# THE UNIVERSITY OF AUCKLAND

**SECOND SEMESTER, 2009**
**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.** Wang et al., in "On the Security of Delegation in Access Control Systems", define dynamic enforcement as follows.

> In dynamic enforcement, the initial state γ of the access control system is recorded. For every workflow instance $X$, the system maintains a list $U_X$ of the participants for the instance. Every user who executed a step of $X$ is added to $U_X$. When a user $u$ requests to execute a step $s$, the system checks whether he/she needs to use a delegated privilege. If a delegated privilege $r$ should be used by $u$ to perform $s$, then both $u$ and the delegator of the privilege are added to $U_X$. Note that if $u$ has received $r$ from multiple delegators, $u$ has to specify the delegator of $r$ for the execution of $s$. At the end of the instance, the system checks whether the users in $U_X$ can complete the workflow in γ without delegation. If they can, then the execution of $X$ is confirmed. Otherwise the system gives warning that users in $U_X$ have enhanced their own power through delegation. The execution of $X$ is rejected.

**1.** Briefly describe a workflow $X$ which can be rejected (i.e. rolled back) safely. **(5 marks)**

**2.** Briefly describe a workflow $X$ which cannot be rejected safely. **(5 marks)**

**3.** Consider Lampson's "gold standard" for implementing security: authenticating principals, authorizing access, and auditing the guard's decisions. Which (if any) of these three mechanisms is implemented by dynamic enforcement, and which (if any) of these mechanisms are required by (but not provided by) dynamic enforcement? **(10 marks)**

**4.** Consider the Transactional Memory Introspection (TMI) architecture for reference monitors, as described in the article by Birgisson et al. Is the TMI architecture suitable for implementing dynamic enforcement? **(5 marks)**

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