

AS • Cambridge (CIE) • Computer Science

 32 mins  8 questions

Exam Questions

Data Security

Security measures / Threats / Data protection

- 1 A program is written in a high-level language by a team of three programmers using an Integrated Development Environment (IDE).

The file containing the final program code will be sent by email for beta testing.

Identify **one** security method that can be used to protect the program code from unauthorised access during email transfer.

Explain how your chosen method protects the program code.

Answer



Mark Scheme and Guidance

1 mark for the security method. **2 marks** for explanation.

Security method:

Encryption

Explanation

- File contents are converted to cipher text
- If intercepted the data cannot be understood without the decryption key

(3 marks)

2 The bank also needs to keep its customers' data private and secure.

The bank's network has a firewall.

Explain how a firewall can help protect the customers' data.

Answer



Mark Scheme and Guidance

1 mark each to max 3:

- Compares all incoming and outgoing transmissions
- ... against set criteria/whitelist/blacklist
- Blocks all transmissions that do not meet rules
- Blocks data entering from specific ports
- Blocks unauthorised/unknown internal software transmitting data

(3 marks)

- 3 An assessment board scans exam papers and stores the digitised papers on a server. Exam markers download the digitised papers to mark. The exam markers then upload the mark for each paper.

The assessment board needs to make sure the data stored on the server is secure.

(i) Authentication methods can help to protect the server against hackers.

Identify **one other** security measure that helps to protect the server from hackers.

Describe how the security measure works.

(3)

(ii) Identify **one** security measure that helps to protect the data when it is being transmitted to its destination. Describe how the security measure works.

(3)

Answer



Mark Scheme and Guidance

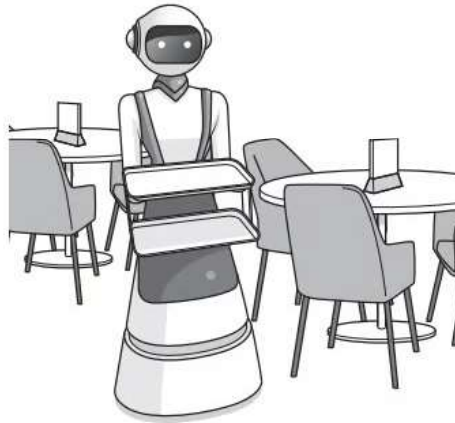
1 mark for security measure

1 mark each to max 2 for how the chosen measure works:

- Firewall
- Checks incoming connections
- ... against criteria
- Blocks data from entering specific ports
- Blocks data that does not meet whitelist that meets blacklist
- Proxy server
- Prevents devices accessing the web server directly
- Intercepts any requests
- Forwards the request using its own IP address
- Screens returning data before sending it to the user

(6 marks)

4 Robots are used to serve food and drink to customers at a restaurant.



The data from the robots is transmitted to a central computer using a wireless connection.

Explain how encryption can protect the security of data during transmission.

Answer



Mark Scheme and Guidance

1 mark each to **max 2**:

- Encodes/scrambles data
- ... so if it is intercepted it cannot be **understood**
- Algorithm/**key** is required to decode the data

(2 marks)

- 5 Authentication is one method a Database Management System (DBMS) can use to improve the security of a database.

Describe **other** methods that a DBMS can use to improve the security of a database.

Answer



Mark Scheme and Guidance

1 mark for each bullet point (**max 4**)

Max 2 if no descriptions

- Backup / recovery procedures
- ... automatically takes copies of the database and store off site on a regular basis / weekly, etc.
- ... so that the data can be recovered if lost
- Use of access rights
- ... some users are given different access permissions to different tables
- ... read/write, read only, full access, etc.
- Views
- ... different users are able to see different parts of the database
- ... only see what users need to see // by example
- Record and table locking
- ... prevents simultaneous access to data
- ... so updates are not lost // data is not overwritten
- Encryption
- ... the data is turned into ciphertext
- ... so it cannot be understood without a decryption key

(4 marks)

6 (a) State the meaning of **privacy of data**.

Answer



Mark Scheme and Guidance

1 mark for:

Either

- Ensuring data can only be accessed by / disclosed to authorised persons

Or

- Ensuring data cannot be accessed by / disclosed to unauthorised persons

(1 mark)

(b) State the meaning of **integrity of data**.

Answer



Mark Scheme and Guidance

1 mark for each bullet point (**max 1**)

- Ensuring the accuracy / completeness / consistency of data (during / after processing) .
- Ensuring the data is up to date

(1 mark)

(c) Describe the following threats to a computer system.

Phishing email

Spyware

Answer



Mark Scheme and Guidance

1 mark for each bullet point.

Phishing email (**max 2**)

- The email pretends to be from an official body
- ... persuading individuals to disclose private information // by example such as bank details
- ... or requesting authentication by redirecting to an unofficial/unauthorised website // inviting a user to click a link

Spyware (**max 2**)

- Malware downloaded **without the user's knowledge**
- ... which secretly records the user's actions / keystrokes on the computer
- ... and sends logs of the actions to a third party

(4 marks)

7 A company sells online Computer Science courses to students in different countries.

The courses are stored on a public cloud.

State how the following security measures can be used to protect computer systems.

Firewall

Encryption

Passwords

Answer



Mark Scheme and Guidance

1 mark each for firewall, encryption and passwords.

Firewall:

- Monitors incoming and outgoing traffic and rejects any traffic that does not meet the set rules

Encryption:

- Ensures that if data is intercepted / obtained it cannot be understood without the decryption key

Passwords:

- Ensures only users with the correct password can access the resources // prevents unauthorised access

(3 marks)

8 (a) State **one** difference and **one** similarity between pharming and phishing.

Answer



Mark Scheme and Guidance

1 mark for difference

1 mark for similarity

Difference:

- Pharming is malicious code that redirects to a **fake website**. Phishing uses an **email** to prompt user action.
- Pharming is **automatic**. Phishing requires **user action**.

Similarity:

- Both try to obtain financial or personal information
- Both are a false representation of an official organisation, e.g. a bank
- Both make use of fake websites

(2 marks)

(b) Explain how the data security risks of malware can be restricted.

Answer



Mark Scheme and Guidance

1 mark for each bullet point (max 3).

- Download programs from reputable websites / sources
- ...as these are less likely to contain malware
- Backup / archive computer systems
- ...so they can be restored in case of data loss from malware program installation
- **Install and run** anti-malware program
- ...so that regular scans can be made for known malware
- ...and if malware is found it can be quarantined / removed
- ...and computer's anti-malware definitions are regularly updated
- Using a firewall to block unused ports
- ...so that malware cannot enter the computer system
- Deny administrator privileges to everyday users
- ...so that malware cannot be downloaded by everyday users
- Avoid the use of / access to removable devices
- ...so that malware cannot be installed from these devices

(3 marks)