Past-paper walk-through

Data Security ▪ 6.1

eXercise

Questions in this set

- 9618/11 J25 Q7 ▪ 11 marks
- 9618/11 J24 Q5 ▪ 16 marks
- 9618/12 J24 Q3 ▪ 14 marks

Reading the mark scheme

- **B1** a mark that stands on its own – the point is either made or not.
- **M1** a *method* mark: the right approach, even if the number is wrong.
- **A1** an *answer* mark, and it usually needs its M mark first.
- **C1** a working mark on the way to the answer.
- // separates answers the examiner accepts equally.
- **ecf** = error carried forward: a later part is marked on your own earlier answer.
- **owtte** = "or words to that effect" – the wording need not match.

Question 7

9618/11 J25 ▪ Q7 ▪ 11 marks

A banker stores personal data on their work computer.

(a) The banker needs to transfer confidential data across the internet.

Identify and describe **one** method of restricting the risks posed by an unauthorised person intercepting the data whilst it is being transferred across the internet.

Description **[3]**

(b) The banker receives confidential data across the internet. The data includes a digital signature.

Explain how a digital signature can make sure the data has **not** been changed during transmission. **[5]**

(c) The data that is transferred can also be verified using a checksum.

Explain how data can be verified using a checksum. **[3]**

Solution 7

(a) Mark scheme

- 1 mark for a correct method:
- 1 mark each to max 2 for a corresponding description
- Method: Encryption
- Description:
- ▪ Data is encoded/scrambled using a key to create cipher text
- ▪ if intercepted it cannot be understood
- ▪ without being decrypted using a key

Solution 7

(b) Mark scheme

- 1 mark each to max 5
- ▪ The sender hashes the document / message
- ▪ to produce a digest
- ▪ The sender encrypts the digest to create the digital signature
- ▪ The message and the signature are sent to the banker / receiver
- ▪ The receiver decrypts the signature to reproduce the digest
- ▪ The receiver uses the same hashing algorithm on the document received to produce a second digest

Solution 7

- The receiver compares this digest with the one from the digital signature
- If both of the receiver's digests are the same the document has not changed

Solution 7

(c)

Mark scheme

- 1 mark each to max 3
- ▪ The data is put through an algorithm to create a checksum value
- ▪ The data and checksum are sent to the receiver
- ▪ The receiver performs the same algorithm on the data
- ▪ if both checksums match the data is verified

Question 5

9618/11 J24 ▪ Q5 ▪ 16 marks

5 A bank allows customers to access their accounts using an application that they can download onto a device such as a smartphone.

(a) The system that allows customers to access their accounts using the application is a client-server model.

Describe the roles of the different devices in this model.

Question 5

(b) The bank wants to protect the integrity of its data while transferring the data to other banks. Parity check is one example of data verification.

Complete the description of parity check when Computer A is transmitting data to Computer B.

Question 5

and the group has an even number of 1s, a parity bit of 1 is appended, otherwise a parity bit of 0 is appended.

In a parity ..... check the bytes are grouped together, for example in a grid. The number of 1s in each column (bit position) is counted. A bit is assigned to each column to make the column match the parity. These parity bits are transmitted with

Question 5

[5]

(c) The bank also needs to keep its customers' data private and secure.

(i) The bank's network has a firewall.

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

Question 5

(ii) Customers need to use biometric authentication to access their accounts.
One biometric authentication method is facial recognition.

Facial recognition uses Artificial Intelligence (AI).

Describe how AI is used in facial recognition.

Solution 5

(a) Mark scheme

- 1 mark each:
- ▪
- Identification of server in the bank scenario
- ▪
- Description e.g. Receives requests, processes the requests
- ▪
- Identification of client in bank scenario
- ▪

Solution 5

- Description e.g. Sends request to the server, waits and outputs the
- response
- 4

Solution 5

(b) Mark scheme

- 1 mark for each correctly completed term:
- ▪
- odd or even
- ▪
- 7-bits
- ▪
- odd
- ▪

Solution 5

- block
- ▪
- byte
- Computer A and Computer B agree on whether to use odd or even parity.
- Computer A divides the data into groups of 7-bits. The number of 1s in each
- group is counted. If the agreed parity is odd and the group has an even
- number of 1s a parity bit of 1 is appended, otherwise a parity bit of 0 is
- appended.
- In a parity block check the bytes are grouped together, for example in a grid.
- The number of 1s in each column (bit position) is counted. A bit is assigned to

Solution 5

- each column to make the column match the parity. These parity bits are
- transmitted with the data as a parity byte.
- 5

Solution 5

(c)(i) Worked steps

Three marks, three steps of the same mechanism:

- It **inspects every transmission** entering or leaving the system.
- It compares each against **set criteria** — a whitelist of what is allowed, or a blacklist of what is not.
- It **blocks** anything that fails those criteria, and can log the attempt.

Saying a firewall "stops hackers" scores nothing; the marks are for inspect, compare, block. **Mark scheme**

- 1 mark each to max 3:

Solution 5

- ▪
- 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

Solution 5

- 3

Solution 5

(c)(ii) Worked steps

- The system **captures an image** of the face with a camera.
- It uses **image recognition** to locate the face and measure its features — the distances between eyes, nose and mouth, for example.
- Those measurements are compared against the **stored template** for that user.
- If they match within a set tolerance the user is authenticated; otherwise access is refused.

The tolerance matters and is worth stating: a face is never captured identically twice, so biometric matching is a similarity threshold rather than an exact comparison — unlike a password. **Mark scheme**

Solution 5

- 1 mark each to max 4:
- e.g.
- ▪
- Captures an image of the face
- ▪
- Uses image recognition
- ▪
- Trained to identify the features of a face in an image
- ▪
- ... using a large number of images

Solution 5

- ▪
- Analyse images for facial features
- ▪
- Uses the probability of a match
- 4
- 9618/11
- May/June 2024

Question 3

9618/12 J24 ▪ Q3 ▪ 14 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.

(a) 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.

Question 3

[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.

Question 3

[3]

(b) The exam markers use software that operates as a thin-client to mark the exam papers.

Complete the table by identifying **two** characteristics of a thin-client.

Describe how each characteristic will be used in this software.

	Thin-client characteristic	Description of use in this software
1	.....	.....
	.....	.....
	.....	.....

Question 3

Question 3

	.....	.....
2	.....	.....
	.....	.....
	.....	.....
	.....	.....

[4]

(c) Data transmitted on the internet passes through multiple different systems.

(i) Describe the role of routers in the transmission of data through the internet.

Question 3

(ii) Describe the role of the PSTN (Public Switched Telephone Network) in the transmission of data through the internet.

Solution 3

(a)(i) Mark scheme

- 1 mark for security measure
- 1 mark each to max 2 for how the chosen measure works:
- ▪
- Firewall
- ▪
- Checks incoming connections
- ▪
- ... against criteria

Solution 3

- ▪
- 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

Solution 3

- ▪
- Forwards the request using its own IP address
- ▪
- Screens returning data before sending it to the user
- 3

Solution 3

(a)(ii) Worked steps

One mark names the measure and **two** describe it, so choose something you can say three things about.

- **Encryption**
- It **encodes or scrambles** the data ...
- ... so that if it is **intercepted it cannot be understood** ...
- ... and a **key or algorithm** is needed to decode it.

Solution 3

The shape the marks want is *what it does*, *what that prevents*, *what is needed to reverse it*. Naming "a firewall" or "a password" and stopping there earns one mark of three.
Note what encryption does **not** do: it does not stop the data being intercepted, only from being read. Saying so is a good way to show the mechanism is understood. **Mark scheme**

- 1 mark for security measure
- 1 mark each to max 2 for description of the chosen measure:
- ▪
- Encryption

Solution 3

- ▪
- Encodes/scrambles data
- ▪
- ... so if it is intercepted it cannot be understood
- ▪
- Algorithm/key is required to decode the data
- 3
- 9618/12
- May/June 2024

Solution 3

(b) Worked steps

One mark for a **characteristic** of a thin client, one for **applying it to this system** — so every point must be written twice, generally and then specifically.

- **Data is not stored on the client.** The exam papers live on the server, not permanently on the examiner's own computer.
- **The client depends on access to the server.** An examiner cannot mark if their device cannot reach it, or the server goes down.
- **Processing happens on the server.** The examiner's machine needs little power, so ordinary hardware is enough.

Solution 3

The security consequence is worth making explicit, since it is why a thin client was chosen here: confidential papers are never held on a machine outside the board's control. **Mark scheme**

- 1 mark for characteristic
- 1 mark for description of application to examination software:
- Thin-client characteristic
- Description of use in this software
- Data is not stored on the
- client computer

Solution 3

- Exam papers are stored on the server and
- not on the examiner's computer // exam
- papers are not permanently stored on the
- examiners' computers
- Client computer is reliant on
- access to server
- Examiners cannot mark if their device
- cannot access the server / the server 'goes
- down'
- Client computer heavily

Solution 3

- reliant on network/internet
- connection
- The marking software will not operate
- without network/internet access
- Client computer requires few
- local resources/memory
- Examiners can use devices with low
- resources and the marking software will still
- function
- Client computer performs

Solution 3

- minimal functions/processes
- The marking software transmits requests,
- the server responds and sends the
- response to the user
- 4

Solution 3

(c)(i) Worked steps

Describe what a router does to **one packet**. Two marks from:

- **Receives packets** from the internet.
- **Reads the destination IP address** of each one.
- **Forwards it towards its destination** ...
- ... using the **routing table**.
- **Maintains and updates** that table, choosing the most efficient route.

The distinction being tested is with a switch, which forwards within one network using MAC addresses. A router works between networks, using **IP addresses** — say "IP address" and the answer cannot be misread. **Mark scheme**

Solution 3

- 1 mark each to max 2:
- ▪
- Receives packets from internet
- ▪
- Analyses the destination IP address of each packet
- ▪
- Forwards the packet towards its destination
- ▪
- ... using the routing table
- ▪

Solution 3

- Maintains/updates the routing table
- ▪
- Finds the most efficient route to the destination
- 2

Solution 3

(c)(ii) Worked steps

Two marks about the **public switched telephone network** specifically:

- The PSTN is made of **many different kinds of line**, so digital data may have to be **converted to another form** — an analogue signal — to travel over parts of it.
- Data travels in **both directions at once** — duplex transmission.
- The communication passes through **several switching centres and ISPs** on the way.

The first point is the one the question is really about, and it is why a modem exists: it **mod**ulates digital data onto an analogue carrier and **dem**odulates it at the far end.

Mark scheme

Solution 3

- 1 mark each to max 2:
- ▪
- The PSTN consists of many different types of communication lines
- ▪
- ... therefore the digital data may need to be converted into a different
- form/analogue signal
- ▪
- Data is transmitted in both directions at the same time // duplex data
- transmission
- ▪

Solution 3

- Using a PSTN the communication passes through different switching
- centres/ISPs
- 2
- 9618/12
- May/June 2024