The University of Nottingham Ningbo China

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, SPRING SEMESTER 2018-2019

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 a professor of computer security, and the only thing you enjoy more than securing computer systems is discussing and explaining aspects of computer security. Here are a series of questions from your students. Please answer all of them:

(a) Define the three components of the CIA model of computer security. [2 marks]

(b) Define Kerckhoffs's Principle. [2 marks]

(c) In the context of software testing, what is the oracle problem? [3 marks]

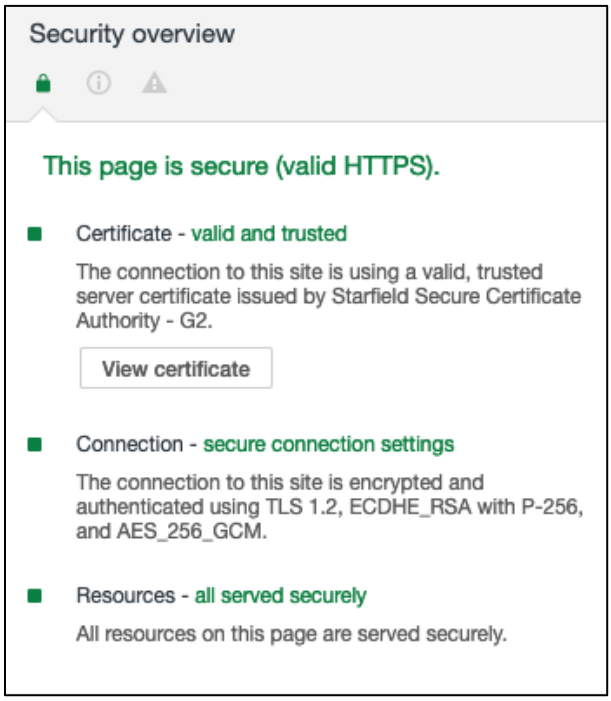
(d) What is the value of 17^{17} (MOD 9)? [3 marks]

(e) When passwords are used for authentication, they are usually are stored in hashed form in a database. Briefly outline the principles of offline password cracking based on dictionaries. [5 marks]

(f) What is the difference between heuristics-based and signature-based malware detection? Give two examples of security risks for a system that only uses signature-based detection. [5 Marks]

[TOTAL MARKS FOR QUESTION 1 : 20 MARKS]

2. You know that your students interact a lot on the Internet. They often come to you to discuss aspects of Internet-related security. After surfing the web (on Google Chrome), and interacting with the website www.flowersforangrygirlfriends.com, a student asks you how secure his connection to the website is. You look at the connection security information, which says:



(a) What do the letters TLS stand for? [1 mark]

(b) What does "ECDHE_RSA" stand for? [2 marks]

(c) Explain clearly (and briefly) two uses for RSA. [2 marks]

(d) If the Euler totient value (Φ) of 9 is 6 (1, 2, 4, 5, 7, 8), given two prime numbers 67 and 71, what is the Euler totient value of their product 4757?
[2 marks]

(e) Explain the process of the Diffie-Hellman key exchange.
(Note: there is no need to explain why this process is secure, you only need to list the process steps.)
[5 marks]

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

[TOTAL MARKS FOR QUESTION 2 : 20 MARKS]

3. As a professor, in addition to working with your students, you also often need to interact with industry. You sometimes offer expert advice to people working in local companies. Recently, the CEO of a medium-sized company has come to you for advice about all aspects of his company's security systems. He is curious about obfuscation, and wants to know how well a powerful code obfuscator may help protect his system from viruses.

(a) Explain briefly what a code obfuscator does. [3 marks]

(b) How much protection can a good code obfuscator offer against viruses, worms, and Trojans? [2 marks]

The CEO is curious about how to implement some aspects of a password policy. His company follows best practice, including storing hashes of passwords in a database, and not storing the passwords themselves. He wants to know how he can ensure that when his employees change passwords, how can he check that the new passwords are not similar to previously used ones.

(c) Briefly outline how this might be achieved. [5 marks]

The CEO has a large corporate network, and plans to use a signature-based intrusion detection system. He has also said that he will not need any host-based anomaly detection system.

(d) Describe the strengths and weaknesses of the CEO’s intended system. Explain what threats the system may be exposed to. Make any recommendations for the system that you think appropriate.

[10 marks]

[TOTAL MARKS FOR QUESTION 3 : 20 MARKS]

End of Exam

<<End>>