A36930

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

Fourth Year Undergraduate/Postgraduate

06-34244

LM Designing and Managing Secure Systems

Main Summer Examinations 2025

Time allowed: 2 hours

[Answer all questions]

Note

Answer ALL questions.

Question 1

ORAM is a technology used in the context of cloud security. It uses client-side encryption to secure the contents of the data stored in the cloud, and also protects the access patterns to data.

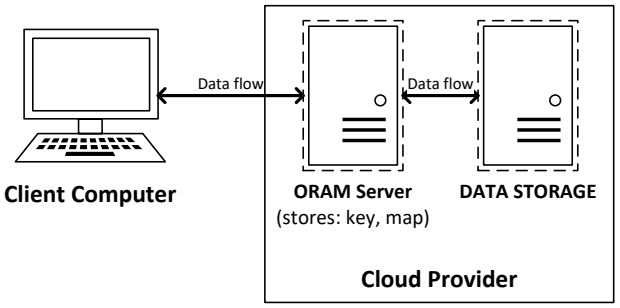


Fig.1

(a) What do you understand by access patterns to data? Why should these be protected?

[8 marks]

(b) In a standard ORAM deployment who is considered to be the adversary?

[7 marks]

(c) In general how does the ORAM protocol protect data? Please *do not* reproduce the ORAM algorithm. Instead focus on describing important and relevant data structures, the contents of data flows with respect to encryption and authentication, and the entities/parties participating in the protocol.

[10 marks]

(d) Analyse Fig.1 above, and state:

(i) Which entity stores the important data that is being protected by ORAM?

(ii) Is the setup from the figure above able to protect access patterns from the standard ORAM adversary? If *yes* explain why, if *no* propose a fix and justify it.

[10 marks]

Question 2

An attacker has somehow managed to gain access to your laptop and boot the OS but it cannot bypass the OS password and login. The attacker then decides to restart the laptop and boot from an external disk. Your laptop, however, is using a TPM-based *secure boot*.

(a) Briefly explain how the TPM-based *secure boot* works. Refer to what is being verified, what is being protected, and how. **[8 marks]**

(b) What can the attacker expect relative to its access to hard drive data? **[7 marks]**

(c) You are travelling to a foreign country where it is assumed that the contents of your laptop are of interest to the security services. Outline two attacks that might be attempted, and what counter-measures your company might consider. **[15 marks]**

Question 3

You are a consultant for SecurityHelp Ltd; SecurityHelp helps businesses improve their information security. You have been called in by a SoftwareCo, who are expanding rapidly. SoftwareCo has gone from the four founders to forty employees in the last year. SoftwareCo make a popular mobile phone application used by businesses to share information about customers. Almost all of SoftwareCo's employees are remote, and use their own computers. SoftwareCo's application runs entirely on Cloud services.

SoftwareCo has just won a large contract with BigMultiNational Ltd, to supply their product to all of BigMultiNational's sales staff. BigMultiNational want documentary evidence that their data will secure.

(a) What documents should SoftwareCo produce to demonstrate to BigMultiNational and their clients that their security policies are appropriate and effective? You should describe their contents and the process by which they are produced. **[15 marks]**

(b) We can call a company that has its own buildings with all computers under control of its IT function a *traditional* company. Remote workers with their own computers, and services running in the cloud, present novel risks. State **three** risks that SoftwareCo will experience that would not be present in a *traditional* company. What controls would you recommend be put in place to reduce or mitigate these risks? How could SoftwareCo show these controls are effective? **[20 marks]**

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.