CS590U: Access Control: Theory and Practice Spring 2005

Assignment #2 Due: Thursday, Jan 27, 2005.

1. Do the exercises in the handout on partial order and lattices. There are six of them.
2. Exercise 3.7 in Gollmann's Book
3. Exercise 3.8 in Gollmann's Book

The following problem should be answered after the lecture on Tuesday Jan 25.

4. On Page 20 of Bell and LaPadula's "Secure Computer System: Unified Exposition and MULTICS Interpretation", the authors say

   > We say that the basic security theorem establishes the "inductive nature" of security in that it shows that the preservation of security from one state to the next guarantees total system security.
   >
   > The importance of this result should not be underestimated. Other problems of seemingly comparable difficulty are not of an inductive nature. The problems of data- and resource-sharing, for example, are not inductive. In fact, the most trivial example of deadlock (Figure 5) can arise in any nontrivial sharing system that decides immediately to grant or deny a request for access. Resolution of this problem requires knowledge of future possibilities, queues of requests, and process priorities [18]. The result, therefore, that security (as defined in the model) is inductive establishes the relative simplicity of maintaining security: the minimum check that the proposed new state is "secure" is both necessary and sufficient for full maintenance of security.

   On the other hand, we argue in class that the basic security theorem is purely an artifact of defining a secure system to be one in which every state satisfies a certain property. There is nothing inherently important or insightful about the theorem, as it is true by definition.

   How do you reconcile the above two views? In particular, would you accept Bell and LaPadula's comparisons of the deadlock problem in resource sharing with the security problem as defined in their model? Why or why not?

The following problem is optional. There is no extra credit for it. Do it only if you are interested. May be submitted together with Proposal (on Feb 3).

5. Read John McLean's paper "Reasoning about security models", which criticizes the Bell-LaPadula model, and Bell's response "Concerning 'Modeling' of Computer Security", and describe your take on their debate.