The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2019-2020

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

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 fascinated by computer security, knowing more about it than most people. This results in a lot of people asking you basic questions about the topic. Please (briefly) answer all of the following:

(a) Define a "Security Engineer." [1 mark]

(b) Define a "Cybercrime Ecosystem." [1 mark]

(c) What do the letters stand for in the CIA model of computer security. [1 mark]

(d) State Kerckhoffs's Principle. [1 mark]

(e) Briefly outline the principles of offline password cracking. [4 marks]

(f) Define a "Reference Monitor." [1 mark]

(g) Define a "Code Obfuscator." [1 mark]

(h) In the context of software testing, what is the oracle problem? [2 marks]

(i) Consider a program that reads in a series of integers and calculates their average value. One Metamorphic Relation for this program would be that any permutation of the series should not impact the output value (**`avg(a,b,c,d)== avg(d,c,b,a)`**). Very briefly outline one more possible Metamorphic Relation for this program. [3 marks]

(j) What is the difference between a virus, a worm, and a trojan? [4 marks]

(k) If a firewall policy allows access by default, and restricts specific listed services / ports: would this policy most accurately be called a Blacklisting or Whitelisting policy? [1 mark]

[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

2. One of your favourite aspect of Computer Security is cryptography. Please answer all of the following related questions:

(a) Very briefly define the words cryptography, cryptanalysis, and cryptology. [2 marks]

(b) Explain clearly (and briefly) two uses for asymmetric cryptography. [2 marks]

(c) What is the value of 21^{11} (MOD 44)? [2 marks]

(d) If the Euler totient value (Φ) of 9 is 6 ({1, 2, 4, 5, 7, 8}), given two prime numbers 101 and 1901, what is the Euler totient value of their product 192001? [3 marks]

(e) Alice and Bob want to use Diffie-Hellman to establish a shared secret key (Z). Explain the steps involved to do this. [5 marks]

(f) Explain why the Diffie-Hellman key exchange is considered to be secure. [3 marks]

(g) If Jerry wants to listen in on the communication between Alice and Bob, very briefly explain an attack against the Diffie-Hellman key exchange that could work. [3 marks]

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

3. You are working for a medium-sized company, where part of your responsibility is to ensure the security of the organisation.

(a) Your CEO has mentioned that they really want their network to be perfectly, and completely, secure. Is perfect and complete security a feasible goal? Give three points to support your opinion on “perfect and complete” security.

[4 marks]

(b) Describe three aspects of the organisation that are vulnerable to network attacks. Describe a vulnerability for each aspect, and give a specific example.

[6 marks]

(c) Currently, your organisation uses a signature-based intrusion detection system, but you would like to add a host-based anomaly detection system. Give five points why.

[5 marks]

(d) Ransomware threats are growing in popularity and impact. What is Ransomware? What can you do to ensure that the network is as secure as possible?

[5 Marks]

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam

<<End>>