ALIGNED WITH THE 2023-2025 SYLLABUS

CAIE IGCSE

COMPUTER SCIENCE (0478)

THEORY

1. The Internet and Its Uses

1.1. The Internet and the World Wide Web

Internet	World Wide Web (WWW)
Uses transmission protocols such as TCP and IP (Internet Protocols)	Collection of webpages and other information on websites
Allows the user to communicate with other users via chat, email, calling and more	Uses HTTP(S) protocols that are written using Hypertext Mark-up Language (HTML)
Worldwide Collection of Interconnected Networks and Devices	URLs (Uniform Resource Locator) are used for the location of the web pages
	Web browsers can access web pages.

Uniform Resource Locator (URLs)

- URLs are used to locate and access web pages. The typical format of URLs is -

  protocol://website address/path/file name

- The protocol would usually be **HTTP** or **HTTPS**
- The website address would contain -
  - domain host (www)
  - domain name (website name)
  - domain type (.com, .org, .net, .gov) or sometimes country codes (.uk, .in, .cy)
- The path would usually become the file directory roots. for example, https://www.znotes.com/computer-science
  - The /computer-science is the file name

HTTP and HTTPS

- HTTP stands for Hypertext Transfer Protocol, and HTTPS stands for Hypertext Transfer Protocol secure
- They are safety protocols maintained while transmitting data.

Web Browsers

- It is software used to connect to the internet
- It translates the HTML code
- ensures SSL & TLS security can be established
- Offers additional features like search history & ad blockers

Retrieval and Location of web pages

- The browser sends the URL to the domain name server (DNS)
- DNS stores the index and matches it with the IP
- IP is sent to the browser if it exists
- The browser sends a request to the IP of the webserver
- Browser interprets the HTML

Cookies

- Cookies are small files stored on the user's computer
- They are used to track data about the users and autofill forms or give suggestions accordingly
- Types of Cookies -

Session Cookie	Persistent Cookie
Temporary cookies are stored in the RAM till the browser is closed.	Remembers the user's login details so the user doesn't have to log in every time they visit a website
Doesn't collect any information on the user	Stored on the hard disk on the computer until their expiry date or the user deletes them
A good example is the virtual shopping basket on e-commerce websites.	

1.2. Digital Currency

- Form of payment to pay for goods and services
- A few examples are Debit/Credit Cards, Apps (Paypal, Apple Pay, Bank Transfers and many more)
- Cryptocurrency was later introduced due to the problem in centralised banking systems.
- Cryptocurrency uses cryptography to maintain track of transactions.
- Cryptocurrency is also more secure because it uses **Blockchain Network**

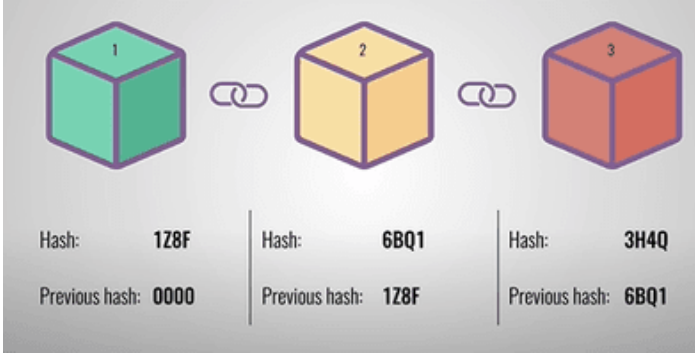
Blockchain Network

- Blockchain Network involves several interconnected computers where the transaction data is stored
- Hacking isn't possible here as transaction details would be sent to all the computers, and the data can't be changed without the consent of all the network members

How do blockchains work

Every time a transaction takes place, A block is created. The block would contain -

- Data - Name of the sender and the receiver, amount of money and more
- Hash Value - Unique value generated by an algorithm
- Previous Hash Value - Hash Value of the previous block in the chain



The first block is called the genesis block as it doesn't point to any previous block (Previous Hash Value - 0000)

1.3. Cyber Security

Brute Force Attack:

- Hackers try to guess your password by trying all the different combinations of letters, numbers and symbols.
- Effect:
  - Hacker gets access to user's personal data (credit cards, passwords and more)
- To remove risk:
  - Use stronger passwords with more characters and symbols

Data Interception:

- This involves stealing data by tapping into a wired or a wireless transmission line
  - Wardriving - The act of locating and using wireless internet connections illegally
  - Packet Sniffing - Uses Packet sniffers to examine packets sent over a line; all the data collected is sent back to the attacker
- Effect:
  - It can cause a computer to crash
  - Can delete or corrupt files/data
- To remove risk:
  - Install anti-virus software
  - Don't use software from unknown sources
  - Be careful when opening emails from unknown

Distributed Denial of Service Attacks (DDoS)

- An attempt at preventing users from accessing part of a network
- Usually temporary but may be damaging
- An attacker may be able to prevent the user from:
  - Accessing their emails
  - Accessing websites
  - Accessing online services

Hacking

- The act of gaining illegal access to a computer system
- Effect:
  - This leads to identity theft, gaining personal information
  - Data can be deleted, changed or corrupted
- To remove risk:
  - Firewalls
  - Strong passwords/ user IDs
  - Use of anti-hacking software
- Difference between hacking and cracking
  - Hacking breaks into computer systems to steal data
  - Cracking is when someone edits a program code, malicious

Malware

- Stands for Malicious Software. A few examples are -
  - Virus - A program that can replicate itself with the intention of deleting or corrupting files, causing a computer malfunction
  - Ransomware - Attackers encrypt the user's data until a certain amount of money is paid
  - Adware - Displays unwanted ads on the user's screen
  - Trojan Horse - Programs that are disguised as legitimate software
  - Spyware - Sends data about all the activities of the user to the attacker
  - Worms - Programs that can replicate themselves with the intention of corrupting the entire network instead of the computer alone

Phishing

- Attackers send legitimate-looking emails to bait the user into giving out their information.
- To remove risk:
  - Don't open links from unknown receivers
  - Use anti-phishing tools
  - Block pop-up ads
  - Have an up-to-date browser

Pharming

- The attacker installs a malicious code on the computer, which redirects the user to fake websites
- Effect:
  - The user gives out login details and other personal details
- To remove risk:
  - Using anti-virus software
  - Checking the spelling and the weblink carefully
  - Make sure that the green padlock is present in the URL bar

Social Engineering

- Attackers create a social situation which leads to victims giving out their details (For example - Spam calls informing them that their account has been hacked)

Keeping data safe from threats

- Access Levels - Having Different levels of access for different people (for example - Only doctors can have access to patient's data)
- Antivirus - Protects user's computer from malware attacks
- Authentication - User proving who they are. The most common methods are passwords, PINs, Mobiles (OTPs), biometrics and more)

Benefits and Drawbacks of Biometric Method

Biometric Methods	Benefits	Drawbacks
Fingerprint Scans	Most development methods are very easy to use and require very low storage space to store the biometric data.	Intrusive as used to identify criminals, Can't be used if the finger gets dirty or damaged (e.g. cuts)
Retina Scan	With very high accuracy, it Impossible to replicate a person's retina	It is very intrusive, Takes longer to verify, Expensive to install and set up
Face Recognition	Non-intrusive method, Relatively cheaper	Can't identify if there are any changes in the lighting or a person's age or if the person is wearing glasses
Voice Recognition	Non-Intrusive method, verification is done quickly and relatively cheaper	Voices can be recorded and used for verification, but low accuracy and illnesses such as colds or coughs can affect a person's voice, making identification impossible.

- Two-Step Verification - Requires two methods of authentication to prove who the user is
- Automatic Software Updates - Latest updates contain patches which improve device security
- Spelling and Tone - Fake emails tend to have wrong spelling and grammar (amazonn instead of amazon), and the tone would also seem urgent
- Firewalls - Hardware or Software which monitors the traffic between a network and the user's computer
- Proxy Servers - Acts as an intermediate between the user's computer and the web server. They are used for -
  - Filtering Internet traffic
  - Keeping the user's IP Address Confidential
  - Blocking access to certain websites
  - Attacks like DDoS and Hacking attack the proxy server, keeping the web server safe.
  - Acts as a firewall as well.
- Privacy Settings - Used to limit who can access and see a user's profile
- SSL (Secure Socket Layer) - Set of rules used while communicating with other users on the internet.

ZNOTES.ORG

CAIE IGCSE
COMPUTER SCIENCE (0478)

THEORY