

CMPSCI 177 - Computer Security
Fall 2009

Seventh Homework - The Lattice Model and the Noninterference Model

Due: 30 NOV 09 2:00pm

Part I: Lattice Model

Please answer question #1 in Bishop's Chapter 27.

Suppose that you are hired as the Security Officer for company Foobar International, which never had a security officer before. To try and determine what the existing undocumented security policy is you interview the supervisors in each of the areas of the company to determine what the allowable interdepartmental information flows are. The results of your interviews yield the following allowable information flows between the departments labeled A through K. (A to C), (B to A), (C to D), (C to G), (D to B), (D to F), (E to F), (E to G), (F to H), (F to I), (G to J), (H to K), (I to K)

2. Give a graphical representation of the information flow policy, where an arrow from node A to node B indicates that information is allowed to flow from Department A to Department B.
3. Give all the reasons why this graph is not a lattice?
4. Convert the graph to a lattice.

Part II: Noninterference Model

1. Let U, S, TS be (disjoint) sets of users with Unclassified, Secret, and Top Secret clearances, respectively. Let C be the set of all available commands.

Give the necessary noninterference rules for the *multilevel security* policy.

2. For the multilevel example of question 1 instead of assuming that U,S,TS are disjoint, assume that they have one user in common called Admin. Also assume that Admin is the only user common to any two of the user sets. Because Admin is trusted to do the right thing he/she is allowed to interfere using any of the commands.

Give the necessary noninterference rules for this *multilevel security* policy with a trusted user called Admin.

3. Again for the multilevel example of question 1 assume that users in a subset T1 of TS can send messages to users with a lower clearance using a special set of commands called Msg, but they can have no other effect on these lower level users.

Let $T' = TS - T1$ and $C' = C - \text{Msg}$, and give the necessary noninterference rules to express this modified policy