The University of Nottingham

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2018-2019

COMPUTER SECURITY

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. What is a Permissive (Black Listing) firewall policy? Provide one example of why this might not always be the best solution.

[3 Marks]

b. Data integrity is a core component of the CIA model of computer security. For a message transmitted over the internet, explain what it means for it to have integrity. Give an example of a mechanism that enforces this property and describe how it works.

[5 Marks]

c. You have been tasked with securing a database of usernames and passwords. The passwords are currently stored using the SHA-1 algorithm, without salting. Propose some improvements to this system and explain your reasoning.

[5 Marks]

d. You have been asked by a superior to help protect your corporate network against new ransomware threats. Discuss what practical steps would you take to make the network as secure as possible, and prevent damage to assets. Explain your answer.

[7 Marks]

Question 2: Network and Internet Security [overall 20 marks]

a. What is the main principle behind a denial of service amplification attack? Give an example of such an attack and outline how it achieves the amplification.

[5 Marks]

b. Suppose that a new exploit has been developed that targets a common protocol such as SSH. Would either a packet filter or application gateway have any chance of being effective against this? Explain your reasoning.

[4 Marks]

c. IP security can operate in either transport or tunnel mode. Briefly explain the difference between these two modes, including how they affect the structure of the packets.

[5 Marks]

d. During a TLS handshake a server will send a digital signature and a public key certificate to the client. What security benefit does this part of the protocol provide, and how? What is an appropriate response from the client if the certificate fails validation?

[6 Marks]

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

a. What is the birthday paradox? Explain how birthday attacks must be considered when designing a hash function.

[4 Marks]

b. Explain, with reference to Kerckhoffs' Principle, why it is common practice to publish the mechanisms behind cryptographic algorithms rather than keep them a secret.

[4 Marks]

c. Explain the principle of the One Time Pad. In theory the One Time Pad offers perfect secrecy. Why isn't it used in practice?

[5 Marks]

d. A web server uses an RSA key pair to verify its identity, by signing messages with the private key, d. Clients may verify these messages using the public key (n, e). If an attacker was able to determine the private key, they would be able to impersonate the server. Explain how the private key can be calculated from the public key in RSA, and discuss whether this is practical.

[7 Marks]