THE UNIVERSITY OF AUCKLAND

FIRST SEMESTER, 2003
Campus: City

COMPUTER SCIENCE

Software Security

(Time Allowed: TWO hours)

NOTE: Attempt **ALL** questions in the 12-page script book provided. Total possible: **100 marks.**

1. Consider the four types of security threat, defined in Pfleeger's book: interception, interruption, modification, fabrication. Also consider the following clause in the "Guidelines for the Use of University Computing Facilities and Services":

> Users shall work in a manner that does not jeopardise the security of the system and shall satisfy all reasonable demands by authorised staff to demonstrate that they are authorised to use the facilities. This includes: ... not conducting or attempting to conduct security experiments or security scans involving or using University computer or network resources without the expressed written permission of the University Computer and Network Security Officer.

Which (if any) of Pfleeger's threats are controlled by this clause? Explain your answer briefly, in approximately 50 words. **[10 marks]**

2. The designers of DIDAFIT describe their system in the following words:

> [DIDAFIT] can be broadly classified as a signature-based IDS with enhanced capabilities for learning and deducing new signatures... It works by fingerprinting access patterns of legitimate database transactions... Every submitted SQL statement is matched with the set of legitimate fingerprints. If the SQL statement cannot match any of the fingerprints, then an intrusion may have occurred... [We present an] algorithm to automatically generate the set of fingerprints ... from a trace log *LOG*... Each "unsafe" or "derived" fingerprint that is approved by the DBA will be marked as "safe". If there remains any "unsafe" fingerprints then an intrusion has occurred in *LOG*. ...

a. Consider the following definitions, drawn from McHugh's article, of anomaly-based IDSs and signature based IDSs.

- An anomaly-based system reports an intrusion whenever it observes any significant departure from normal activity. Such intrusion detection systems determine what is "normal" by comparing the current activity to some model of normal activity.

- A signature-based system reports an intrusion whenever it observes activity that matches an attack signature. Every signature-based system has a model consisting of a set of attacks that it can recognize.

Is DIDAFIT a signature-based IDS, or is it an anomaly-based IDS? Explain briefly. Your answer should be about 50 words in length. **[10 marks]**

b. McHugh makes the following distinction between self-learning IDSs and programmed IDSs.

- A self-learning IDS updates its own model more or less continuously, with little or no intervention by the system administrator.
- By contrast, the model in a programmed IDS is updated only occasionally: perhaps once per week, possibly by an automated download of a revised model from a remote site.

McHugh gives two reasons why self-learning **anomaly-based** intrusion detection systems are not perfectly accurate: "Changes [in the normal distribution of activities] may cause false alarms while intrusive activities that appear to be normal may cause missed detections."

Would both of McHugh's reasons be applicable to self-learning **signature-based** intrusion detection systems? For full credit your answer must briefly describe how an actual, or proposed, self-learning signature-based IDS would learn new signatures; and then your answer should very briefly give separate consideration to each of McHugh's two reasons. Your answer should be approximately 50 words in length. **[10 marks]**

3. The design of a security system often involves tradeoffs between desirable objectives.

a. Briefly describe a system, which you studied in COMPSCI 725, involving a tradeoff between confidentiality and integrity. For full credit your answer should clearly indicate how this system could be modified to achieve a different tradeoff between these objectives, i.e. more confidentiality at the expense of integrity, or more integrity at the expense of confidentiality. Your answer should be approximately 50 words in length. **[10 marks]**

b. Briefly describe a system, which you studied in COMPSCI 725, involving a tradeoff between integrity and availability. For full credit your answer should clearly indicate how this system could be modified to achieve a different tradeoff between these objectives. Your answer should be approximately 50 words in length. **[10 marks]**

c. Briefly describe a system, which you studied in COMPSCI 725, involving a tradeoff between availability and confidentiality. For full credit your answer should clearly indicate how this system could be modified to achieve a different tradeoff between these objectives. Your answer should be approximately 50 words in length. **[10 marks]**

4. Maude and Maude have described a method for protecting software, in the following words:

> ... portions of the program code are encrypted, so that at run time they have to be decrypted before they can be obeyed. ... Each computer would be provided with its own pair of public and private keys so that a program would have to be customized for a computer and would only run on that particular machine.
>
> ... although many programs may be run, the computer owner only needs to purchase a single security unit.
>
> ... Computer programs need to be modified in two ways to use the system. First, some program steps have to be selected such that, without knowing what these steps do, the program will be so opaque that it cannot be understood. Second, the coding of these parts must be put into a form so that they may be deciphered by a particular security unit.
>
> ... The function of the unit may be split into two parts, each using a separate cryptographic system. At program start-up, a "decoding key" is passed from the program to the unit. This operation is only performed once for each run of a program. The decoding key is itself encrypted using the security unit's public key cryptogram. The security unit deciphers this decoding key so that it is available for the second cryptographic system. The second function is to decode and obey instructions as they are passed to the unit. This function uses the second cryptographic system. ...

In this exam question, we will use the acronym MM to refer to Maude and Maude's method.

Maña and Pimental have described two methods (which they call "schemes") for protecting software. In this examination, we will use the acronym MP to refer to their "final scheme". They describe their schemes as follows:

> [In our production phase] original code sections are substituted by calls to a function that transmits their equivalent [i.e. translated for the card's execution environment] code and data, to the card, where [the translated sections] are decrypted and executed. When finished, the card sends back the results. [In our first scheme, the translated] sections are encrypted with the public key of the card using an asymmetric cryptosystem... [but this] introduces a high computational cost.
>
> [In our final scheme MP] the production phase includes the encryption of the protected sections (which include code and data) with a symmetric cryptosystem. ... [We also add] a code authentication mechanism... [which allows] license transfer or expressive authorisation... [With MP] the software [may] be freely distributed, although to run it the user will need to get a license...
>
> In [MP's] authorization phase (equivalent to the personalization phase of our first scheme), a new license is produced containing the random symmetric key used to encrypt the protected sections, information about conditions of use (i.e. time limits, number of executions, etc.), the identification of the software (ID, version number, etc.) and finally the identification of the license. All this information is encrypted with the card public key. When the license is received by the client it is stored in the card. ...

Compare and contrast MM with MP. For full credit your answer should clearly state (and very briefly explain) whether or not MM has a design element that is similar to each of the following design elements of MP: production phase, authorization phase, license, public key of the card, private key of the card, and symmetric key. Your answer should also briefly discuss any other important similarities and differences between MM and MP. Your answer should rely primarily on information drawn from the quotations above; however in cases where you rely on your memory of your readings about these proposals, you should indicate this in your answer. Your answer should be approximately 75 words in length. **[15 marks]**

5. The Malaysian government recently started using biometric smart cards for identification purposes. These cards store many kilobytes of personal information, including fingerprint biometrics, medical records, and a drivers license number. A police officer may use a smart-card reader and fingerprint reader to determine the identity of a driver who is being issued a ticket for a motor vehicle offense.

   As noted by Armington in his article "Biometric Authentication in Infrastructure Security", the following problems may arise in any biometric authentication scheme: false acceptance (FA) of biometric authentication, false rejection (FR) of biometric authentication, and failure to enrol (FTE). Which of these issues are relevant to the use of the Malaysian smart card by a police officer when issuing a ticket?

   For full credit your answer should clearly note whether or not you believe each of the three problems (FR, FA, and FTE) is relevant, and you must justify each of these three answers briefly. **[15 marks]**

6. In Benes' proposal for a strong eternity service, a client C selects an eternity server E and pays a data storage fee to a bank B. After the storage period (perhaps one year) has expired, the bank B pays the client's data storage fee to any Eternity Server E' that is able to prove (by a cryptographic protocol) it is able to retrieve a copy of C's data. We may assume that the cryptographic protocol is not faulty, so that E will be able to properly claim payment as E'. The client C is given a way to send its data to E, and C is also given a way retrieve its data from E any number of times during the paid storage period, however C has no other information about E. The client C is fully anonymous to E. So we may say that E offers an anonymous data storage facility to C.

   Consider a client C who is trying to decide whether or not they should trust the strong eternity service to provide access, during the storage period, to the data they have stored on E – where this access should have a very high degree of confidentiality, integrity and availability.

   Are Benes' arguments in favour of his strong eternity service an example of the "trust shell game" defined by Ellison? Discuss your answer briefly in approximately 50 words. For full credit your answer should indicate the most important trust relationships among E, C, B and other actors in the strong eternity service; your answer should define the "trust shell game"; and your answer should give a reason why Benes' paper is, or is not, a "trust shell game". **[10 marks]**