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

Designing and Managing Secure Systems

Main Summer Examinations 2024

Time allowed: 2 hours

[Answer all questions]

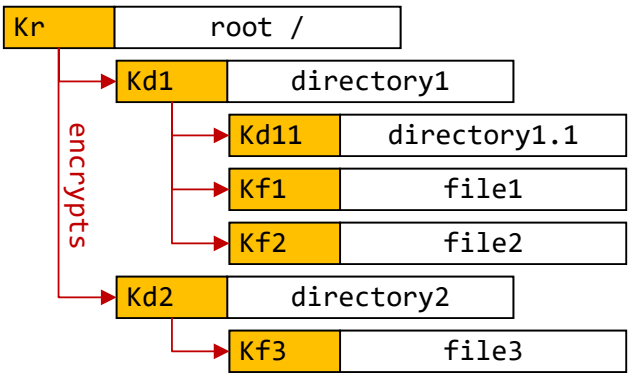
Turn Over

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1

A file-based encryption (FBE) system is set up as follows: files have keys Kf associated to them which are used to encrypt their contents and metadata. Directories have keys Kd associated with them, which are used to encrypt keys Kf belonging to the files inside the directory, and keys Kd belonging to sub-directories, as shown in the figure to the right. Finally, all the 1st level keys Kd are encrypted with the root key Kr.



(a) What is file-based encryption, and how does it differ from other encryption methods commonly used to secure mobile devices?

[7 marks]

(b) Is this scheme able to protect the filesystem's metadata? Provide a description of what you understand by metadata protection in this context, and then, for reach of the the elements in the figure explain if they are protected or not.

[7 marks]

(c) Describe what needs to happen to $Kf3$ when `file3` is moved from `directory2` to `directory1.1`, in order for `file3` to remain accessible, assuming knowledge of only Kr.

[6 marks]

Question 2

(a) You work for a start-up company and are tasked with implementing a "root of trust" on a hardware device.

(i) What do you understand by "root of trust"? What cryptographic functionality do you require from the device in order to implement the "root of trust"? Explain its/their purpose(s). **[6 marks]**

(ii) Now consider a specific mobile phone D produced by a manufacturer M. The manufacturer M has a public-private key pair $(M_{prv}; M_{pub})$. Briefly explain how the "root of trust" can be used to verify a firmware update file assuming it was generated by M, the phone manufacturer, using the keys referred. You can use additional cryptographic data, that you define, (e.g. keys) in your explanation. **[4 marks]**

(b) A strong temptation for IT security departments is to "lock down" user devices, making them only usable for the IT security department's conception of the user's job. This policy has advantages and disadvantages. Consider the case of laptops being used by university lecturers. Write a short note (total perhaps one page) listing two advantages and two disadvantages of such an approach, and give a recommendation as to the best approach. **[10 marks]**

Question 3

MyBank needs to demonstrate to the financial regulator that its IT systems and processes are effective. It has been strongly recommended that ISO 27001 would be a good starting point for this. Compliance with ISO27001 will show that the security management system is effective and complies with the bank's requirements. Write a briefing for your CEO outlining the process to follow to obtain and maintain ISO27001 certification, and the potential benefits and problems that ISO 27001 compliance might bring. Your CEO has a history of bringing in consultants to do large exercises such as compliance certification, so your briefing should include a discussion of the benefits and problems that consultants might cause.

Your response should be approximately two to three pages long. **[20 marks]**

End of Paper

This page intentionally left blank.

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.