The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2016-2017

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 recognised expert in computer security, working at the company PerfectSecurity. In addition to the regular work of securing computer systems, PerfectSecurity encourages all employees to ask questions, and often seeks help from senior colleagues (such as yourself) to answer them. A recent series of questions that you have been asked to reply to are as follows:

(a) What is a hash function?

[2 marks]

(b) What is the meaning of collision avoidance, in terms of hash functions?

[3 marks]

(c) What is the birthday paradox?

[3 marks]

(d) Why is the birthday paradox relevant to hash function choices?

[3 marks]

(e) Define Kerckhoffs' Principle (in the context of Cryptology).

[2 marks]

(f) What is the value of 13^{11} (MOD 7)?

[3 marks]

(g) What is the difference between signature-based and heuristics-based malware detection?

[4 marks]

[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

<<Turn over>>

2. At PerfectSecurity, you also take responsibility for mentoring a number of junior colleagues.

(a) A young colleague has been talking about how important firewalls are, but seems confused over the labels of black and white for different firewall policies, and for other things.

i) Briefly explain the difference between permissive (Black listing) and restrictive (White listing) firewall policies.

[2 marks]

ii) Regarding software testing, briefly explain the difference between black box and white box testing.

[2 marks]

iii) Briefly explain the difference between a "black hat" hacker and a "white hat" hacker?

[2 marks]

(b) One of the first things you like to discuss with newly hired colleagues is what you call "the basics" — a list of basic rules that you want all colleagues to follow to help ensure the security of the PerfectSecurity systems, and those of your clients. Number one on this list is to always install software updates.

i) What kind of attack does this help defend against? Explain clearly the attack and the defence.

[4 marks]

ii) What is a "zero-day" attack?

[2 marks]

iii) How well can following your basic rule help defend against zero-day attacks?

[2 marks]

(c) You overhear a group of colleagues talking about how they design their email passwords. One of them explains how he creates new passwords, at least 15 characters in length, by combining words to form a sentence, and then changing some letters into symbols, such as o to 0 (zero), 1 to !, A to 4, and so on. A recent password he used was: br0wnh0us3l!v3dth3r3, which he says was "brownhouselivedthere" with o changed to 0, e changed to 3, and i changed to !.

i) What is a brute-force attack?

[2 marks]

ii) Is this a good choice of password? Briefly explain your answer

[4 marks]

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

3. While working at PerfectSecurity, you are approached by one of the newer security engineers, John, who was previously a software tester. He asks you about how secure web sites work, and, opening up a page on his browser shows you a message saying that the site is secure because it uses TLS 1.2.

(a) What do the letters TLS stand for?

[1 mark]

John later asks you about the “Heartbleed” incident, and how you think the security bug might have been avoided through reasonable application of Software Quality Assurance (SQA) and testing.

(b) Explain what the Heartbleed bug is, and how it could be exploited.

[8 marks]

(c) Explain how 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.

[6 marks]

John is curious about how distributed denial of services (DDOS) attacks can happen.

(d) Explain what a botnet is, and how an attacker could use one to launch a DDOS attack.

[5 marks]

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam

<<End>>