UNIVERSITY OF SOUTHAMPTON COMP6224W1

SEMESTER 1 EXAMINATION 2015 - 2016

FOUNDATIONS OF CYBER SECURITY

DURATION 120 MINS (2 Hours)

This paper contains 5 questions

Answer THREE of the following questions.

An outline marking scheme is shown in brackets to the right of each question.

Each question is worth 33 marks. The overall mark out of 99 will then be scaled up to 100.

University approved calculators MAY be used.

A foreign language dictionary is permitted ONLY IF it is a paper version of a direct ‘Word to Word’ translation dictionary AND it contains no notes, additions or annotations.

Page 1 of 6

Question 1.

(a) Explain what the ‘*Net Present Value*’ (NPV) of a investment is in the context of cyber security economics and cyber risk assessment, how it is estimated, and compare it with alternative approaches.

[10 marks]

(b) In the literature about cyber security economics it has been argued that the value of a company is the ‘*total lock-in*’ of all its customers. Explain in your own words what this means.

[7 marks]

(c) Explain what the terms ‘*best-effort*,’ ‘*sum-of-all-efforts*,’ and “*minimum-effort*’ mean in the context of secure software production. List at least one typical task for each category, and explain what conclusions might to be drawn from this by a security company.

[8 marks]

(d) In the scientific literature of economics, what does the term ‘*Market for lemons*’ refer to? Explain how this is relevant to cyber security.

[8 marks]

Question 2.

(a) What is meant by '*Mandatory Access Control*' (MAC)? Describe the notion, explain why it is important in cyber security, and illustrate one of its main implementations.

[7 marks]

(b) Describe and discuss the '*simple property*' and the '*-property' from the *Bell-LaPadula*' model (BLP). What are the main criticisms of such security model?

[10 marks]

(c) What does 'RBAC' stand for? How does it differ from the multilevel security model? What are its advantages?

[8 marks]

(d) What is meant by the term '*covert channel*'? List some examples of covert channels.

[8 marks]

TURN OVER

Question 3.

(a) What is meant by information warfare? And by cyberwarfare? Illustrate concisely the USA and the Chinese approaches.

[9 marks]

(b) In the context of cyberwarfare, what are the problems of '*attribution*' and '*deterrance*'? Describe the problems and discuss their impact and consequences.

[7 marks]

(c) Describe concisely the STUXNET attack. Illustrate your answer with a diagram to explain the various phases of the attack.

[10 marks]

(d) Describe and discuss the three components of a cyber weapon. Describe some noticeable difference between conventional (tactical) weapons and cyber weapons. [7 marks]

Question 4.

As distributed denial of service (DDoS) attacks have become more common, attackers have sought to find the means to maximise the impact of their attacks, and –generally– to minimise the chances of attacks being traced back to them. The DNS has been used in recent years as one such means.

(a) What do you consider are the main reasons for individuals or groups to want to conduct denial of service attacks?

[5 marks]

(b) Describe the sequence of interactions required for a DNS resolver to perform a recursive lookup on a hostname (as e.g. `www.bbc.co.uk`) to return its IPv4 address. Illustrate your answer with a diagram.

[7 marks]

(c) In early 2013, a large distributed denial of service (DDoS) attack took place against Spamhaus, in what was termed a 'DNS amplification attack.' Describe how the DDoS attack was believed to have been made, explaining clearly how the DNS was 'abused' to make the attack so effective, and the role of IP spoofing in the attack.

[9 marks]

(d) How would the use of a content delivery network, based on IP anycast or an equivalent technology, help mitigate such DDoS attacks for a content provider, and what other benefits might that use bring?

[6 marks]

(e) A generic problem in DDoS attacks is the ability of attackers to use IP spoofing. How might that problem be addressed by ISPs and operators of commercial or academic enterprise sites, and why do you think it has not been addressed seriously enough to date?

[6 marks]

TURN OVER

Question 5.

(a) Describe the main methods of *biometric* authentications, and their relative strengths and weaknesses.

[7 marks]

(b) Describe the basic *‘GSM’ authentication protocol*, and discuss its main vulnerabilities.

[10 marks]

(c) What is meant by API attack? Describe the ‘*Xor-To-Null-Key*’ attack as perpetrated against ATMs.

[9 marks]

(d) What is the ‘*Orange Book*’? Describe some of the ‘levels’ it mandates.

[7 marks]

END OF PAPER