The University of Nottingham

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2017-2018

COMPUTER SECURITY (G53SEC)

Time allowed ONE Hour

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 THREE Questions

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 examination paper over until instructed to do so

ADDITIONAL MATERIAL: None

INFORMATION FOR INVIGILATORS: Please ensure that the Exam Paper is also collected at the end of the examination.

Question 1: General Computer Security [overall 20 marks]

a. Give an example of something you *are*, something you *have*, and something you *know*, with respect to authentication on a computer system.

[3 Marks]

b. Define the three components of the CIA model of computer security. For each of these, name one example of an attack that might seek to break the component.

[6 Marks]

c. Explain the strengths and/or weaknesses of the password “football!” if, once hashed, it is subjected to a brute force and dictionary attack.

[5 Marks]

d. Explain DNS Spoofing (DNS Cache Poisoning) attacks. Assuming such an attack was successful, give two examples of further attacks that could then be mounted.

[6 Marks]

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

a. What is a “Time of Check to Time of Use” issue? Give an example of a situation where this might cause a problem.

[4 Marks]

b. Explain briefly how controlled invocation, through the use of system calls, is used within an operating system to restrict access to privileged modes of operation. Why is this hard for an attacker to circumvent?

[5 Marks]

c. Many databases support queries written in SQL. Explain the concept of an SQL injection attack. What are the possible steps a developer could take to prevent such an attack?

[6 Marks]

d. Explain the difference between signature-based, and heuristic-based malware detection. Suppose an anti-virus package offers only signature-based detection, in what ways might this pose a security risk?

[5 Marks]

Question 3: Cryptography **[overall 20 marks]**

a. What is a digital signature? If you were sent a document with a digital signature, how would you verify it?

[4 Marks]

b. Describe how a cipher operates when in Electronic Code Book (ECB) mode. What is the major weakness of ECB, and why? Give an example of a different mode of operation and explain how it overcomes this weakness.

[5 Marks]

c. Alice and Bob have established a shared secret key. When sending messages, in what way will Message Authentication Codes help them? Explain in detail how they do this.

[5 Marks]

d. During their key exchange, an attacker eavesdropped on Alice and Bob. From their conversation the attacker obtained values for g, p, g^a mod p and g^b mod p. Explain how the attacker could use these values to calculate their shared private key, and discuss if this is practical.

[6 Marks]