Outline for February 5, 2003

Reading: text, §5.2.2, 5.3, 6.1–6.2

Discussion Problem

We discussed the Bell-LaPadula Model, and noted that subjects could read and write objects only if the subjects were in the same compartment as objects. This leads to a notion of confinement, and raises the issue of leaking information among compartments. Such leakage led one security expert to speculate that, as the need for secure computing continued to climb, people would gradually shift from multi-user computing systems to single-user computer systems, because then information could not leak among compartments (as there are no other processes on the system to leak information to).

1. How do single-user systems connected by a network (such as the Internet) differ from multi-user systems?
2. Do you agree or disagree with the expert?

Outline for the Day

1. DG/UX B2 UNIX System
   a. Hierarchy of levels
   b. Labels, explicit and implicit
   c. MAC tuples
2. Tranquility
   a. Strong tranquility
   b. Weak tranquility
3. Integrity models
   a. Requirements
      i. Users won't write their own programs, but will use existing programs, databases, etc.
      ii. Programmers develop and test programs on non-production systems
      iii. Installing a program from the development system requires a special process
      iv. This process must be controlled and auditable
      v. System managers must be able to access the system state and the system logs
   b. Separation of duty
   c. Separation of function
   d. Auditing
4. Biba: mathematical dual of BLP
   a. P may read O if $L(P) \le L(O)$ and $C(P) \subseteq C(O)$
   b. P may write O if $L(O) \le L(P)$ and $C(O) \subseteq C(P)$
   c. Combined with BLP: continue example