COMPUTER SCIENCE TRIPOS Part II – 2013 – Paper 7

13 Security II (FMS)

(*a*) Formally state the two rules of the Bell-LaPadula (BLP) security policy model and then re-state them informally in terms of a single rule about the direction of information flow. [2 marks]

(*b*) Consider a distributed system in which A is a *TOP SECRET* process running on machine Alice and B is a *CONFIDENTIAL* object residing on machine Bob.

(*i*) Explain and justify whether A is allowed to read and/or write from B according to the BLP policy. [2 marks]

(*ii*) Discuss the claim made by some researchers that this scenario highlights a fundamental problem with the BLP policy. [4 marks]

(*c*) Consider the following description of Brewer and Nash's Chinese Wall security policy model.

- *Simple rule*: Read or write access to object o_2 by subject s is granted if and only if, for all objects o_1 to which s has had access, we have: (class(company(o_1)) $\neq$ class(company(o_2)) **or** (company(o_1) = company(o_2)).

- **-rule*: Write access to object o_2 by subject s is granted if and only if access is granted by the *simple rule* and there does not exist any unsanitized object o_1, readable by s, for which company(o_1) $\neq$ company(o_2).

(*i*) Explain the context and goal of the Chinese Wall security policy model. Then explain what each of the two rules is intended to enforce or prevent. [4 marks]

(*ii*) Some researchers have claimed that the formal rules of Chinese Wall do not match the policy that Brewer and Nash intended to enforce, to the extent that the resulting policy is unusable in practice. Explain precisely why the policy would be unusable and give a clear proof of this claim. [8 marks]