. What may have been intended to be humorous could offend somebody if they misunderstand your message and make the wrong conclusions. Always be aware of this when posting messages or sending emails.

There are a number of rules governing netiquette – one such source is *The Core Rules of Netiquette* by Virginia Shea (published in 1994); but the following diagram gives the reader some idea of what constitutes netiquette.

Figure 10.2 Rules of netiquette

- **portable network graphics**: these files have a **.png** file extension. It is a file format that compresses graphics (image) files without any loss of image quality. It was created to replace graphics interchange format and is now the most-used **lossless compression** format used for images on the internet.
- **moving picture experts group layer 4**: these files have a **.mp4** file extension. It is not a single file format; it is a multimedia **container** that is used for storing video files, still images, audio files, subtitles and so on. This container is often used to transfer video files on the internet.

Common generic audio files include:

- **moving picture experts group layer 3**: these files have a **.mp3** file extension. It is a compressed file format used for storing audio files. This format cannot store still or moving images. The file sizes are relatively small but have near CD quality, which makes them suitable for use on the internet.

Common generic files used for website authoring include:

- **cascading stylesheet**: these files have a **.css** file extension. This is a stylesheet that is saved in cascading stylesheet format and attached to one or more web pages (often written in HTML) to define the pages' colour scheme, fonts and so on.
- **hyper text markup language**: these files have a **.htm** (or sometimes a .html) file extension. This text-based language is used to create markup that a web browser will be able to display information as a web page.

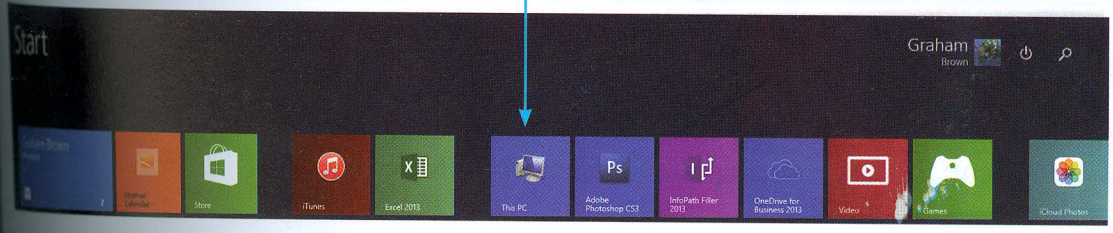
Common generic compressed files include:

- **Roshal archive**: these files have a **.rar** file extension. This is a container that can hold almost any file types in a compressed format. It is used to reduce the number of bytes needed to save a file, either to save storage space or to reduce transmission time when sent from one device to another. It was developed for Windows by Russian software engineer Eugene Roshal (and takes its acronym from '**r**oshal **ar**chive').
- **zip**: these files have a **.zip** file extension. This is a container that can hold almost any file types in a compressed format. It is used to reduce the number of bytes needed to save a file, either to save storage space or to reduce transmission time when sent from one device to another.

11.2 Manage files effectively

11.2.1 Locate and open stored files

Make sure that you are familiar with the file structure of your local system. If you are using a stand-alone computer, files are likely to be stored on local hard disks or SSD drives. If you are using a networked system, files are likely to be stored on a network drive, usually in a secure area where only you have access. Each system is different and you must use the 'This PC' icon from the *Windows 8* Start Screen to access these drives.



17.3 Mail merge

17.3.1 What is a mail merged document?

A mail merged document is created to save the repeated typing of similar documents that are designed to be sent to different people. It uses a master document and a source file containing data. Data, like the names and addresses of people to send the letter to, is taken from the source file and placed into a copy of the original document. This is done automatically.

17.3.2 Why are mail merged documents used?

Mail merge is used to save retyping or editing lots of documents. It saves time (and therefore money) and helps to reduce the number of errors that may occur in editing or retyping the document. The most common use of mail merged documents is to produce personalised letters for a number of people. The contents of the letter have parts that are the same for all people and parts that are personal to the reader. When using the mail merge, the parts that are the same for all people only need to be typed once, even if hundreds of letters are to be created. The personal part of this letter is added using a **placeholder**, which will hold the individual information taken from the data source. The placeholders can hold information from a data source and/or instructions called **merge codes** (sometimes called **field codes**). The information from the data source is often a person's name and address, but may also include information about products that they have bought from a company.

You will be given a copy of a document that will become your master document. This contains the parts for all people. You will also be given a source file, which may be a database, spreadsheet or text file. You will need to merge the files into a number of personalised documents.

17.3.3 Create a mail merged document

Create a master document

A master document will usually be supplied to you as a source file. However, if a document to be used as a master document is only small you may be asked to create this document. The source document may be provided in a format suitable for use with any word processor. For example, it might be in a .rtf (rich text format) or a .txt (text format) file. This may need importing or opening in your word processor program and you will need to save it as a word-processor (.docx) file. You will need to import or create the document, carefully spell check and proofread the document and check that it has a consistent layout. You must then save two copies of this document as word-processed (.docx) files, making sure that you have a backup copy before you start to add the placeholders. You may need to go back to this backup copy if you experience any problems.

Task 17f

Use the file **mailmerge.rtf** as the master letter for a mail merge and the file **mmstudents.csv** as the data source file. In the master letter:

- insert relevant merge fields from the data source file to replace the text shown in chevrons, e.g. <field>
- replace the text <Date> with today's date in DD MMMM YYYY format
- replace the *Headteacher's name* with your name.

Save the file.