The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2023-2024

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.

Question 1: General Computer Security **[overall 20 marks]**

a. 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.

[5 Marks]

b. 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?

[5 Marks]

c. Although we would generally advocate that organisations perform risk assessment to properly understand the threats and vulnerabilities facing their assets, various safeguards can already be recommended based on the notion of *baseline security*.

(i) Explain what is meant by baseline security and discuss why it is relevant.

[2 marks]

(ii) A small retailer wants to adopt a baseline approach that enables them to demonstrate to clients that they take cyber security seriously. Which of the baseline approaches would you recommend for this purpose and why?

[2 Marks]

d. 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.

[6 Marks]

Question 2: Operating Systems and Software Security [overall 20 marks]

a. In the context of Computer Security, what is a Trojan? How are Trojans usually delivered to victims, and what advice would you give users on protecting themselves against these threats?

[4 Marks]

b. A security researcher has found a serious vulnerability in a piece of software. They would like to detail the vulnerability in a talk at a high-profile conference. Explain why a prudent course of action would be for the researcher to first alert the software developers of the issue, before disclosing the vulnerability publicly?

[4 Marks]

c. Describe the process that occurs when an operating system makes a discretionary access control decision for a principal performing an operation on an object. You may use either Windows or Linux as an example.

[5 Marks]

d. What security vulnerability exists in the following code? Outline how a hacker would attempt to exploit it, and what steps the operating system may take to stop them.

```
int main (int argc, char** argv)
{
     char buffer[256];
     strcpy(buffer, argv[1]);

     return 0;
}
```

[7 Marks]

Question 3: Network and Internet Security **[overall 20 marks]**

a. 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?

[4 Marks]

b. 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?

[4 Marks]

c. 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.

[5 Marks]

d. 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 potential damage from this attack, and what longer-term steps you might take to mitigate the risk from attacks similar to this?

[7 Marks]

End of Exam