Class Exercise: Lipner Integrity Matrix Scenario

CS461/ECE422 Fall 2010

Overview

Recall that Lipner identified the following requirements for high integrity systems.

1. Users will not write their own programs, but will use existing production programs and databases.
2. Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
3. A special process must be followed to install a program from the development system onto the production system.
4. The special process in requirement 3 must be controlled and audited.
5. The managers and auditors must have access to both the system state and the system logs that are generated.

Consider a high integrity “enterprise” or “commercial” environment. Lipner considered the following sets of subjects.

- Ordinary users
- Application developers
- System programmers
- System managers and auditors
- System controllers

Lipner considered the following sets of objects.

- Development code and test data
- Production code
- Production data
- Software tools, e.g. compilers
- System programs
- System programs in modification
- System and application logs

Tasks

Your group is tasked with reasoning through sets of Bell-LaPadula (BLP) security labels and strict Biba integrity labels for these subjects and objects (or for similar sets of subjects and objects and match your interpretation of a commercial environment). You might try first identifying a BLP or Biba only solution and then adding in the other labels (assuming you thing that the solution using only confidentiality or integrity labels is insufficient).

The text discusses Lipner's solution to this scenario, but there are no doubt many ways to meet the requirements given the security and integrity labels. I would like you to discuss the assignments from first principles. The standards and assumptions in an commercial environment today no doubt differ somewhat from the time of Lipner's work.

For each label , you should be able to walk through the 5 integrity requirements and argue how your label assignments are sufficient.

After class, one person from each group should post on the class newsgroup a summary of your label assignments and identify how the meet the integrity requirements, or where your assignments fall short.