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

EXAMINATIONS — 2011

END OF YEAR

NWEN 405

Security Engineering

Time Allowed: 2 Hours

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

This examination will be marked out of **60** 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.

Question	Topic	Marks
1	Security in the Real World	20 marks
2	Secure Software Engineering	20 marks
3	Secure Networks	20 marks

Question 1. Security in the Real World [20 marks]

(a) [10 marks] During a work meeting at Goliath National Bank, one of your colleagues claims that *only stupid people fall for phishing scams*. Drawing upon what is known about cognitive and social psychology, write a counter-argument to his claim.

(b) [10 marks] With respect to **both** physical assets and physical protective measures, what are arguments in favour of and against the claim *obscurity provides security*? Your discussion should draw upon appropriate theories and experimental evidence.

Question 2. Secure Software Engineering [20 marks]

(a) [10 marks] Consider a web application written in C++ that accepts user input via a form and uses it to construct a SQL query. Explain what vulnerabilities should be mitigated in this web application, which general secure design principles are being violated and outline one or more mitigation strategies.

(b) [10 marks] Consider the relationship between risk modelling (threat modelling in the Microsoft software development lifecycle) and secure software evaluation. In particular, discuss what is risk modelling, what are the limitations of functional tests with respect to security testing, 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. Secure Networks [20 marks]

(a) [10 marks] Outline four examples of different denial-of-service attacks based upon amplification techniques at the network and application layer. For each example, explain the vulnerability being exploited, the type of amplification that results and possible mitigations for the attack. Make sure you include at least one example of both impact and traffic amplification.

(b) [10 marks] Consider misuse (also known as signature-detection) and anomaly-detection network intrusion detection systems. In particular, discuss how these compare in terms of false positive rates, what effect does the stability of the environment into which they are deployed have upon their accuracy, how these compare in terms of performance as time goes on and how they compare in terms of allowing the type of attack to be determined.

****