IGCSE Computer Science CIE

YOUR NOTES

5. The internet and its uses

CONTENTS

5.1 The internet and the World Wide Web

The Internet & WWW

The Internet & WWW

The internet and the world wide web are often used interchangeably, but they are **not the same thing.**

The Internet

- The internet refers to the **global network of computers** and other electronic devices connected together through a system of **routers and servers**
- It is the infrastructure that allows us to **send and receive information**, including email, instant messaging, and file transfers
- The internet also provides **access to other services** such as online gaming, video streaming, and cloud computing

The World Wide Web

- The world wide web, or simply **the web**, is a **collection of websites** and web pages that are **accessed using the internet**
- It was created in **1989 by Tim Berners-Lee**, who envisioned it as a way to share and access information on a global scale
- The web consists of **interconnected documents and multimedia files** that are **stored on web servers** around the world
- Web pages are accessed using a **web** browser, which communicates with web **server** to retrieve and display the content

YOUR NOTES

YOUR NOTES

URL

What is a URL?

- The URL is a **text-based address** that identifies the **location of a resource** on the internet
- It is the **address** of a web page, image, video, or any other resource available on the internet

Components of a URL

- A URL can contain three main components:
  - Protocol
  - **Domain** name
  - Web page / file name
- The protocol is the communication protocol used to transfer data between the client and the server
  - E.g. HTTP, HTTPS, FTP, and others
- The domain name is the **name of the server** where the resource is located
  - It can be a name or an **IP address**
- The web page / file name is the **location of the file** or resource **on the server**
  - It can contain the name of the file or directory where the resource is located
- A URL looks like this:
  - protocol://domain/path
  - E.g. **https://www.example.com/index.html** is a URL that consists of the **HTTPS protocol**, the domain name "www.example.com", and the file name is "/index.html".

YOUR NOTES

Protocols

Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) are the **two most common protocols** used for **transferring data between clients and servers** on the internet.

Hypertext Transfer Protocol (HTTP)

- **HTTP** is the protocol used for **transferring data between a client and a server** on the internet
- It is a stateless protocol, meaning it does not store any information about previous requests or responses
- HTTP operates on **port 80** by default and **sends data in plain text format**, making it **vulnerable to interception** and manipulation

Hypertext Transfer Protocol Secure (HTTPS)

- HTTPS is a **secure** version of HTTP that uses **encryption** to protect data transferred between a client and a server
- It operates on **port 443** by default and uses Transport Layer Security (**TLS**) or Secure Socket Layer (**SSL**) to encrypt data
- HTTPS ensures that data transferred between the client and server is secure, making it **harder for unauthorised users to intercept** or manipulate data

SSL & TLS

- SSL is a **security protocol** developed by Netscape in the 1990s to provide secure communication over the internet
- TLS is a **successor to SSL** and is a security protocol used to provide secure communication over the internet
- They both use a combination of symmetric and asymmetric **encryption** to secure data and ensure data integrity
- SSL operates at the transport layer of the OSI model, ensuring that data is encrypted before it is sent over the network
- The TLS protocol is made up of 2 layers:
    - **Handshake Layer**
        - This is used to establish a secure connection between two endpoints
    - **Record Layer**
        - This is responsible for transmitting data securely between the client and the server
- The client/browser **requests secure connection** to the server
- The client/browser requests the **server to identify itself**
- The server **provides a digital certificate**
- The client/browser **validates** the certificate
- The client/browser sends a **signal** back to the server to **begin data transmission**
- The **encryption method** will be agreed & a **session key** is generated

Exam Tip

- You will only be asked to name the layers of TLS

YOUR NOTES

YOUR NOTES

Web Browser

A web browser is a **piece of software** used to access and **display** information on the internet.

Purpose of a Web Browser

- The main purpose of a web browser is to **render hypertext markup language (HTML)** and display web pages
- Web browsers **interpret the code in HTML** documents and translate it into a visual display for the user

Functions of a Web Browser

- **Render HTML**
  - This will display the webpage
- **Storing bookmarks and favourites**
  - Web browsers allow users to save links to frequently visited websites and access them easily using bookmarks or favourites
- **Recording user history**
  - Web browsers record the user's browsing history, allowing them to quickly revisit recently viewed pages
- Allowing use of **multiple tabs**
  - Web browsers allow users to open multiple tabs and switch between them quickly and easily
- **Storing cookies**
  - Web browsers store cookies, which are small files that contain user preferences and login information for websites
- Providing **navigation tools**
  - Web browsers provide navigation tools, such as back and forward buttons and a home button, to help users move between pages
- Providing an **address bar**

Web browsers provide an address bar, which allows users to enter a URL or search term and navigate to a website or search for information

- **Homepage**
  - This is the initial page that appears when the browser is launched
  - The homepage can be customised to display frequently visited websites or specific content
- Runs **Active Scripts**
  - These are small programs embedded in web pages that allow interactive content such as animations, videos, and pop-up windows to be displayed
- **Download Files**
  - A web browser allows files to be downloaded from the internet, such as documents, images, and software
- **Request Web Pages**
  - When you enter a web address in the address bar, the web browser sends a request to the web server to obtain the contents of the web page

- The server responds by sending the web page to the browser, which displays it on the screen

- **DNS**
  - The web browser sends the URL to the DNS, which translates the URL into an IP address, which is used to locate the web server
- **Manages Protocols**
  - Web browsers manage the HTTP and HTTPS protocols, which are used to transfer data between web servers and browsers
  - HTTP is used for regular web pages, while HTTPS is used for secure pages that require encryption, such as online banking or shopping sites

YOUR NOTES

YOUR NOTES

Web Pages

- When you type in a URL / click on a link the browser sends the URL to the DNS using HTTP
- The DNS finds the matching IP addresses for the URL and sends the IP address to the web browser
- The web browser sends a request to the web server for web pages
- The web pages are sent from the web server to the browser
- The browser renders HTML to display web pages
- Any security certificates are exchanged
- SSL/HTTPS is used to secure the data which will encrypt any data that is sent

Worked Example

Describe how the web pages for the website are requested and displayed on a user's computer

[4]

- The browser sends the URL to the DNS [1]
- The DNS returns the IP address to the browser [1]
- The browser sends a request to the web server [1]
- The browser interprets and renders the HTML to display web pages [1]

Structure & Presentation

Websites can be separated into **structure** and **presentation**.

HTML is:

- A language used to create the structure/layout of a website
- Written in plain text
- Used in the content layer
- Made up of a set of markup codes
- Used to tell the browser how to display the page

For example

- Where text is placed
- Margins of page
- Line break
- Padding

CSS is:

- A language used to create the presentation / formatting of the page
- Written in plain text
- Used in the presentation layer
- Used by web pages to produce a consistent format between different web pages

For example

- Font size
- Font colour
- Background colour

YOUR NOTES

Why are they kept separately?

- The presentation of the page can be changed without needing to alter the structure so regular updates can be made without needing to check the structure
- The formatting document (written in CSS) can be used again for a different website
- If further content and web pages are added to the website, the necessary formatting can be easily applied so this can save time when developing a website
- CSS to standardise formatting so CSS only needs to be created once and be applied to each webpage
- One person can develop the structure and one can develop the presentation so this can save time when developing and updating a website

Exam Tip

- Make sure you know the definition for structure and presentation and know at least one example of each
- You also need to have a greater understanding of the reasons for the separation of structure and presentation

YOUR NOTES

Cookies

What are cookies?

Cookies are small **files** that are **stored on a user's device** by a website. They are used for various functions, including:

- **Saving Personal Details**
  - Cookies can save personal details which can be used to personalise the user experience. This can include
    - Name
    - Email address
    - Other preferences
- **Tracking User Preferences**
  - Cookies can track user preferences such as language settings, font size, and colour scheme, which can be used to customise the website experience
- **Holding Items in an Online Shopping Basket**
  - Cookies can hold items in an online shopping cart, so that users can continue shopping or return later without losing their selected items
- **Storing Login Details**
  - Cookies can store login details such as usernames and passwords, which can be used to remember users' login credentials and make it easier for them to log in
- **Storing Relevant Purchases**
- **Displaying Relevant Adverts**
- **Tracking Visitor Statistics**
  - Determining whether a visitor to a website is a new visitor or repeat visitor

There are two types of cookies: session cookies and persistent cookies.

- **Session Cookies**
  - These are temporary and are stored only during a user's browsing session
  - They are used to maintain a user's state or activity during a single session, such as when filling out a form or navigating through a website
- **Persistent Cookies**
  - These are stored on a user's device for a longer period, usually for a few weeks to several years
  - They are used to remember user preferences and settings, such as language preferences, login details, and shopping cart items

Cookies enhance the user experience and make it more convenient for users to interact with websites. However, cookies can also raise privacy concerns and should be used responsibly by website owners.

YOUR NOTES

5.2 Digital Currency

Digital Currency

Digital Currency

A digital currency is a type of currency that exists only in electronic form and is **not backed by** any physical commodity or **government**.

- **Only Exists Electronically**
  - Digital currencies are purely electronic, meaning they do not exist in physical form like traditional currencies such as cash or coins. They are stored in digital wallets or accounts and can be transferred electronically between individuals or businesses
- **Decentralised**
  - Many digital currencies operate on a decentralised network; meaning that they are not controlled by any central authority like a government or financial institution
  - Instead, transactions are verified and recorded on a public ledger known as a **blockchain**
- **Used for Transactions**
  - Digital currencies can be used for various transactions, including purchasing goods and services online or transferring money internationally
  - They can also be used for investments or as a store of value
- **Volatile**
  - Digital currencies can be highly volatile; meaning their value can fluctuate rapidly over short periods of time
  - This can make them risky investments and can also make it difficult to use them as a stable store of value
- Examples include **Bitcoin**, Ethereum, Litecoin, and Ripple

Blockchain

- Blockchain is a **digital ledger** that records every transaction made with a particular digital currency
  - Each transaction is time-stamped and added to the blockchain in a permanent and unalterable way
- Blockchain is a decentralised technology, meaning that it is not controlled by a single entity or authority
  - Instead, **every participant** in the network has **a copy of the ledger** and can **verify the transactions** independently
- The blockchain is made up of "blocks" of transactions that are linked together in a "chain" using cryptographic algorithms
  - This creates a **secure** and tamper-proof record of **every transaction** made with the digital currency
- Each transaction in the blockchain must be **verified by multiple participants** in the network
  - This verification process ensures that the transaction is legitimate and **prevents any fraudulent activity**

YOUR NOTES

5.3 Cyber Security

Cyber Security Threats

Cyber Security Threats

Cybersecurity threats pose a major challenge for individuals and organisations that rely on digital technology to store and transmit sensitive information.

Brute-Force Attack

- A brute-force attack is a **trial-and-error** method used to **crack passwords** or encryption keys by **trying every possible combination** until the correct one is found
- The aim of a brute-force attack is to **gain unauthorised access** to a system or network

Data Interception

- Data interception involves **eavesdropping on communication** channels to intercept and **steal sensitive information**, such as passwords, credit card numbers, or personal data
- The aim of data interception is to steal sensitive information for personal gain or to use it for further cyber attacks

Distributed Denial of Service (DDoS) Attack

- A DDoS attack is where **multiple computers** are used as bots
- They **flood a server** with **lots of requests** at the same time which the server can't respond to; causing it to **crash** or become unavailable to users
- The aim of a DDoS attack is to disrupt the normal functioning of a system or network by denying users access

Hacking

- Hacking involves **gaining unauthorised access** to a system or network to steal or manipulate data, disrupt services, or cause damage
- The aim of hacking can vary from personal gain to activism or cyber espionage

Malware

Malware is malicious software designed to harm or gain unauthorised access to a system or network. Types of malware include:

- **A virus** is a piece of code that attaches itself to a legitimate program or file and then replicates itself to spread to other programs or files on the computer. It can cause damage to the system, including deleting data or damaging hardware
- **A worm** is similar to a virus but is a standalone program that can spread and replicate itself over computer networks. It can take up storage space or bandwidth
- A **Trojan horse** is a program that disguises itself as a legitimate program or file, but when installed, it can delete data or damage hardware
- **Spyware** is software that records all key presses and transmits these to a third party
- **Adware** is a type of software that displays unwanted advertisements on the computer without the user's consent. Some of these may contain spyware and some may link to viruses when clicked

YOUR NOTES

- **Ransomware** is a type of malware that encrypts the user's files and demands a ransom payment to decrypt them. It can cause data loss, and financial damage and disrupt business operations

The aim of malware attacks can range from data theft to extortion or disruption of services

Phishing

- Phishing involves the **user is sent an email** which looks legitimate
- This contains a **link to a fake website** where the user is encouraged to enter their details
- The aim of phishing is to **steal sensitive information** for personal gain or to use it for further cyber attacks

Pharming

- Pharming involves **malware being downloaded** without the user's knowledge
- This **redirects the user to a fake website** where they're encouraged to enter their personal details
- The aim of pharming is to **steal sensitive information** for personal gain or to use it for further cyber attacks

Exam Tip

- A user needs to click on a link or an attachment to open the fake web page or trigger a download of malicious code, and not just open the email

Social Engineering

- Social engineering involves **manipulating individuals** to gain access to confidential information or to perform an action that benefits the attacker
- This can include techniques such as:
  - This involves posing as someone else to gain trust or access to sensitive information
  - Attackers might pretend to be a co-worker, IT support personnel, or a law enforcement officer to get people to divulge sensitive information or perform an action they wouldn't otherwise do
  - Baiting is a social engineering technique that involves enticing a victim with a desirable item or promise to extract sensitive information or gain access to a system
  - Attackers might leave a USB drive with a tempting label, like "salary information," in a public place and wait for someone to pick it up and plug it into a computer
  - Once the drive is connected to the computer, the attacker can access sensitive information or install malware
  - Pretexting involves creating a fake scenario to extract sensitive information
  - The attacker might pose as a bank representative and ask for personal information to "verify your account"
  - Impersonation
  - Baiting
  - Pretexting
- The aim of social engineering is to exploit human behaviour and vulnerabilities to **gain unauthorised access** to a system or network

YOUR NOTES

Accidental Damage

Data could also be **accidentally damaged** in many ways:

Example	Prevention
Loss of power	Use a UPS
Liquids being spilt	Don't have water near the device
Flooding	Keep device in a waterproof box when not is use
Fire	Use electrics safety and keep device in a fireproof box when not is use
Hardware failure	Correct care and maintenance of hardware
Software failure	Making sure it is always up to date
Human error: • Pressing delete by mistake • Not saving data • Not shutting down the computer correctly	Add verification method for data deletion Set access levels for data to limit who can delete the data
Incorrect use of storage device	Making sure device is ejected before removing

Exam Tip

- If you are given context in a question, you should apply your answer to the scenario
- Back-up of data is not a method to help prevent the data being damaged. It can replace the data if it is damaged, but it does not stop the data being damaged

YOUR NOTES

Keeping Data Safe

Access Levels

- Access levels are used to **restrict access** to sensitive information to **only authorised personnel**
- This helps to **prevent unauthorised access**, which is one of the main security threats to data
- Access levels can be set based on a user's role, responsibility, or clearance level
  - This allows the user to open, create, edit & delete files
  - This only allows the user to open files without editing or deleting
  - This hides the file from the user
  - **Full access**
  - **Read-only access**
  - **No access**

Anti-Malware

- Anti-malware solutions are used to **prevent and remove malware**, which is a common type of security threat to data
- Anti-malware software includes **anti-virus and anti-spyware** programs, which help to detect and remove malicious software from a computer system
- This software works by **scanning the computer**'s files and any files being downloaded and comparing them to a list of known malware
- If any malware is found, it is **quarantined** to prevent the spread
- The malware is then deleted

Authentication

- Authentication is used to ensure that **only authorised users** can access data
- There are several methods of authentication:
  - **Passwords** are used to protect sensitive data by preventing unauthorised access. A strong password should be complex, unique, and not easily guessed. Passwords should be changed regularly, and users should avoid reusing passwords across multiple accounts.
  - **Biometrics** uses biological data for authentication by identifying unique physical characteristics of a human such as fingerprints, facial recognition, or iris scans. Biometric authentication is more secure than using passwords as:
    - A biometric password cannot be guessed
    - It is very difficult to fake a biometric password
    - A biometric password cannot be recorded by spyware
    - A perpetrator cannot shoulder surf to see a biometric password
  - **Two-factor authentication** (2FA) requires users to provide two forms of authentication before accessing data, such as a password and a verification code sent to a mobile device. This provides an extra layer of security and reduces the risk of unauthorised access. 2FA is widely used to protect online accounts, such as email or banking.
- These methods help to prevent unauthorised access and protect sensitive data

YOUR NOTES

Automating Software Updates

- Automating software updates ensures that **software** systems are **up-to-date** with the latest security patches, which helps to prevent security threats
- This is especially important for **operating systems** and software that are frequently targeted by hackers
- It does this by **scanning the Internet** for known updates to software which are installed on the computer
- If any updates are found, these can either **install automatically** or **notify the user** to install them

Communications

- Checking the **spelling** and tone of communications is important to prevent phishing attacks

URL

- Checking the **URL attached to a link** is another way to prevent phishing attacks.
- Hackers often use fake URLs to trick users into visiting fraudulent websites
  - e.g. http://amaz.on.co.uk/ rather than http://amazon.co.uk/

Firewalls

- A firewall can be **software** or **hardware** based
- It **monitors incoming and outgoing traffic** between the computer and the network and keeps a log of the traffic
- The user **sets criteria** for the traffic (this is called the whitelist/blacklist) and the traffic is compared with this
- The firewall will **accept or reject** the traffic based on this and an alert can be sent to the user
- It can help prevent hacking and malicious software that could be a threat to the security of the data

Privacy Settings

- Privacy settings are used to **control the amount of personal information** that is shared online
- They are an important measure to prevent identity theft and other forms of online fraud
- Users should **regularly review** their privacy settings and adjust them as needed

Proxy-Servers

- Proxy-servers are used to **hide a user's IP address** and location, making it more **difficult for hackers to track them**
- They **act as a firewall** and can also be used to **filter web traffic** by setting criteria for traffic
- Malicious content is blocked and a warning message can be sent to the user
- Proxy-servers are a useful security measure for protecting against external security threats as it can direct traffic away from the server

Secure Socket Layer

- SSL is a **security protocol** which is used to **encrypt data** transmitted over the internet
- This helps to prevent eavesdropping and other forms of interception
- SSL is widely used to protect online transactions, such as those involving credit card information or other sensitive data

YOUR NOTES

- It works by sending a **digital certificate** to the user's browser
- This contains the **public key** which can be used for authentication
- Once the certificate is authenticated, the transaction will begin

Physical Methods

- Physical methods are used to physically protect hardware that stores sensitive data
- This can include:
  - **Locked rooms** needing a key or card access
  - **CCTV**
  - Bodyguards

Backup

- This is the process of **making a copy of files** in case something happens to the original ones
- Backing up data is important to protect against **data loss** due to hardware failure, cyber-attacks, or other disasters
- Backups should be **stored in a secure location**, and multiple copies should be made
- **Regular backups** ensure that data can be recovered in the event of a security breach or data loss

Ethics

YOUR NOTES ⬇

There are a number of ethical concerns when using the Internet:

- Addiction
  - Aspects of the internet e.g. social media can cause this
- Breaching copyright
  - Breaking the law by copying someone's work
- Cyber bullying
  - Using the internet to bully people
- Data protection
  - A person's data is not used according to the law
- Environmental effects
  - Increased use of the internet increases the use of electrical power
- Fake news
  - News stories that could be very misleading or harmful
- Inappropriate materials
  - Materials that could cause harm/offence to people e.g. children
- Intellectual property theft
  - Stealing other people's work
- Piracy
  - Using piracy websites to gain content for free that should have been paid for
- Plagiarism
  - The copying of other people's work without their permission
  - Claiming someone else's work as your own
- Privacy
  - A person's data could be leaked