THE UNIVERSITY OF AUCKLAND

FIRST SEMESTER, 2001
Campus: City

COMPUTER SCIENCE

Software Security

(Time allowed: TWO hours)

NOTE: Attempt **ALL** questions in the 12-page script book provided, using approximately **50** words to answer each of the four 10-mark questions, and approximately **75** words to answer each of the four 15-mark questions. 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 respects the rights of other users of the services or facilities and of people elsewhere. This includes: ... not sending obscene, abusive, fraudulent, threatening or repetitive messages to others. ..."

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

2. A company is planning to release software for an implementation of IBM's 2KP protocol for electronic payment. This software is designed as a client-server architecture, where the client software is a Java applet. The end-user of this software must type their 16-digit credit card number and 4-digit PIN to authenticate themselves to the Java applet, every time they authorise a new charge to their credit card.

This company is concerned about the following security threat. A hacker "H" might insert "Trojan Horse" code into the Java applet, before it is used by some unsuspecting user "U". The Trojan Horse would intercept the user's credit card number and PIN, then transmit this information over the internet to the hacker "H". The hacker "H" could use this information to make fraudulent credit card transactions in the future.

What *two* security techniques, discussed in this class, could be used to control this security threat? For full credit, you must name and briefly explain *two* (and no more than two) applicable control techniques, and you must indicate a possible "counter-attack" that could be mounted by H to subvert each control you propose. [15 marks]

3. Hunt's paper on "Internet/Intranet Firewall Security..." describes two types of firewalls in the following words.

> Packet-level firewalls ... operate at the network (IP) and transport (TCP) layers. These are commonly referred to as screening routers or packet filters and block transmission of certain classes of traffic.
>
> [A]pplication-level firewalls ... operate at the session, presentation and application layers. They are usually implemented using dedicated hosts running specialised software and can also be referred to as bastion hosts or proxy servers, usually running under UNIX or Windows NT. They can also provide relay services to compensate for the effects of the filters.

In addition to reading Hunt's paper, you read a paper by Gilmore *et al.* This paper describes a PushWeb/Absent system, which was designed to permit only "valid absent users" to access AT&T's intranet.

Which (if any) of Hunt's two types of firewalls is a good description of the PushWeb/Absent system? For full credit, you must briefly and accurately explain the operation of the PushWeb/Absent system using as much of Hunt's terminology as possible. [10 marks]

4. Law *et al.* list the following security properties as "necessary" for electronic payment systems:

- *Privacy*, or protection against eavesdropping. This is obviously of importance for transactions involving, *e.g.*, credit card numbers sent on the Internet.
- *User identification*, or protection against impersonation. Clearly, any scheme for electronic commerce must require that a user knows with whom she is dealing (if only as an alias or credit card number).
- *Message integrity*, or protection against tampering or substitution. One must know that the recipient's copy of the message is the same as what was sent.
- *Nonrepudiation*, or protection against later denial of a transaction. This is clearly necessary for electronic commerce, for such things as digital receipts and payments.

Note: Law does not claim these four properties are "sufficient", so it is left to the reader to decide if additional properties are required.

What additional security property would be important in an electronic payment system? (Hint: analyse Law's properties in terms of Pfleeger's three security goals.) For full credit, your answer must name, briefly explain, and argue the importance of *one* security property that is not in Law's list. [10 marks]

5. Consider the following method for collecting evidence from the computer of someone who is suspected of a serious crime that may have been committed using this computer:

   - If the suspect's computer is running, shut it down by "switching it off at the power plug" (if there is a switch at the wall) or "pulling the plug" (otherwise).
   - Connect a portable ZIP drive to the suspect computer's printer port, disconnecting the suspect's printer if necessary.
   - Boot up the suspect's computer after reconnecting its power.
   - Back up the filesystem of the suspect's computer, using the standard archiving utility provided by ZIP. Carefully label each disk in the resulting ZIP archive with the suspect's name, your name, the current time of day, and the date.
   - Repeat the previous step, so that you have a second set of ZIP archive disks (for use in case the first set becomes unreadable, *e.g.* because of a catastrophic "click-of-death" failure on one of the ZIP cartridges).

   Briefly explain *two* defects in this procedure, which may result in the collection of data that is not "forensically sound". [15 marks]

6. Alireza *et al.* describe some of the principal features of CORBAsec, including its access control mechanism. Here is a rough summary of this mechanism, as it might be applied in a client-server database system. When two ORBs communicate using the IIOP (Internet Inter-ORB Protocol), the ORB representing a database server would use the CORBAsec "security service" to decide whether to allow the prospective client to access this database server. The client software (possibly implemented in Java) would access the database server only through CORBA "call stubs".

   Alireza *et al.* critically and appreciatively assess the security features of CORBAsec in their article. Briefly describe *one* of their criticisms of the access control mechanism in CORBAsec, and indicate a "work-around" or improvement that takes advantage of *one* of the Java security mechanisms described in required readings for this class. [10 marks]

7. Girard and Lanet write "... smart card security is based on two assumptions: the JCRE [Java Card Runtime Environment] is correctly implemented and applets loaded onto the card have been previously checked." The procedure for checking applets is based on the "sign and seal" method described by Li Gong *et al.*

   a. Briefly describe an attack on a smart card that violates one (or both) of these assumptions. [10 marks]

   b. State, and briefly justify, an additional assumption that is necessary to assure security of a smart card. [5 marks]

8. In 1998, Bean *et al.* identified a number of vulnerabilities in Java, as it was implemented in early versions. In particular, they noted the following two attacks:

   - A degradation-of-service attack, in which a hostile applet consumes large amounts of memory and CPU cycles;

   - An attack on privacy, in which a hostile applet exploits implementation errors to gain unauthorized access to "system properties" such as the user's login name, and to communicate this information to the webserver from which the hostile applet was downloaded.

   Briefly discuss the likelihood of controlling such attacks on a Java browser that implements any *one* of the "extensible security architectures" (capabilities, extended stack introspection, and name space management) defined in the paper you read by Wallach *et al.* For full credit, your answer should discuss only *one* extensible security architecture, and *both* of the attacks listed above. [15 marks]
