The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2017-2018

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. As an expert in computer security, you are often approached and asked technical questions. A recent series of questions that you have been asked to reply to are as follows:

(a) Define the three components of the CIA model of computer security.

[3 marks]

(b) What is the difference between a virus, a worm, and a trojan?

[3 marks]

(c) Explain briefly what TOCTTOU means?

[2 marks]

(d) What is the value of 11^{11} (MOD 12)?

[3 marks]

(e) Explain the difference between signature-based and heuristic-based malware detection. If an anti-virus package only uses signature-based detection, give two examples of when this could result in a security risk.

[4 Marks]

(f) In terms of access control structures, explain briefly the difference between "Access Control Lists" and "Capabilities".

[2 marks]

(g) Briefly explain how ARP Cache Poisoning works.

[3 marks]

[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

<<Turn over>>

2. Cryptography is one of your favourite parts of computer security, and you enjoy discussing many aspects of this.

(a) What is the difference between cryptology, cryptanalysis, and cryptography?

[2 marks]

(b) A young colleague has asked if it is OK to use Data Encryption Standard (DES) instead of the Advanced Encryption Standard (AES)

i) Is it OK to use DES instead of AES?

[1 mark]

ii) Briefly explain the difference between DES and AES.

[3 marks]

iii) Briefly explain how to run a block cipher using the Electronic Code Book (ECB) mode of operation.

[2 marks]

iv) What is a weakness of the ECB mode of operation for a block cipher?

[1 mark]

v) Name a different mode of operation to ECB.

[1 mark]

(c) When surfing the web, a colleague looked at the security information of a particular website and read that:

```
The connection to this site is
encrypted and authenticated
… ECDHE_RSA with P-256 …
```

i) What does “ECDHE_RSA” stand for?

[2 marks]

ii) If the Euler totient value (Φ) of 6 is 3 (1, 4, 5), what is the Euler totient value of the prime number 7919?

[1 mark]

iii) Explain clearly two uses for RSA.

[2 marks]

(d) With user authentication, passwords are usually stored in hashed form in a database.

i) Briefly outline the principles of offline password cracking based on dictionaries.

[3 marks]

ii) How does password salting impact on this attack?

[2 marks]

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

3. You have a lot of experience protecting systems, and like to stay up to date on the latest security research and news.

(a) Your top priority for maintaining the security of your system 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 always installing updates help defend against zero-day attacks?

[2 marks]

(b) Recently, it came to your attention that a website hosted by another company had vulnerabilities that made cross-site scripting attacks possible.

i) Briefly explain what an internet cookie is.

[2 marks]

ii) How could cross-site scripting attacks be used to steal a user’s cookies

[2 marks]

iii) What can an attacker do with stolen cookies?

[2 marks]

(c) You recall reading an article about metamorphic testing approaches applied to cybersecurity.

i) Briefly explain the motivation behind metamorphic testing.

[2 marks]

ii) Explain briefly what a code obfuscator does?

[2 marks]

iii) Based on your knowledge of metamorphic testing and code obfuscators, briefly explain one metamorphic relation that you could use to test a code obfustator.

[2 marks]

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam

<<End>>