The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2022-2023

Computer Security

Time allowed: ONE HOUR (60 MINUTES)

Candidates may complete the front cover of their answer book and sign their desk card but must NOT write anything else until the start of the examination period is announced

Answer ALL questions

This exam is worth a total of 60 marks

This is a **closed-book exam**. No calculators are permitted in this examination.

Dictionaries are not allowed with one exception. Those whose first language is not English may use a standard translation dictionary to translate between that language and English provided that neither language is the subject of this examination. Subject specific translation dictionaries are not permitted.

No electronic devices capable of storing and retrieving text, including electronic dictionaries, may be used.

DO NOT turn your examination paper over until instructed to do so

Collect examination question papers at the end of the examination.

1. Please answer all of the following questions about Computer Security.

(a) **[5 Marks]** Data availability is a core component of the CIA model of computer security. Using an example of a service running on the Internet, explain the concept of availability. Give an example of a situation in which new security measures added to this service may inadvertently affect availability, and explain why.

(b) **[2 marks]** When talking about malware, what is the difference between a virus and a worm?

(c) **[2 marks]** What is a zero-day vulnerability or zero-day attack?

(d) **[5 Marks]** Traditional password-based authentication has a number of recognised weaknesses due to the way that users often tend to select and manage them. Identify three examples of these weaknesses, and indicate the extent to which can be overcome by using biometric-based authentication instead? What are the potential downsides for biometrics that passwords do not possess?

(e) **[6 marks]** Consider a program that reads in a set of integers and calculates their average. One Metamorphic Relation for this program would be that any permutation of the series should not impact the output value (`average(a,b,c,d) == average(d,c,b,a)`). Briefly outline two more (different) Metamorphic Relations for this program.

[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

2. Please answer all of the following questions about Network and Internet Security.

(a) **[4 Marks]** Explain the issues raised if an attacker was able to obtain persistent session cookies for other users on a website. How might websites be designed to avoid attacks based on this?

(b) **[4 Marks]** A computer network uses a signature-based intrusion detection system such as Snort to monitor network packets for possible attacks. How effective will this system be for previously unknown threats? What effects, if any, would the pervasive use of encryption have on the ability of a system like this to function well?

(c) **[5 Marks]** What is the main principle behind a denial of service amplification attack? Give an example of such an attack and explain in detail how it achieves the amplification.

(d) **[7 Marks]** A recent security event at your organisation has seen that every member of staff has received the same email containing a malware attachment. You have been tasked with the immediate and longer-term responses to this threat. What would you do immediately to limit the potential damage from this attack, and what longer-term steps you might take to mitigate the risk from attacks similar to this?

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

3. You work at a company where one of your responsibilities is to ensure password and authentication policies.

(a) **[1 mark]** State Kerckhoffs's Principle.

(b) **[2 marks]** If you are the root user on a GNU/Linux system, can you open the system file containing users' hashed passwords and decrypt them to retrieve the original passwords? Briefly explain your answer.

(c) **[3 marks]** Briefly outline the principles of offline password cracking.

(d) **[2 marks]** Give an example of 2-factor authentication.

(e) **[4 marks]** Explain TOCTTOU, including what the letters stand for, and give an example of a potential security problem related to it.

(f) **[3 marks]** Your boss has asked you to ensure perfect security for the entire network. Based on what you have learned in this module, briefly discuss the concept of absolute/complete computer security.

(g) **[5 marks]** Your company currently uses a signature-based intrusion detection system. Your boss has said that he will probably use a host-based anomaly detection system. Describe two **strengths** and two **weaknesses** of host-based anomaly detection system. In your description, explain what threats the company may be exposed to. Make any recommendations for the system that you think appropriate.

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam