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

EXAMINATIONS — 2010

END OF YEAR

NWEN 405

Security Engineering

Time Allowed: 3 Hours

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

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

Answer all **five** questions. Each question has the same value, and should take approximately 30 minutes to answer.

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

Non-electronic foreign language-English dictionaries are permitted.

Question	Topic	Marks
1	Security Policies	30 marks
2	Secure Software Engineering	30 marks
3	Securing Networks	30 marks
4	Security in the Real World	30 marks
5	Security Economics	30 marks

Question 1. Security Policies [30 marks]

(a) [4 marks] List THREE approaches that an organisation might choose to implement a security policy and write a sentence to describe each approach.

(b) [12 marks] Describe THREE problems from which classical multilevel-secure systems suffer. Write several sentences to illustrate each problem.

ro **(c)** [4 marks] Explain the concept of a Trusted Computing Base and outline its meaning in the context of the access control provided by a typical Unix workstation.

(d) [10 marks] Describe at least THREE reasons that led to the BMA policy model being proposed for the United Kingdom's National Health Service instead of a multilevel security policy.

Question 2. Secure Software Engineering [30 marks]

(a) [5 marks] A common approach to secure software engineering is based developing software patches as vulnerabilities are discovered (the *Patch cycle*). Briefly make an argument against the sustainability of this approach.

(b) [5 marks] Briefly define the term *secure software architecture*.

(c) [5 marks] Discuss whether the security engineering approaches discussed in class are limited to being applied to the waterfall model.

(d) You have hired by a company which is bidding to take over the provision of the New Zealand LOTTO website. This website allows customers to:

- Purchase LOTTO tickets and pay for these using their credit cards.
- Check whether they have won or not in the Wednesday or Saturday draws.

(i) [6 marks] Develop part of a threat model for a replacement system. The threat model should identify at least THREE risks and briefly describe how the risks might be realised by an attacker.

(ii) [4 marks] Assume that you are now implementing the system. Identify FOUR security implementation practices that your team should follow and illustrate how they might apply in this particular case.

(iii) [5 marks] Your boss suggests that the evaluation approach used by the previous supplier should be used. This consisted of a series of checklists to be followed by the security evaluators. Explain whether you agree or disagree with this approach.

Question 3. Securing Networks [30 marks]

(a) [8 marks] Denial-of-service attacks upon companies can be seen as a form of blackmail. Identify FOUR security principles that can be applied to mitigate the risk of such attacks and write TWO or THREE sentences illlustrating the application of each principle.

(b) [6 marks] Write THREE or FOUR sentences to describe each of the following:

(i) The Internet Worm

(ii) Trojan horses

(iii) Polymorphic viruses

(c) [4 marks] Discuss the similarities and differences between the immunization and scanning approaches to dealing with computer viruses.

(d) You are developing a multi-user computer game, and wish to make it harder for players to cheat.

Discuss the *pros and cons* of using:

(i) [4 marks] Encryption/authentication

(ii) [4 marks] Virus detection technology

(iii) [4 marks] Intrusion detection techniques

Question 4. Security in the Real World [30 marks]

(a) [5 marks] List the FIVE common elements of a physical protection system and write one sentence describing each element.

(b) [10 marks] You are planning the physical security of a server farm that will host business websites. Colleagues suggest locating the server farm in an isolated industrial area surrounded by high fences and with a permanently staffed guard post. Propose an alternative to this design that based upon what you have learnt about theories of deterrence in this course. You should be aiming to identify FIVE design features. Justify your choices.

(c) [15 marks] You have been commissioned by New Zealand's Ministry of Economic Development (MED) to manage a project to replace New Zealand's 4 million electricity meters with smart meters that report energy use every 30 minutes. These reports go to a central service, and energy companies have access to their customers readings. The goals of the system are to facilitate more flexible pricing, so customer demand can be brought more into line with supply; to make it simpler for customers to switch energy companies; and to help MED predict and manage energy demand.

What could go wrong and what measures would you take to reduce the likelihood of a project disaster.

Question 5. Security Economics [30 marks]

(a) [6 marks] Write THREE or FOUR sentences to describe each of the following concepts:

(i) Marginal cost of production

(ii) Pareto efficient allocation

(iii) Discriminating monopolist

(b) [6 marks] Consider the Apple iPhone and an Android-compatible phone such as the (High Tech Computer Corporation) HTC Desire. Discuss, with respect to the consumer, whether Apple has achieved more or less *lock-in* than HTC.

(c) [10 marks] You are the owner of a startup and involved in advertising for new staff to join your development team. Security is a key issue for you. Discuss, with respect to *Hal Varain's* work, whether you should hire a security tester or a programmer.

(d) [8 marks] It is 1980 and L33T/DOS has been chosen over MS-DOS as the operating system for the new IBM PC. Several academics have voiced concerns over the security of L33T/DOS.

Outline a least FOUR policy measures that the US Government could take that might lead to better operating system security.

****