The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2015-2016

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

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. You are a senior software engineer, and an expert in computer security, at SecureSolutions. Your company is a recognised leader in providing all kinds of solutions to all kinds of computer security problems. A newly recruited member of your team, Eric, has asked you to mentor him, and to help him understand the many things that SecureSolutions does.

(a) As part of your attempt to explain cryptography to Eric, you used the example of a Caesar Cipher. You and Eric then used a Caesar Cipher to exchange some messages, one of which, using a key 'D', gave the ciphertext "L DP DQ HQJLQHHU".

i) Briefly define the differences between cryptography, cryptanalysis, and cryptology. [3 marks]

ii) What is the plaintext obtained by decrypting the ciphertext "L DP DQ HQJLQHHU"? [3 marks]

iii) Discuss briefly some of the **strengths** and **weaknesses** of the Caesar Cipher (both in general, and specifically for this plaintext). Discuss **four** points. [4 marks]

(b) After studying more about cryptology, Eric has come to you to suggest using a One Time Pad instead of the Caesar Cipher. Assuming Eric wants to encrypt the message "**I love working for SecureSolutions**", give him a key that he can use to do so. Explain your choice. [4 marks]

(c) Eric used the Google Chrome web browser to connect to the company's website, https://www.securesolutions.com, and clicked on the green padlock icon shown in the address bar. He was satisfied to see the following:

```
Your connection to
www.securesolutions.com is encrypted
using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and
authenticated using AES_128_GCM and
uses ECDHE_RSA as the key exchange
mechanism.
```

Briefly define the following (in the context that Eric sees them):

i) TLS 1.2 [2 marks]

ii) AES_128_GCM [2 marks]

iii) ECDHE_RSA [2 marks]

[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

2. While working at SecureSolutions, you have seen many security threats and other issues. "Heartbleed" was a significant security bug that was announced in April 2014. It is probably the most widely known cybersecurity breach in recent years. Given the technical simplicity of its fix, it has been suggested that Metamorphic Testing, amongst other approaches, would probably have caught the bug before release.

(a) Explain what the Heartbleed bug is, and how it could be exploited. [8 marks]

(b) What is Metamorphic Testing:

i) Briefly outline the original motivation for the development of Metamorphic Testing. [4 marks]

ii) Using an example, illustrate how Metamorphic Testing can (typically) be used. [4 marks]

(c) Explain how a tester using Metamorphic Testing might have been expected to test the relevant code, and how this would probably have led to identifying what became the Heartbleed bug.

[4 marks]

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

3. Because of your experience and expertise, you are often consulted by the senior management at SecureSolutions, especially when they are working with important clients. A senior partner has recently taken on a new client. The client is running a medium sized corporate network, and has asked advice on including a signature-based intrusion detection system as a security measure. They have indicated that they will probably not use any host-based anomaly detection system. The SecureSolutions partner has expressed concern about this, and has come to you for advice.

(a) Describe three aspects of any organization which are vulnerable to network attacks. Describe a vulnerability for each aspect, and give a specific example.

[6 marks]

(b) The client has mentioned that they really want their network to be perfectly, and completely, secure. Is perfect and complete security a feasible goal? Based on what you have learned in this module, give three points to support your opinion on "perfect and complete" security.

[4 marks]

(c) Give the partner your opinion on the security of the client's network. Describe the **strengths** and **weaknesses** of the client's intended system. In your description, explain what threats the client may be exposed to. Make any recommendations for the client's system that you think appropriate.

[10 marks]

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam