University of St Andrews

MARTINMAS 2022-23 EXAMINATION DIET
SCHOOL OF COMPUTER SCIENCE

MODULE CODE: CS4203

MODULE TITLE: Computer Security

EXAM DURATION: 3 hours

EXAM INSTRUCTIONS

a. Answer all three questions
b. Each question carries 20 marks

This assessment consists of exam-style questions and you should answer as you would in an exam. You cannot copy or paraphrase text or material from other sources and present this as your own work. Your exam answers should be entirely your own work without unacknowledged input from others. If you are in any doubt, you should clearly acknowledge the origin of any material, text passages or ideas presented (e.g. through references). You must not co-operate with any other person when completing the exam, which must be entirely your own work. You must not share any information about the exam with another person (e.g. another student) or act on any such information you may receive. Any attempt to do so will be dealt with under the University's Policy for Good Academic Practice and may result in severe sanctions. You must submit your completed assessment on MMS within 3 hours of you downloading the exam. Assuming you have revised the module contents beforehand, answering the questions should take no more than three hours.

1. **Cryptography and its applications**

(a) Certificates are the public side of public-key key-pairs that are themselves signed by a trusted certificate authority. Why is public-key cryptography appropriate for this application? Explain how a web browser performs certificate checks when connecting to a secure web site, and explain in detail how public-key cryptography ensures the correct behaviour of each step. Comment on **one** possible attack. [6 marks]

(b) Suppose that you are asked to comment on adding security features to a new consumer product: a battery-powered home monitor that detects people moving around in a room, to be given to elderly or vulnerable people to check their well-being. The monitor sends a stream of data back to its home server over wifi, and can act as a speaker and microphone to allow caregivers to communicate with the resident.

(i) Identify **two** security risks that this system poses to its users. Describe their implications. [4 marks]

(ii) Describe in detail how the monitor might use public-key cryptography to secure communications to and from its server. Briefly explain any key management issues. [6 marks]

(iii) Are there any limitations to the application of public-key cryptography in this scenario? What would be the implications of using symmetric-key encryption instead? [4 marks]

[Total marks 20]

2. **Distributed security and intrusion detection**

(a) A "back door" is an attack that creates a new, unexpected, opportunity to log-in to a system.

(i) Describe **two** ways by which a back door could be introduced onto a system. [4 marks]

(ii) For each approach you identified in 2(a)(i), describe a mechanism that you could use to detect and prevent the attack – in other words, to prevent the back door being introduced onto the system. [4 marks]

(b) Now assume that the countermeasures you introduced in 2(a)(ii) have failed, and the attacker has successfully introduced their back door.

(i) Describe how you might use host-based intrusion detection to detect the presence of the back door. Be clear about what sorts of indications you might observe, and how you would observe them. [4 marks]

(ii) In the same manner as 2(b)(i), describe how you might use network-based intrusion detection to detect the presence of the back door. [4 marks]

(iii) Once you have installed an intrusion detection system (IDS), it becomes a target for attack itself. How would you protect its core data and functionality? Be sure to consider the problem end-to-end:

for example, how can the IDS securely alert system administrators when it finds a problem? [4 marks]

[Total marks 20]

3. **Security policies, access control, and virtual infrastructure**

(a) Suppose you are called into an organisation that consists of three types of users: ordinary employees, summer interns, and system managers. Different security policies need to be applied uniformly to each type of user. (You may make any assumptions you like about the exact permissions being given to each type of user: please state any assumptions clearly.)

(i) Discuss how access control lists (ACLs) can be used to control access to information. [4 marks]

(ii) What are the potential issues in using ACLs in practice? In what ways would role-based access control (RBAC) be a better or worse choice for managing permissions in this situation? [4 marks]

(b) The organisation now decides to move some of its operations into the cloud. Specifically it places its data into zero-knowledge cloud storage, but keeps its access and processing servers locally.

(i) What are the security implications of this hybrid architecture? Discuss what needs to be done in terms of user authentication, key management, and secure communications. [6 marks]

(ii) The organisation believes that this hybrid architecture is more resilient to attacks since it can hold some of its data locally, outside the cloud. Does this actually improve resilience? How might an attack on the local data centre corrupt the cloud data? How would you protect against such an attack? [6 marks]

[Total marks 20]

***** END OF PAPER *****