THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2013
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: 20 minutes)

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. Please do not put your name on your answer sheet.

A. As discussed recently in a lecture, Boaz Barak distinguishes systems with “well-defined security” from those that have “fuzzy security”. A system with fuzzy security is composed of “fuzzily specified components”. A system with well-defined security has “rigorously specified components”, and these components are accompanied by “security proofs [which] can be validated by anyone” that are based on “assumptions [which] can be checked for validity by anyone”.

1. Pick any article on the required-reading list for CompSci 725. Identify some secure system that is analysed or attacked in this article. Determine whether this analysis or attack is on a security property that is well-defined. Discuss briefly. To receive full marks, your answer must name (or very briefly describe) ***one*** **article**, ***one*** **secure system**, ***one*** **security analysis or attack**, and ***one*** **security property**, and it must explain **why** you consider this security property to be “fuzzy” or “well-defined”. ***[15 marks]***

B. A system with Mandatory Access Control (MAC) does not allow a user to delegate, to others, the access rights for resources owned by that user.

2. Describe the primary data structure used in a typical realisation of MAC, and explain how this data structure controls what each user can and cannot do. ***[5 marks]***

C. (Other questions). ***[80 marks]***