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. Gallery et al. analyse the Digital Video Broadcasting standards in the context of mobile receivers such as 3G cellphones. The security requirements considered in this analysis are to maintain the integrity and confidentiality of the conditional-access software Z during its transport to the mobile receiver R, during its storage on R, and during its execution on R. The other actors in Gallery's model are the video broadcaster B, the software provider S, and the attacker A. The goal of the attacker A is to access some video V which can be decrypted by legitimate users of the software Z. Gallery identifies seven threats, quoted below:

T1. Unauthorised reading of the application code and data while in transit.

T2. Unauthorised alteration of the application while in transit.

T3. Unknowingly communicating with an unknown and potentially malicious entity.

T4. The inability to corroborate [get independent verificaition of] the source of the conditional access application.

T5. Replay of communications.

T6. Unauthorised reading or modification of the application while in storage on the mobile host.

T7. Unauthorised reading or modification of the application while it executes on the mobile host.

1. Draw a diagram of the information flow in this system. Label your diagram so that it shows the seven threats (T1 through T7) listed above. Discuss your diagram and its labelling briefly. **(10 marks)**

2. Draw a fishbone cause-effect diagram of these seven threats. To receive full credit, your diagram must show names for at least two, and no more than four, general categories of threat. Note: the fishbone diagram in the survey article by Jain shows five categories of threat: Administrative, Infrastructure, Non-Secure Processing, Intrinsic, Patent. Your fishbone diagram should use these categories, if you think they are appropriate in this context. **(10 marks)**

3. Analyse your diagrams from the previous questions, and consider other required readings in COMPSCI 725, in order to identify an eighth threat to Gallery's security requirements. To receive full credit, you must briefly discuss a plausible way in which an attacker might implement this threat. **(10 marks)**

4. Consider this content-distribution system from the perspective of the readers as well as the writers and administrators of the controlled content. In particular, consider Garden's analysis of IRM v1.0. State and briefly discuss an additional security requirement that an end-user might reasonably expect to be enforced by this content-distribution system. To receive full credit, your discussion must briefly describe a plausible goal for an attacker who would want to prevent the system from meeting your new requirement. You must also identify a plausible threat to your new requirement, at a level of detail similar to T1 through T7 above. **(10 marks)**

B. Facial biometrics might be used to screen the people attending a sporting event, in an effort to identify and then apprehend terrorists. The terrorist screening is conducted in a region with 10 million people, any of whom is equally likely to be one of the 10,000 people attending a sporting event. The screening database contains facial biometric information on 100 suspected terrorists.

5. Name, and briefly discuss three types of error that would occur in this screening system. To receive full marks, your discussion should include a calculation of an acceptable error rate, with reference to Axelsson's article on the "base rate fallacy". **(15 marks)**

C. An automated teller machine (ATM) has been equipped with a video camera to detect insider fraud. This ATM creates an audit trail of the account number, facial biometrics, and dollar amount withdrawn by each person who makes a withdrawal.

6. Draw a security use-case diagram for withdrawals on this ATM machine, using notation from the article by Gomaa et al. Discuss your diagram briefly. **(10 marks)**

7. Draw a key-challenge graph, using notation from the article by Chinchani et al., to illustrate one way an insider might make an unauthorised withdrawal with a fraudulent card, if they know the PIN. Discuss your graph briefly. To receive full credit, your graph and your accompanying discussion must describe a plausible attack on a plausibly-designed auditing subsystem, where the attacker's goal is that their identity should not be revealed by the biometrics stored in the audit record of the fraudulent transaction. You should use terminology from the Jain article in your discussion. **(10 marks)** .

D. Consider the following portion of our University's IT Acceptable Use Policy v1.3.

"Users must ... keep their computer password confidential [and] where systems currently permit it, select a password that ... [has] a minimum of eight characters and at least one character from three of the following four classes:

- English upper case letters
- English lower case letters
- Numerals (0,1,2,...)
- Non-alphanumeric (special) characters such as punctuation symbols."

8. Would any password complying with this policy be resistant to the brute force attack that was described by Amesbury? Briefly explain and justify your answer. **(5 marks)**

9. Would any password complying with this policy be resistant to the dictionary attack that was described by Amesbury? Briefly explain and justify your answer. **(5 marks)**

10. Would any password complying with this policy be resistant to the keyboard acoustic attack that was described by Zhuang et al? Briefly explain and justify your answer. **(5 marks)**

E. This year in COMPSCI 725, we read about two experimental estimations of the prevalence of malware on the internet. One set of experiments was conducted by Moshchuk et al. of the University of Washington, and was described in their article "A Crawler-based Study of Spyware on the Web". The other set of experiments was conducted by Wang et al. of Microsoft, and was described in "Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites that Exploit Browser Vulnerabilities".

11. Compare and contrast the experimental methodologies of these two studies. **(10 marks)**