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

EXAMINATIONS — 2012

MID TERM

NWEN 405

Security Engineering

Time Allowed: 45 minutes

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

This examination will be marked out of **30** marks.

Answer all **three** 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 allowed one single sided A4 page that can be handwritten or typed.

Question	Topic	Marks
1	Security problems and code review	10 marks
2	Risk modelling and security testing	10 marks
3	Malware, viruses and worms	10 marks

Question 1. Security Problems and Code Review [10 marks]

(a) [5 marks] You are developing the new user interface for the *GERTY 3001* computer and have been told to use a computer vision library *Tuhere-Computer Vision Library*. Assume that the source code is available for the library. Outline how you would evaluate the security of the library in the context of your application.

(b) [5 marks] During a work meeting at *Wolfram & Hart Attorneys at Law*, one of your colleagues claims that static analysis tools are a waste of time because they only capture 5-10% of software quality problems. He claims that it would better to test the completed code. Make an argument for the use of static analysis tools as part of secure software development.

Question 2. Risk Modelling and Security Testing [10 marks]

(a) [5 marks] You are a security consultant hired to do a security analaysis of the risks faced by backpackers who do their Internet banking at the local *T'Rain Cyber Cafe*. Design a threat tree that that represents an attacker's goal of transfering money from a victim's account to one controlled by the attacker.

Assume that you have physical access to the machines in the cybercafe. Your tree should contain both AND-nodes, OR-nodes, have at least one branch that is two levels deep, and include social engineering, physical and cyber threats.

(b) [5 marks] Consider the relationship between risk modelling (threat modelling in the Microsoft software development lifecycle) and security testing. In particular, how risk modelling help in the choice of security-relevant tests and how risk modelling can be used to determine how you choose mitigation strategies for security bugs found during testing.

Question 3. Malware, Viruses and Worms [10 marks]

(a) [5 marks] Discuss the differences and similarities between a trojan, a virus and a worm. You should use the characteristics discussed in lectures when answering this question.

(b) [5 marks] Consider the following approaches to malware protection: (1) a first-generation virus scanner; (2) digital immune systems; and, (3) behaviour blocking software. Briefly evaluate the potential effectiveness of each of these approaches for limiting the effects of an outbreak of the *Atreides flash worm* within an organisation. Assume that this is the *first time* that the worm has ever been seen in the wild.

****