Cambridge (CIE) IGCSE ICT

Your notes

Network Issues

Contents

Data Transfer

Why is data transfer a network issue?

- Sharing data is a fundamental reason to use a network, electronic data is constantly moving between sender and receiver
- The transfer of data on a network **poses potential security risks**, such as:
    - **Unauthorised access**
    - **Data manipulation**

Common causes of data transfer security risks

Cause	Risks
Hackers	Exploit network weaknesses and access/delete/steal confidential data
Insider threats	Intentionally/unintentionally compromising network security polices leading to data interception/theft
Social engineering	Manipulating network users into giving away confidential information and/or clicking links which installs malware leading to the compromise of data
Unencrypted transfers	No encryption protocols used when transferring sensitive data
Weak encryption	Weak or outdated encryption protocols used when transferring sensitive data
Insecure protocols	Using HTTP instead of HTTPS when dealing with sensitive information

Passwords

What are passwords?

- Passwords are a **digital lock** to prevent unauthorised access to an account
- They are often stored as an **encrypted/ciphered** text entry in a database, ensuring that even with unauthorised access to a database, a hacker would not be able to gain access to the individual passwords of users
- Passwords must be kept safe, this can be achieved by:

- Using **anti-spyware** software to ensure 'keyloggers' are not used
- Periodically **changing passwords** to ensure they have not been compromised
- Ensuring **passwords are 'strong'**
  - Mixture of upper/lower case
  - Contain at least one number
  - Contain at least one symbol
  - Minimum of eight characters

Authentication

What is authentication?

- Authentication is the process of **ensuring that a system is secure** by asking the user to **complete tasks to prove they are an authorised** user of the system
- Authentication is done because **bots can submit data in online forms**
- Authentication can be done in several ways, these include
  - **Zero login & biometrics**
  - **Magnetic stripe**
  - **Smart cards**
  - **Physical & electronic tokens**

Authentication method	Description	Advantages & disadvantages
Zero login & biometrics	▪ Allows a user to **login without** using a username & password ▪ **Uses biometric data** (fingerprint, face, gestures) to create a profile of a user so that they can log in without having to authenticate each time	▪ **Convenient** for devices when users **need to log in frequently** throughout the day e.g. smartphones ▪ If **compromised**, biometric data **cannot be changed** ▪ Biometric **recognition** can be **less than perfect** and lead to failed login attempts and user frustration

Magnetic stripe	▪ Magnetic stripe **contains unique data used to authenticate** a user e.g. ID, name & date of birth ▪ When **swiped through a magnetic card reader**, details are used to identify a user	▪ **Easy** and **cheap to setup** ▪ Cards can be used to access **multiple systems** ▪ Cards can be **remotely deactivated** ▪ Magnetic stripes **can wear** ▪ Card readers **must be maintained** ▪ **Less secure** than biometrics (easy copied)
Smart cards	▪ **Enhances** a magnetic stripe cards with the **addition of a microchip** to create a **contactless card** ▪ Microchip **stores additional information** such as a pin to add extra layer of security ▪ Data in **encrypted**	▪ **More secure** than magnetic stripe cards ▪ **Multi-purpose** ▪ Transactions can be much **faster** ▪ More **expensive** to manufacture ▪ **Lack of compatibility** can cause inconvenience
Physical tokens	▪ A physical device used to **authenticate a user remotely** ▪ The device **generates a random one time password** (OTP) that a user must type in ▪ Banks may ask customers to insert their bank card into the device and **use the OTP to access internet banking** ▪ OTPs **change** after a few minutes	▪ **Very secure** ▪ **Inconvenient** to the user as they need a physical device, card and login credentials to access one site
Electronic tokens	▪ **Software token** generated by an app ▪ **App generates OTPs** ▪ Users authenticate in app e.g. fingerprint and OTP is generated	▪ **Very secure** ▪ **More convenient**

Anti-Malware Software

What is anti-malware software?

- Anti-malware software is a term used to describe a combination of different software to prevent computers from being susceptible to **viruses** and other **malicious software**
- The different software anti-malware includes are
  - **Anti-virus**
  - **Anti-spam**
  - **Anti-spyware**

How does anti-malware work?

- Anti-malware **scans** through **email** attachments, **websites** and downloaded **files** to search for threats
- Anti-malware software has a list of known malware **signatures to block** immediately if they try to access your device in any way
- Anti-malware will also perform **checks for updates** to ensure the database of known issues is up to date
- Anti-malware will **quarantine** infected files
  - Quarantining files allows threats to be automatically deleted
  - Allows the user to determine if the file is a legitimate threat and not a **false positive**
- Anti-malware can make use of **heuristic checking**
  - The identification of potential threats within a file from behavioural patterns and characteristics rather than just relying on a database of known viruses

Worked Example

Give two examples of how Anti-Malware protects devices against malicious software

[4]

Answer

Regular updates by the Anti-Malware software will keep an up to date list of threats [1]

If any of the threats are detected on the device, the Anti-Malware software will quarantine the files [1]

> Anti-Malware software will scan external storage media when they are connected to the device [1]
>
> Preventing viruses from being transferred from storage media onto the device [1]

Electronic Conferencing

Video-Conferencing

What is video-conferencing?

Copyright © Save My Exams. All Rights Reserved

- Video-conferencing is a way of enabling **real-time audio** and **visual communication** between **geographically separated parties**
- Video-conferencing is ideal for **small groups of users** to create an **engaging meeting experience**
- Video-conferencing is typically used for:
  - **Staff meetings**
  - **Presentations**
- To successfully host a video-conference, the following **hardware is required**:
  - **Webcam**
  - **Large output display** (projector, screen, TV etc.)
  - **Microphone**
  - **Speakers**
- Specialist **software is also required**, such as:
  - **Drivers** to control the output of the webcam
  - A **codec** to encode (compress) and decode (decompress) data being transmitted

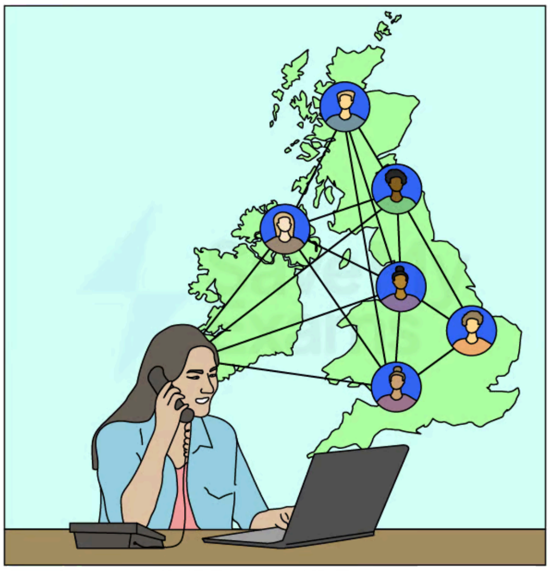
Advantages and disadvantages of video-conferencing

Advantages	Disadvantages
- Convenience - Cost saving - Better for the environment - Attendees do not have to travel to the event - Anyone within the company can attend regardless of location - Events can be held at short notice as travel is not required - Allows other members outside of the organisation to attend easily without having to visit on premises - Some video conferencing software allows record and playback to allow members to review the meeting	- The initial purchase of equipment can be costly - Possible issues amongst employees when working across different time zones - Those using the system may need to be trained to use it effectively which can: - Take time - Be costly - Video-conferencing systems require a strong and stable network connection - Poor picture/sound quality caused by the speed of connection/quality of the hardware - Delays (audio & visual) can disrupt the flow of the meeting

Your notes

Audio-Conferencing

What is audio-conferencing?



- Audio-conferencing is a way of enabling real-time **audio only** communication between **geographically separated parties**

- Audio-conferencing uses standard **phone lines**
- To host an audio-conference, the host must be given a **personal PIN** and a **participant PIN** by the phone company
- The host starts the conference using their personal PIN and participants **dial in** and join using their participant PIN
- Voice over Internet Protocol (**VoIP**) can be used on computers to hold audio-conferences

Advantages and disadvantages of audio-conferencing

Advantages	Disadvantages
▪ Cheaper than video-conferencing as less hardware is required ▪ More accessible as less training is needed for participants ▪ Gives participants the ability to focus only on voice and not get distracted by video	▪ participants can lose focus due to lack of visual interaction ▪ A lack of visual clues may lead to miscommunication ▪ Audio quality can be poor ▪ Does not suit collaboration

Web-Conferencing

What is web-conferencing?

- Web-conferencing is a way of enabling real-time audio and visual communication between geographically separated parties **on the internet**
- Web-conferencing is ideal for **large groups of users** to create an **engaging meeting experience**
- Web-conferencing is typically used for:

- **Webinars**
- **Lectures**
- **Presentations**

- To host a web-conference the emphasis is placed on a **high-speed**, **stable internet connection**

Advantages	Disadvantages
▪ Pre-shared/downloadable presentation notes/slides ▪ Participants can use instant messaging within conference to ask questions ▪ Collaboration via virtual 'whiteboards' ▪ Screen sharing/annotations	▪ Technical issues usually relating to participant internet connections ▪ Security concerns, risk of data interception ▪ Distractions ▪ Some users may feel overloaded with information which can lead to a lack of focus

Examiner Tips and Tricks

Web-conferencing and video-conferencing are very similar however, the key differences are:

- Video conferencing has a focus on face to face communication
- Web conferencing has a focus on interaction and collaboration such as document sharing, whiteboards etc

Worked Example

A motor car company has some designers based in London and some in Beijing.

The cost of travel between the two cities is very high, so when they wish to meet to discuss new products they use video-conferencing.

The designers all have PCs with a keyboard and a mouse in order to take part in video-conferencing.

a. Name three other devices used to input or output data which would be needed to take part in the video-conference.

[3]

b. Describe three potential problems of the designers using video-conferencing systems rather than meeting in either London or Beijing.

[3]

Your notes

Answers

a. Three of:

Webcam / video camera [1]
Speakers / headset / headphones [1]
Large monitor / television / data projector [1]
Microphone [1]

b. Three from:

Time lag / lip sync caused by the image not being synchronised with the sound [1]
Poor picture quality caused by the speed of connection / quality of the hardware [1]
More likely to have poorer sound quality caused by the quality of the hardware / connection [1]
Confidential material about the new cars may have to be signed / viewed in person [1]
The new car may have to be viewed in person [1]
Hardware breakdown stops the conference taking place [1]
Communication breakdown stops the conference taking place [1]
Different time zones will mean the conference has to take place at inconvenient times [1]