THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2006
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: TWO hours)

NOTE: Attempt **ALL** questions in the 12-page script book provided, using approximately **25** words to answer each 5-mark question, **50** words to answer each 10-mark question, and approximately **75** words to answer each 15-mark question. Total possible: **100 marks.**

A. Chen et al. have defined two goals for their biometric identification system.

G1. The end-user's biometric information is not disclosed to to any unauthorized entity.

G2. No unauthorised entity should know that the end-user is accessing, or has accessed the biometric system.

They consider the following threats:

T1. Interception of communications between the SC and the platform,

T2. Interception of communications between the platform and the BR,

T3. Malicious BRs, and

T4. Malicious platforms.

1. Butler Lampson, in his article "Computer Security in the Real World", identifies four general goals of security: Secrecy, Integrity, Availability, and Accountability. He identifies three basic mechanisms for implementing security: Authentication, Authorisation, and Auditing. His five defensive strategies are isolate, exclude, restrict, recover, and punish. Using Lampson's terminology, describe the security specification and implementation of the biometric identification system proposed by Chen et al. **(10 marks)**

2. Draw and briefly discuss a system diagram showing an end-user (U), a platform (P), a smart card (SC), a biometric reader (BR), and an attacker (A) who is attempting to violate G1 or G2. To obtain full credit, your diagram must contain numbered labels showing how the information flows through the system during normal use and during an attack. Your diagram should indicate the location of the valuable item, information, or service ($$) which is being protected by the system. Briefly discuss the operation of the system, referring to all arcs and entities in your system diagram. **(15 marks)**

3. Discuss the trust boundary in this system. Which of the entities are trusted, and which are untrusted? **(5 marks)**

4. Chen et al. argue that their system is secure against threats T1, T2, T3, and T4. Describe another plausible threat (T5) to G1 or G2. If the design of Chen et al. provides any defense against your new threat T5, discuss this defence, otherwise indicate **one way** in which some defence might be provided. **(10 marks)**

5. Communication links may be vulnerable to modification, fabrication, and interruption attacks, in addition to the interception attacks of threats T1 and T2. Write a new threat (T6) which involves the modification of messages on the link between the platform and the BR, and which could harm either the end-user or the owner of the system. Does T6 threaten either G1 or G2? Briefly explain, proposing a new security goal (G3) if your answer is "no". **(10 marks)**

B. In two of your required readings, virtual machines were an important part of the experimental setup.

6. Describe one experiment described in your required readings in which virtual machines were used. If real machines had been used instead, would the results have been less accurate? Would there have been any other significant advantage or disadvantage? Explain your answers briefly. **(10 marks)**

C. Some of your required readings described a malware detector, an intrusion detector, or a spam detector.

7. One of the detectors uses an "address dispersion" heuristic to distinguish malware from non-malicious network traffic. Would a similar heuristic help a spam detector to distinguish spam from non-spam email? Explain briefly. **(5 marks)**

8. The spam detector in your required reading used a data compressor to distinguish spam from non-spam email. Would a similar heuristic help distinguish malware from non-malicious network traffic? **(5 marks)**

9. Describe a simple experiment which would allow you to estimate the false-positive and false-negative error rates of a spam filter. Your dataset for this experiment should be 1000 email messages, chosen at random from the incoming traffic of our University's email system on Monday 8 October 2007. For full credit, your description should identify and briefly discuss two experimental limitations. **(10 marks)**

D. Giorgini et al. describe an ECO model. In this model, actors are characterised by their entitlements, capabilities, and objectives. In order to reach their objectives, actors must form relationships with other actors, and there are three types of such relationships: functional dependencies, trust relations, and delegations of permission.

10. Use the ECO model to describe the actors and relationships between a guard and a subject in the access-control scenario of Lampson's survey article. Discuss the success (or failure) of the ECO model in this application. **(10 marks)**

11. In the article by Blaze et al., the authors described a purchase-order authorisation system, in which three directors' signatures are required on every purchase order. Assume there are four directors, named Alice, Jack, Jean, and Matt. Assume someone named Paul wants to obtain authorisation on a purchase order. Describe this situation in the ECO model. For full credit, you must characterise (and discuss) the entitlements, capabilities, and objectives of all five actors (Paul, and the four directors). You must characterise (and discuss) the relationship (if any) between Paul and each of the directors, as well as the relationship (if any) between any two of the directors. **(10 marks)**
