MODULE G SECURITY · G5

Hacking and data interception: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.1 (processes involved in, and aim of, data interception and hacking), 5.3.2 (solutions that keep data safe) and 2.3.1 (purpose of encryption when transmitting data)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. The term "packet sniffer" is credited but never required. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1 0478 5.3.1	One mark for each correct row: Captured while being transmitted: Data interception Gains access without the owner's permission: Hacking Aim can be to steal personal data such as passwords: Both Can delete or change stored files: Hacking	**4**	A row with more than one box ticked scores 0.
2(a) 0478 5.3.1	Any four from: Data is sent across the network in packets Wireless signals can be picked up by any device within range (of the hotel network) The attacker uses a packet sniffer // software/hardware that captures/copies packets The packets are intercepted/captured/copied while they are being transmitted // in transit The captured packets are sent to / stored on the attacker's device The attacker examines/analyses the contents of the packets ... to find useful data, e.g. login details / payment details The data still reaches the booking website // the interception can go unnoticed If the data is not encrypted, the attacker can understand it	**4**	max 4. Do not credit "hacks the network" / "steals the data" alone. Do not credit descriptions of other threats (e.g. flooding the network, redirecting to a fake website).
2(b) 0478 5.3.1	Any two from: To steal login details / username and password // to use them to access the guest's account To steal payment / bank / card details // to commit fraud / take money To steal personal data // to commit identity theft To sell the data (to other criminals) To blackmail the guest To monitor / spy on the guest's communications	**2**	max 2. Do not credit "to steal data" alone. Do not award two aims that are the same point (e.g. bank details and card details).

QUESTION	ANSWER	MARKS	GUIDANCE
2(c) 0478 2.3.1	Any two from: Encryption does not stop/prevent the data being intercepted // the data can still be captured (But) the intercepted data cannot be understood // is meaningless without the (decryption) key The data is sent as ciphertext // it has been scrambled, so the person who intercepts it only gets ciphertext	**2**	max 2. Do not credit "the data cannot be read" alone (it can be captured and read as ciphertext; it cannot be understood). Do not credit answers saying encryption stops the data being intercepted or stolen.
3(a) 0478 5.3.1	Any two from: Gaining access to a computer system / network / data ... ... that is unauthorised // without the owner's permission (Often) by finding / exploiting weaknesses in security // by getting round security measures // using stolen or guessed login details	**2**	max 2. The second point builds on the first. "Gaining unauthorised access to a computer system" scores both of the first two points. "Breaking into a computer" alone scores 1.
3(b) 0478 5.3.1	Any three from: Steal data, e.g. building designs / client records Delete data Change / corrupt data Install malware (e.g. ransomware / spyware) on the server Sell / leak the data // blackmail the firm Use the server to carry out further attacks // to access other computers on the network Spy on / monitor the firm's activity Damage the firm's reputation // disrupt its work	**3**	max 3. Accept "steal designs to give to a rival firm". "Delete or change data" written as one point scores 1. Do not credit "to hack the server" or "to cause damage" alone.

QUESTION	ANSWER	MARKS	GUIDANCE
3(c) 0478 5.3.2	One mark for each solution and one mark for its matching explanation (max 2 solutions): Firewall (1) ... monitors traffic between the server / network and the internet and blocks unauthorised traffic / connections that break its rules (1) Access levels (1) ... each user can only access the files they need, so a hacker using one account cannot reach / change all the data (1) Authentication using a (strong) username and password (1) ... only users who enter the correct details can access the server // a strong password is hard to guess (1) Biometrics (1) ... access needs a unique physical feature, e.g. a fingerprint, which a hacker cannot easily copy / guess (1) Two-step verification (1) ... a one-time code is sent to the member of staff's phone / email, so a stolen password alone is not enough to access the server (1) Automating software updates (1) ... security weaknesses that hackers could exploit are fixed as soon as patches are released (1) Proxy server (1) ... sits between the network and the internet and filters / blocks unwanted traffic // hides the IP addresses of devices on the network (1) Anti-malware (1) ... detects and removes malware, e.g. spyware / a Trojan horse, that could give a hacker access (1)	**4**	max 4. The explanation mark must match the solution given. Two different solutions are needed: username and password, biometrics and two-step verification may each count as a separate solution. Do not credit "makes it more secure" alone.

Total: 21 marks