THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2008
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.**

This is an ungraded sample exam, which should take you about 25 minutes to complete.

A. Gurpreet Dhillon, in "Designing Information Systems Security…", is highly critical of the methodology that was used when specifying and designing an information system for a hospital. In the closing section of this article, Dhillon considers each of the primary modules of the hospital system in turn, noting how its *reference* (the system's actions, resulting from its actual use by its end-users) differs from its *usage* (the actions specified for the system).

Dhillon reports that the hospital's "Manage Pharmacy" module has the *usage* of transforming the maintenance of pharmacy records from a manual, paper-based procedure into a computer-based operation. The *reference* of this module is that it "Falls short of fulfilling the basic objective of pharmacy costing and drug utilization reviews." Security concerns may arise from any discrepancy between the usage and the reference. In the case of the Manage Pharmacy module, Dhillon concludes that there are "Threats of vulnerability to competitors and integrity problems of the pharmacy processes."

1. Critically and appreciatively discuss Dhillon's *reference/usage* analysis of a secure system, in the context of Lampson's assertion that "Studying a secure system involves three aspects: Specification/Policy … Implementation/Mechanism … [and] Correctness/Assurance."
(10 marks)

B. Hovav Shacham, in "… Return-into-libc without Function Calls (on the x86)", describes a vulnerability of the W⊕X defense. Shacham describes the W⊕X defense as an assurance that "no memory location in a process image is marked both writeable ("W") and executable ("X")." He notes that, in a system with this defense, "there is no location in memory into which the attacker can inject code to execute."

2. Discuss Shacham's attack, using terminology from COMPSCI 725. To receive full credit, you must indicate whether Shacham's attack is primarily on the Secrecy, Integrity, Availability, or Accountability goals of a secure system; and whether this attack can be used to compromise the other types of goals. You must discuss the defense (W⊕X) which this attack circumvents, indicating why it should be classified into one of the following categories: isolate, exclude, restrict, recover, and punish. Finally, you should consider defenses to Shacham's attack, in the context of your home PC, by indicating what you would do if you believed your PC would be the target of a Shacham-type attack. **(15 marks)**

C. (Other questions). **[75 marks]**