CIS 4360 Introduction to Computer Security – with answers

Home Assignment 7, Fall 2010

Due: Thu 12:30pm, 10/21/2010

This concerns Security models.

1. What does “tranquility” mean in the BLP model.
   Answer.
   The tranquility principle limits the applicability of BLP to systems where security levels do not change dynamically. It allows controlled copying from high security levels to low security levels via trusted subjects. More specifically, the tranquility principle of the BLP model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: “strong tranquility” for which the security levels do not change during the normal operation of the system; “weak tranquility” for which the security levels may never change in such a way as to violate a defined security policy (of BLP). Weak tranquility is desirable as it allows systems to observe the principle of least privilege. That is, processes start with a low clearance level regardless of their owner’s clearance, and progressively accumulate higher clearance levels as actions require it.

2. We get a covert channel in BLP between a low-level subject and a high-level subject in which the low-level subject creates an object, dummy.obj, at its own level. Explain this channel in more detail. What does the accomplice do? Who sends and who receives information?
   Answer.
   The high-level subject may classify the object dummy.obj, thus making it inaccessible to the low-level subject: thus one bit of information has been transferred downwards (an illegal information flow in BLP). Such actions can be repeated thus establishing a covert channel that copies the contents of higher level object to low-level objects.

3. The Biba model can capture a variety of integrity policies. Give examples for application areas where
   a policy with static integrity labels is appropriate.
   Answer.
   There are not many good answers, which is one of the drawbacks of Biba. A policy with static integrity labels could be used in a software engineering process where code that has been released by developers to testers should no longer be changed by developers.
   b. A policy with dynamically changing integrity labels is appropriate.
   Answer.
   Dynamic integrity labels can also be used with software engineering code, allowing for some interaction between developers and testers, even though this may be a dangerous practice.
   c. The ring-property is appropriate.
   Answer.
   The ring-property corresponds to the protection ring policies implemented on the Intel x86 architecture.

4. Can you use Bell-LaPadula and Biba to model confidentiality and integrity simultaneously? In particular can you use the same security labels for both policies?
   Answer.
   The answer is no, unless you want a very inflexible model. If you use the same lattice, then you have total isolation between security levels, which is hardly desirable. If you want to use BLP and Biba simultaneously, then you are better off with separate labels for confidentiality and integrity.

5. Can you fit the Chinese Wall Model into the Bell-LaPadula framework? Discuss.
   Answer.
   The answer is no. There is work in the literature that does just that, but if one accepts tranquillity as a central feature of BLP, then the Chinese Wall model with its dynamically changing access rights does not fit.