Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers

UNIVERSITY OF BIRMINGHAM

School of Computer Science

LM Designing and Managing Secure Systems

Main Summer Examinations 2023

Time allowed: 2 hours

[Answer all questions]

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 80, which will be rescaled to a mark out of 100.

Question 1

You work for a start-up company and are tasked with designing the hardware anchored security for your next generation smartphone.

(a) From the following three approaches which one would you choose and why? Briefly explain how your choice works and give two advantages *over the other two* hardware anchored security choices: ARM TrustZone, TPM, Apple-like Secure Enclave Processor. **[9 marks]**

(b) Your company wants to protect the local data on the device and is considering implementing a new scheme that combines full disk encryption (FDE) with file-based encryption.

(i) Does combining FDE and FBE provide any security benefits? Justify your answer. **[6 marks]**

(ii) Suppose management wants the scheme implemented regardless of your answer above. Give the minimum number of keys needed to secure a test storage device with a file system consisting of 3 directories/folders and 1 file in each directory, without reusing any of the keys. Explain 1) the purpose of each key and 2) its relationship with other keys, i.e., *no-relationship with any other key* or *encrypted by key*. **[5 marks]**

Question 2

You are a security expert tasked with implementing a password-based authentication solution for your company.

(a) What is the role of the salt in password protection? **[5 marks]**

(b) Give a function that can be used to generate secure passwords from user input. Describe the format and purpose of the function's inputs and outputs. **[5 marks]**

(c) Now assume that an attacker has access to passwords database, which uses passwords generated with the function above. 1) The attacker wants to brute-force the password for ANY of the users. Briefly describe what the attacker needs to do in order to obtain one plaintext password. Still assuming the function at (b), would the attack change if the adversary would target one SPECIFIC user. **[6 marks]**

(d) Now assume that the attacker has remote access only to the password input interface. Briefly explain what can be done to reduce the efficiency of brute-force attacks in this case. **[4 marks]**

Question 3

(a) Security management systems set out to identify **risks** and then **control** those risks. Give two examples of security risks, and for each risk two examples of controls (ie, a total of four controls). **[6 marks]**.

(b) A management system needs to show it is operating correctly. For the controls you listed in the previous part, explain how you might **audit** them to show they are operating correctly. **[8 marks]**.

(c) A common document used within a security management system is a **residual risk statement**. Explain the purpose of this document. Who is its audience, and who should approve it? **[6 marks]**

Question 4

One of the key documents in a security management system is an **asset register**.

(a) What is the purpose of an asset register? **[4 marks]**

(b) How might you go about compiling an asset register for a software development company with approximately thirty employees? **[8 marks]**

(c) What can be the consequences of an incomplete asset register? How would you propose to maintain an asset register so that it remains correct? **[8 marks]**

End of Paper

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.