MODULE G SECURITY · G3

Brute-force attacks: mark scheme

20 marks · Cambridge 0478 syllabus 5.3.1 (process and aim of a brute-force attack) and 5.3.2 (solutions: authentication by username and password, biometrics, two-step verification)

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. **...** at the start of a point means it builds on the point before. Credit any other valid answer that shows the same understanding.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	Row 2 ticked only (using a program to try one password after another)	**1**	More than one tick = 0. (Row 1 is DDoS, row 3 pharming, row 4 phishing.)
2(a) 0478 5.3.1	Any three from: Trial and error (is used) to guess / find the password // password after password is tried (with the guest's username) Every possible combination of characters is tried (in turn) ... until the correct password is found / one works // then the hacker logs in to the account It can be carried out automatically by software / a program Common / weak passwords / dictionary words may be tried first A huge number of attempts are made very quickly / every second	**3**	max 3. The "... until" point builds on the trial-and-error or the combination point. Accept "tries to guess the password" for the trial-and-error point. Do not accept "hacks into the account" alone. Do not credit tricking the guest (that is phishing / social engineering).
2(b) 0478 5.3.1	One mark for each correct row: Obtain payment card details: Yes Make the website unavailable by flooding it: No Change or cancel bookings: Yes	**3**	A row with both boxes ticked scores 0. Row 2 is the aim of a DDoS attack.
3(a) 0478 5.3.1, 5.3.2	Any two from: A longer password has (many) more possible combinations // each extra character multiplies the number of combinations // e.g. 456,976 for 4 letters but about 209 billion for 8 letters ... so it takes (much) longer to try them all // e.g. less than 0.1 seconds for 4 letters but about 6 hours for 8 letters ... so a longer password is less likely to be found // the attack is less likely to succeed (in a reasonable time)	**2**	max 2. Credit figures quoted from the table. Do not accept "more secure" / "harder to guess" alone.

QUESTION	ANSWER	MARKS	GUIDANCE
3(b) 0478 5.3.1, 5.3.2	Any two from: More characters can be used in each position // 62 possible characters instead of 26 So there are (many) more possible combinations for the same length // e.g. about 218 million million (218,340,105,584,896) instead of about 209 billion So it takes much longer to try them all // e.g. about 253 days instead of about 6 hours So the guests' accounts / card details are less likely to be accessed	**2**	max 2. Credit figures quoted from the table. Do not accept "more secure" / "harder to guess" alone.
4(a) 0478 5.3.2	Any two from: A brute-force attack needs to make a very large number of attempts Only a few attempts are allowed before the account is locked // the hacker cannot keep repeatedly trying passwords ... so it would take far too long to try enough combinations // the password is very unlikely to be found The guest / hotel can be alerted that someone is trying to get in	**2**	max 2. Do not accept "stops hackers" / "makes it more secure" alone.
4(b) 0478 5.3.2	Any two from: After the password is entered, an extra code / data is sent to the guest's registered device / phone / email (account) ... the code must also be entered (to complete the log-in) The hacker would also need access to the guest's device / email to get the code So finding the password by brute force is not enough to get into the account	**2**	max 2. Do not accept "the guest has to log in twice" alone. Accept "two-factor authentication".
4(c) 0478 5.3.2	Any two from: A fingerprint is unique to the guest / to each person It cannot be found by trying combinations of characters // there is no password to try It is very difficult to copy / fake // the hacker would need the guest's actual finger / biometric data So a brute-force attack (on the app log-in) cannot succeed / is not possible	**2**	max 2. Do not accept "biometrics are more secure" alone.
5(a) 0478 5.3.1	One mark for each correct word, in order: trial and error combination software	**3**	Words must be in the correct gaps. Accept "combinations" for gap 2.

Total: 20 marks