TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS – 2013
TRIMESTER 1

NWEN 405

Security Engineering

Time Allowed: THREE HOURS

Instructions: *Read each question carefully before attempting it.*

This examination will be marked out of **150** marks.

Plan on spending about 1 minute per mark.

Answer **ALL** questions.

You may answer the questions in any order. Make sure you clearly identify the question you are answering.

Only printed foreign/English dictionaries are permitted.

You are permitted one single-sided HANDWRITTEN A4 page of notes.

Question	Topic	Marks
1	Cognitive and social psychology	30 marks
2	Security models	30 marks
3	Security protocols	30 marks
4	Malware	30 marks
5	Network security	30 marks

Question 1. Cognitive and social psychology [30 marks]

(a) [10 marks] Give examples of security problems that may result from the three following classes of human error: (1) Capture errors; (2) Following the wrong rule; and, (3) Cognitive mistakes.

(b) [10 marks] Consider a scenario where you receive an unsolicited phone call at work from a person claiming to work for Visa. They inform you that they are checking some odd activity and your account. They quote your credit card number to you and ask if you could read the three security digits on the signature strip to prove you still are in possession of the card.

What type of attack is this? Discuss how an understanding of social psychology could provide an insight into why this attack might succeed and provide a defence against it.

(c) [10 marks] You have been asked to design a password-based authentication system for an e-commerce website. With reference to the readings, outline a design that meets the following criteria: (a) is scalable; (b) password resets are minimised; and (c) at least one anti-phishing technique is used. When answering consider alternatives and possible problems with your design.

Question 2. Security models [30 marks]

(a) [5 marks] Briefly compare and contrast multilevel and multilateral security models in terms of their goals and application areas.

(b) [5 marks] Explain why the Bell-LaPadula star property was introduced to the security model.

(c) [5 marks] Outline the principle of *least privilege* and explain how this can be implemented by applying the principle of *weak tranquility* in the Bell-LaPadula security model.

(d) [5 marks] Briefly describe how a *covert channel* could be introduced into an operating system implementing Bell La Padula where the existence of files can be tested by any user.

(e) [5 marks] Briefly discuss why the Chinese-Wall model is considered to implement dynamic access control rules. Provide a simple example to illustrate your discussion.

(f) [5 marks] Do you consider inference control for Census data to be an example of multi-lateral or a multi-level security model? Make sure you justify your answer.

Question 3. Security Protocols [30 marks]

(a) [5 marks] List four uses of encryption in security protocols.

(b) [5 marks] Construct a simple protocol that would allow mutual authentication of two parties. The protocol should be secure against replay and man-in-the-middle attacks.

(c) [5 marks] Explain the relationship with a key's "freshnesses" and the likelihood of a replay attack being successful.

(d) [5 marks] Explain why it is prudent to mention the name of a principal in a message if the identity of the principal is essential to the meaning of the message.

(e) [5 marks] Both the formal approaches covered in class (*BAN logic* and *CSP-based model checking* require the simplification of the real-world protocols for analysis. Briefly discuss what is involved in the idealisation process.

(f) [5 marks] You have been shown a formal proof based upon model checking that claims that the protocol is secure. Discuss whether this protocol can be believed to the be completely secure.

Question 4. Malware [30 marks]

(a) Consider Staniford, Paxson and Weaver's paper *How to 0wn the Internet in Your Spare Time* where the authors analyse both the Code Red and Nimda worms and explore new techniques that attackers could use to increase the speed of spread.

(i) [10 marks] Discuss the techniques used by Code Red and Nimda to spread between hosts.

(ii) [5 marks] Explain the three main techniques identified by the authors that could improve the virulence of a worm.

(b) [10 marks] Consider designing a botnet yourself from scratch that will be hard for existing techniques to detect and shutdown. Provide a design that addresses issues related to: injection, spreading, command and control and methods for extracting money from the targets of the attack.

(c) [5 marks] Many viruses will not re-infect a machine that has already been infected. Briefly explain how this functionality is implemented and how it could be used to defend against virus infections.

Question 5. Network Security [30 marks]

(a) [5 marks] Consider ARP spoofing and Source routing attacks. Briefly describe each attack and identify the common trust assumption that made these attacks possible?

(b) [5 marks] Outline the advantages malware gains by being able to manipulate DNS lookups on an infected host and identify at least TWO methods of achieving this manipulation.

(c) [4 marks] Briefly explain how source port randomisation increased the work required by attackers to trick a DNS resolver into accepting a forged DNS reply.

(d) You are developing a multi-user computer game and wish to make it harder for players to cheat. Discuss the possible benefits of using:

(i) [2 marks] Encryption/authentication.

(ii) [2 marks] Firewalls.

(iii) [2 marks] Intrusion detection systems.

(e) [5 marks] Discuss the tradeoffs between the complexity of security policy enforceable by placing filtering at different layers and the cost of doing the filtering.

(f) [5 marks] Discuss to what extent firewalls and intrusion detections can be used to detect confidentiality breaches.

* * * * * * * * * * * * * * *