CAIE Computer Science IGCSE

5 - The internet and its uses

Advanced Notes

5.1 The internet and the world wide web

Differences between the internet and world wide web

The internet is a global network of interconnected computers and devices. It provides the physical and technical infrastructure that allows data to be sent and received.

The World Wide Web (WWW) is a collection of websites and web pages that can be accessed via the internet using web browsers.

The WWW is one of the services that runs on the internet, alongside others such as email, file transfer and messaging.

Uniform Resource Locators (URLs)

A uniform resource locator (or URL) is a text-based address assigned to files on the internet. Different protocols can be used in URLs to access different types of files in different ways.

A URL can typically be split into three parts:

- **Protocol** - The set of rules that determines how data is transmitted between devices over a network.
- **Domain name** - The human-readable address of a website, used instead of an IP address.
- **Web page/file name** - The specific page or file on the website being requested.

```
https://www.physicsandmathstutor.com/computer-science-revision/
```

Take for example the URL above. Each part of the URL is broken down in the table below.

Protocol	Domain name	Web page/file name
https	www.physicsandmathstutor.com	/computer-science-revision/

HyperText Transfer Protocol (HTTP) and HyperText Transfer Protocol Secure (HTTPS)

HTTP and HTTPS are both protocols for transferring web pages and other resources over the internet. HTTPS is the same as HTTP but adds encryption using SSL/TLS for secure communication, protecting data from interception.

Web browsers

A web browser's primary purpose is to allow users to access and view content on the World Wide Web. Its functions include:

- **Storing bookmarks/favourites** - Giving the user quick access to saved web pages.
- **Recording user history** - Keeping a log of all visited URLs, with timestamps, for easy revisiting.
- **Multiple tabs** - Allows several web pages to be open at once.
- **Storing cookies** - Saves small files from websites called "cookies" which enable the user's preferences and login status to be stored for next time they visit a website, as well as tracking.
- **Navigation tools** - Buttons for back, forward, refresh, and stop.
- **Address bar** - Allows entry of URLs to access websites directly.

How web pages are located, retrieved and displayed

When a user enters a URL into a web browser, the browser first interprets the domain name. It contacts a Domain Name Server (DNS) to find the corresponding IP address of the web server that hosts the website. Using this IP address, the browser sends a request to the web server for the page. The web server processes the request and sends back the page resources, often in HTML format along with other files such as CSS and images. The browser then interprets the HTML and other resources to render and display the page on the user's device.

Cookies

Cookies are small text files stored on a user's device by a website. They are used to save information between visits. This can include:

- storing personal details
- remembering user preferences
- keeping items in an online shopping cart
- storing login information.

Session cookies are temporary and are deleted when the browser is closed, while persistent cookies remain on the device for a set period until they expire or are deleted manually.

5.2 Digital currency

A digital currency is a form of money that exists only in electronic form and has no physical counterpart such as coins or notes. It can be exchanged online to pay for goods or services.

Some digital currencies are decentralised systems, meaning that they aren't controlled by banks or the government, whereas other digital currencies are centralised.

Digital currencies are usually encrypted.

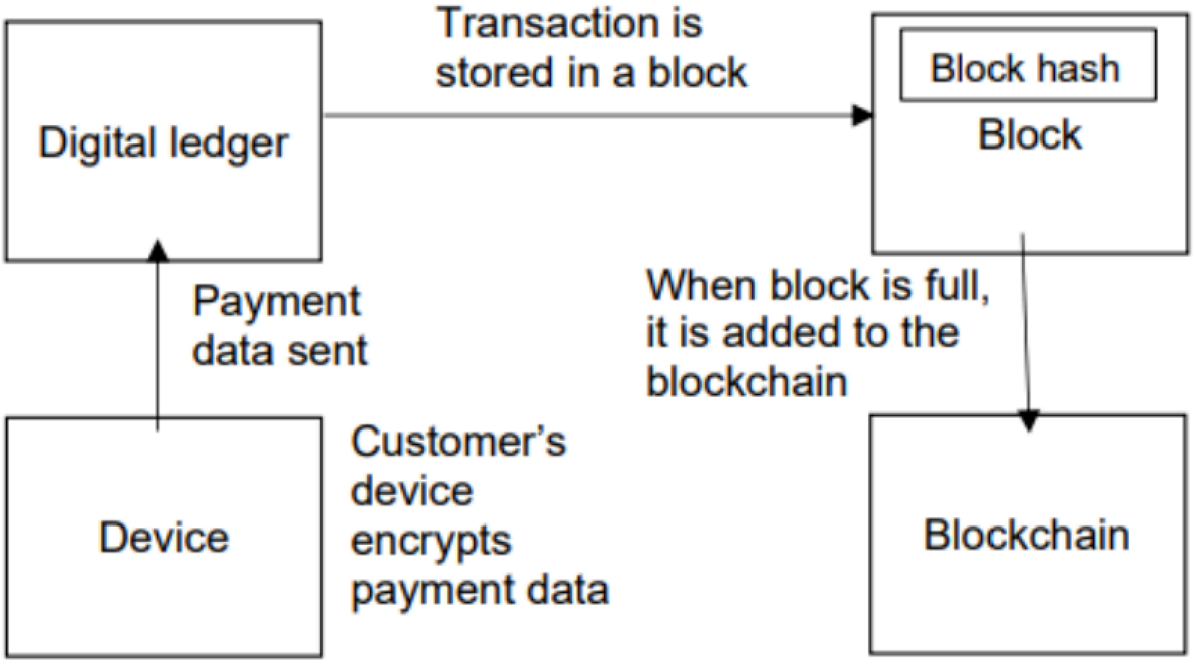
Blockchains

A blockchain, in its basic form, is a digital ledger, that is a time-stamped series of records that cannot be altered.

Here is an outline of the steps for a payment transaction to be made using digital currency and blockchain:

1. The customer's device encrypts payment information for security before sending it.
2. The encrypted payment data is sent from the customer's device to the blockchain network.
3. The transaction details are stored in the ledger, including information like a digital signature, time stamp, and other identifying data.
4. Transactions are grouped together into a "block". A block can contain multiple transactions.
5. Every block contains a "block hash" - a cryptographic code that uniquely identifies the block and links it to the previous one.
6. Once the block has reached its capacity or the transactions are confirmed, it is considered complete.
7. The completed block is added to the blockchain on every device in the network. This ensures that all copies of the ledger are identical and up to date.

This is a diagram showing how a payment transaction is made using digital currency and blockchain.


Digital ledger
Transaction is stored in a block
Block hash
Block
Payment data sent
When block is full, it is added to the blockchain
Device
Customer's device encrypts payment data
Blockchain

5.3 Cyber security

Cyber security threats

Brute-force attacks

A brute-force attack is a method where an attacker tries many different combinations of usernames and passwords until the correct one is found. This is usually automated using software that quickly tests thousands of possible combinations. The purpose of this attack is to break into user accounts or systems by guessing login credentials.

Data interception

Data interception occurs when cybercriminals capture data being transmitted over a network without permission. This is often done on unsecured networks using special software that listens for unencrypted data, such as login details or credit card numbers. The purpose of this attack is to steal sensitive information, which can then be used for identity theft, fraud, or unauthorised access to systems.

Distributed Denial of Service (DDoS) attacks

A distributed denial of service (DDoS) attack is used to overwhelm a website or online service with excessive traffic, making it slow or completely inaccessible to real users. This is usually done by sending a massive number of requests to the server, from multiple different devices and IP addresses, in a short space of time.

Hacking

Hacking is the act of gaining unauthorised access to computer systems or networks. Hackers may exploit vulnerabilities in software, guess passwords, or use stolen credentials to break into systems. The purpose of hacking can vary, from stealing sensitive data to causing disruption, altering files, or damaging systems.

Malicious Software (malware)

Malicious Software (malware) is an umbrella term used to refer to a variety of forms of hostile or intrusive software. Forms of malware include:

- **Virus:** A type of malware that attaches itself to a legitimate program or file and spreads when the infected file is opened. It can corrupt or delete data, slow down systems, or even make them unusable.
- **Worm:** A type of malware that can spread without any user action. Unlike viruses, worms do not need to attach themselves to files or programs. They often spread through networks by exploiting security flaws, and they can quickly infect large numbers of systems.
- **Trojan horse:** A type of malware that disguises itself as legitimate software. Once installed, it can create backdoors, allowing hackers to control the system, steal data, or install more malware without the user's knowledge.
- **Spyware:** A type of malware that secretly gathers information about a user's activity, such as keystrokes, login details, or browsing habits, and sends this information to the attacker.

- **Adware:** Software that automatically displays or downloads unwanted advertising material when a user is online. While some adware is merely annoying, other forms can track user behaviour without consent, slow down a computer, and open the door for more harmful malware. Adware is often bundled with free software and installed without the user's full understanding.

- **Ransomware:** Ransomware is a type of malware that encrypts the user's files, making them unusable, or locks them out of their system. The attacker then demands payment, usually in a form of digital currency, in exchange for restoring access. Even if the ransom is paid, there is no guarantee that the attacker will provide the decryption key or unlock the system.

Pharming

A technique that redirects users from a legitimate website to a fake one without their knowledge. This is usually done by exploiting vulnerabilities in a computer's DNS settings or by compromising a website's server. The fake website looks almost identical to the real one and is designed to steal personal information like passwords, bank details, or credit card numbers when users enter their data.

Phishing

A technique of fraudulently obtaining private information, often using email or SMS. Typically, the victim will receive a communication designed to look like it has come from a reputable source, such as their bank, which then contains a link to trick them into giving away their personal information, such as login details.

Social engineering

Social engineering is the art of manipulating people into giving up confidential information or performing actions that compromise security. It exploits human trust, curiosity, or fear rather than technical vulnerabilities. It is often said that people are the "weak point" of secure systems, as they have access to computer systems and information that outsiders don't - however, they are susceptible to being socially engineered. There are several tactics which can be used, but the key danger of social engineering is that it bypasses many technical security measures by targeting the human element directly.

Solutions to help keep data safe from security threats

There are a range of solutions which can be used to help keep data safe from security threats.

Access levels

Access levels are used to control what data and features different users can access within a system. For example, in a school, an administrator may have full access, while a student or teacher is given limited access. This method helps prevent misuse of data or accidental changes by ensuring users only have access to what they need. It limits attacks by reducing the risk of insider threats or damage if a low-level account is compromised.

Anti-malware software

Scans for malware, by comparing files to a database of known malware. When malware is found on a user's system then the anti-malware software should alert them and request they take an action, such as quarantining or deleting the malware. If malware is identified as being downloaded, then the download will be stopped. Forms of anti-malware software include anti-virus and anti-spyware software.

Authentication

Authentication is the process used to verify a user's identity before granting access to a system. Common methods include usernames and passwords, biometric data like fingerprints or facial recognition, and two-step verification where a user must provide two forms of identification. This helps prevent unauthorised access and protects sensitive data.

Automating software updates

Automated updates ensure that software is kept up-to-date with the latest security patches and bug fixes. This reduces vulnerabilities that attackers can exploit. Automatic updates help users by installing these updates in the background without requiring manual intervention.

Checking the spelling and tone of communications

Users should check the spelling and tone of emails or messages, as phishing attempts often contain spelling mistakes or unusual language (demanding). This helps identify fraudulent or suspicious communications before clicking links or sharing sensitive information.

Checking the URL attached to a link

Before clicking on a hyperlink, users should verify the URL to make sure it leads to a legitimate site. Fake websites often use URLs that look similar to real ones but contain small differences to trick users. Checking the URL helps prevent phishing attacks.

Firewalls

Scans incoming and outgoing traffic, comparing it to a criteria. This data will be blocked or allowed based on a set of security rules. For example, it might block traffic from suspicious IP addresses or stop certain types of data from entering a network.

Privacy settings

Privacy settings allow users to control what personal information is shared online and who can access it. For example, social media platforms offer settings to limit profile visibility or restrict data sharing with third parties. Proper use of privacy settings helps protect personal data from misuse.

Proxy-servers

Proxy servers act as intermediaries between a user's device and the internet. They can provide anonymity by hiding the user's IP address and can filter web traffic to block harmful content. Proxies are often used to improve security and control access to resources.

Secure socket layer (SSL) security protocol

SSL is a security protocol that encrypts data transmitted between a user's browser and a web server. This encryption helps prevent attackers from intercepting or tampering with sensitive information, such as passwords or credit card details. Websites using SSL can be identified by "https" in their URL and a padlock icon displayed in the browser.