TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS — 2009

END OF YEAR

COMP 418

Security

Time Allowed: 3 Hours

Instructions:

- *Read each question carefully before attempting it.*
- This examination will be marked out of **150** marks.
- Answer all **ten** questions. Each question has the same value, and should take approximately 25 minutes to answer.
- You may answer the questions in any order. Make sure you clearly identify the question you are answering.
- Many of the questions require you to discuss an issue, or to express and justify an opinion. For such questions, you will be assessed on your answer, the *evidence* you present, and any *insight* based on these.
- Some of the questions ask for examples. Your answers need only refer to security mechanisms discussed in the course, but you may refer to other security mechanisms if you wish.
- Non-electronic foreign language-English dictionaries are permitted.

Question 1. Security Engineering [15 marks]

(a) [5 marks] With respect to Ross Anderson's definitions. Define the terms: *subject*, *principal* and *identity*.

(b) [5 marks] Identify the different possible principals in the following scenario: "When Alice gets to work she logs onto her computer by inserting a smartcard into a smartcard reader attached to the computer and entering a PIN number into a login dialog. She uses her PC to access the company's human resource system."

(c) [5 marks] Descibe a simple scenario to explain the difference between *trustworthy* and *trusted*

Question 2. Usability and Psychology [15 marks]

(a) [5 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] You have been hired by a bank to evaluate some suggested anti-phishing designs for their online banking system.

Explain briefly *at least* two strengths and weaknesses of each of the following four countermeasures: (1) SSL/TLS client certifications issued to each customer; (2) A handheld password calculator issued to each customer; (3) Displaying a unique picture to each customer during the login process; (4) Requiring that large payments, or payments to new recipients be authorised by telephone or SMS as well as online.

Question 3. Security Protocols [15 marks]

(a) [5 marks] Define the *Chosen Protocol Attack*. Describe a simple example.

(b) [10 marks] Consider this protocol that enables Alice to send a message m to Bob in the following way:

$A \longrightarrow B : m^{ka}(modp)$
$B \longrightarrow A : m^{ka,kb}(modp)$
$A \longrightarrow B : m^{kb}(modp)$

Explain what is happening in this protocol and its main vulnerability.

Question 4. Cryptography [15 marks]

(a) [10 marks] Describe the following modes of operation of a block cipher: electronic codebook; cipher block chaining, output feedback, cipher feedback, message authentication code and hash function.

(b) [5 marks] What mode(s) of operation would you use to protect the confidentiality of data traffic on a radio link with known rates of (a) bit errors and (b) burst errors causing loss of synchronisation.

Question 5. Access Control [15 marks]

(a) [2 marks] Define the main function of *access control*.

(b) [3 marks] Briefly summarise the strengths and weaknesses of *capabilities*.

(c) [5 marks] Discuss the tradeoffs between implementing access control at the middleware level and the operating system level. Make sure that you discuss issues such as granularity and the likelihood of errors in the access control mechanisms.

(d) [5 marks] You have been given the task of securing a database system. Briefly describe possible attacks that may be possible upon such a system.

Question 6. Distributed Systems [15 marks]

(a) [5 marks] List two security problems related to naming in a distributed system. Provide an example for each and make sure you make it clear how it is a security problem.

(b) [10 marks] One means of improving system reliabilty is to have three or more replicated systems and act on their majority output. Give *two* examples of security failure that can be stopped and *one* that cannot.

Question 7. Network Security [15 marks]

(a) [5 marks] Discuss the differences and similarities between a trojan, a virus and a worm.

(b) [10 marks] You discover a website promoting a new intrusion detection system that claims to address system integrity, confidentiality and availability. Evaluate whether it is actually possible to achieve all of these three aims.

Question 8. Security Policies [15 marks]

(a) [3 marks] Explain the difference between discretionary and mandatory access control.

(b) [7 marks] Describe the Bell-LaPadula security policy model.

(c) [5 marks] Explain what covert channels are, and how they can limit the usefulness of multilevel secure systems.

Question 9. Security engineering design, assurance and evaluation [15 marks]

(a) [5 marks] Briefly define the terms *assurance* and *evaluation*, and discuss their relationship with each other.

(b) [5 marks] You have just bought a new firewall. The vendor says that it has been proven secure through evaluation against the Common Criteria. What else do you need to know in order to evaluate the security of this system? What additional steps might you take to evaluate the security of the firewall product?

(c) [5 marks] You are developing a new secure database product. You have applied the traditional assurance techniques for such a project. Discuss how you might use some newer techniques for evaluation and assurance in your development process and briefly describe their benefits.

Question 10. Biometrics [15 marks]

(a) [5 marks] Briefly describe the steps involved in using a biometric to check the identity of a person.

(b) [5 marks] Briefly describe the strengths and weakness of using the patterns of people's irises for identification.

(c) [5 marks] Your employer has purchased a fingerprint biometric system. At the start of each day you check in by presenting your fingerprint and at the end of the day you do the same thing. Your workplace has 100 employees and for this numner of people the fraud rate is .01% and the insult rate is .1%. Discuss the potential issues that would arise if you scaled such a system up to a workplace of 10,000 people.

****