THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2005
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.**

1. Butler Lampson, in his article "Computer Security in the Real World", identifies three basic mechanisms for implementing security: Authentication (of principals), Authorisation (of access), and Auditing (of the guard's decisions). Lee et al., in their "Architecture for Protecting Critical Secrets in Microprocessors", defines a computing system they call an SP-architecture.

(a) Draw a picture to illustrate the operation of an SP-architecture, when end-user Alice types her passphrase in order to access her Trusted Software Module (TSM). To obtain full credit, your picture must clearly show the interactions between its elements, which must include at least two of the security mechanisms, Alice, the guard, and the TSM. Your picture must also have an appropriate caption of approximately 50 words, in which you very briefly explain each of its elements and their interactions. **[10 marks]**

(b) Alice is using an internet kiosk that is advertised as having an SP-architecture. She downloads her TSM from her homepage, then types her passphrase, and then accesses her bank account. Briefly describe a plausible attack on the confidentiality of her TSM, and analyse this attack. Your analysis should clearly indicate what the attacker would do, in order to mount this attack. Your analysis should also identify which of Lampson's basic mechanisms has a vulnerability in this system which is being exploited by this attack. **[5 marks]**

(c) Alice uses an internet kiosk that claims to have a Trusted Platform Module (TPM) as well as an SP-architecture. Briefly discuss what protection Alice's Internet Service Provider (ISP) might provide, against the attack you described in your answer to the previous question. For full credit, your discussion should clearly describe how (or whether) the ISP might prevent this attack, how it might detect this attack, and how it might respond if an attack is detected. **[10 marks]**

(d) Camenisch, in "Better Privacy for Trusted Computing Platforms", discusses a privacy risk to users of TPMs. Briefly evaluate this privacy risk to Alice, when she is using a TPM when accessing her bank account from an internet kiosk. For full credit, your discussion should either include a plausible attack scenario, or else it should include an argument that Camenisch's privacy risk is unimportant to Alice in this situation. **[5 marks]**

2. A webservice is available for the users of smart cellphones. Webservice subscribers can use either a web interface, or their cellphone interface, to update their current list of the names and phone numbers of their friends and acquaintances. The version of the contact list in a subscriber's cellphone is updated with information from their contact list at the webservice, and vice versa, whenever the subscriber calls a special telephone number maintained by the webservice. Caller-ID is used for authentication on these calls. Name-password authentication is used on the web interface.

(a) Write a security requirement for this webservice, specifying a level of confidentiality that you believe would be acceptable to at least 20% of the population in New Zealand. For full credit your goal should be, at least roughly, in the format proposed by Firesmith in "Specifying Reusable Security Requirements". **[5 marks]**

(b) Discuss how an attacker might violate your security requirement, by exploiting a vulnerability in the authentication method. For full credit, you should describe a vulnerability that was discussed in our classroom. **[5 marks]**

3. You have been asked, by your employer, to examine the files on a desktop computer at your workplace. This computer is used by Bob, one of your co-workers. Your employer suspects that Bob has sent email, containing company secrets, to a competitor. This would be a clear violation of his employment contract. Bob's employment contract also gives you (as a fellow employee) the right to examine the files on Bob's desktop computer at any time, and without his consent, if you are directed to examine these files by your employer.

What would you do in this situation? Discuss your decision briefly, from a technical and legal perspective. For full credit, you must either indicate how you would go about examining Bob's files, or else you must supply a good argument (on either technical or legal grounds) why you should not agree to examine these files. **[5 marks]**

4. Consider the attacks discussed in Byers et al., "How to Cheat at Chess: A Security Analysis of the Internet Chess Club".

Conduct a misuse case analysis of the Internet Chess Club. For full credit your analysis should include a diagram in the style of Alexander's "Misuse Cases: Use Cases with Hostile Intent", and it should cover one of the attacks discussed in the article by Byers et al. **[10 marks]**

5. Soman et al., in "Detecting Malicious Java Code Using Virtual Machine Auditing", suggested using a Java thread to audit the activities of other Java threads. If malicious activity is detected, the offending thread is terminated.

(a) Discuss the errors and correct responses of Soman's system. For full credit, you must clearly identify four cases using the following acronyms: FP, TP, FN, TN. **[10 marks]**

(b) Herzog et al., in "Problems Running Untrusted Services as Java Threads", identified three problematic areas: safe termination, resource control, and isolation. Critically and appreciatively discuss the system proposed by Soman et al., considering these problematic areas. **[5 marks]**

6. Imagine a world in which a billion people are using a superdistribution system similar to the one proposed by Mori et al. in "Superdistribution: An Electronic Infrastructure for the Economy of the Future". A few thousand people are actively attacking the system, either as pirates or as liberators. The active attackers are called pirates when they modify superdistribution labels so that the attacker will receive payment, through the superdistribution system, from future uses of the digital object with the modified label. The active attackers are called liberators when they remove the superdistribution label. Both pirates and liberators post the modified digital objects to their website.

(a) Could pirated or liberated objects be detected reliably, and easily, by users who actively support the superdistribution system? If modified objects are detected by superdistribution supporters, and are reported to some central authority, what legal or financial responses could taken by the central authority, in order to minimize the effects of object piracy and liberation? Write a very short essay (approximately 50 words) in response to these questions. **[10 marks]**

(b) Name, and briefly discuss, two technologies discussed in required readings other than the Mori superdistribution paper, which could be used to improve the security of the superdistribution system. **[10 marks]**

7. In our classroom, we discussed many aspects of scientific writing.

Name, and briefly discuss, two ethical issues in scientific writing. For full credit, for each issue you should analyse a situation arising in our required readings, in terms of an ethical conflict between two of Pfleeger's three rights (knowledge, confidentiality, compensation). **[10 marks]**
