

CSCI 283 and CSCI 172- Graduate and Undergraduate Cryptography - Spring 2008
George Washington University

Homework 2 Solutions

1. A. To show that a system is secure, assume it starts in a secure state and show it ends in a secure state.

a. (2 points)

Trivially true. Suppose the system starts in any secure state, i.e. any state in V . It will always end in a state in V , which represents all the states of the system. Hence the end state is also secure. Hence the system is secure.

b. (4 points)

Suppose the system starts in any secure state, i.e. any state in V_1 . As there is no edge from any state in V_1 to a state in V_2 , the system cannot end in a state in V_2 . Further, all states belong to $V - 1$ or V_2 , hence it only ends in states in V_1 . Hence it ends in a secure state. Hence it is secure.

c. (1 point)

Similar to above, with V_1 and V_2 swapped.

B.

d. (6 points)

Assume the system starts in a state x in V_1' . As x is a vertex in V_1 , there is a path from x to v . Hence the system can end in $v \in V_2'$, an insecure state. Hence the system is insecure. The system cannot end in any other insecure state, i.e. in any other vertex of V_2' , as all other vertices of V_2' are in V_2 and hence there is no path from x to this other vertex. Hence the system can end up in exactly one insecure state, v .

e. (4 points)

Assume the system starts in a state v . As $v \in V_2'$, it is secure. Consider any insecure state, i.e. any $x \in V_1'$, i.e. any $x \in V_1$ such that $x \neq v$. There is a path from v to x . Hence the system can end in $x \in V_1'$, an insecure state. Hence the system is insecure.

Suppose the system starts in any other secure state, i.e. in $y \in V_2'$, such that $y \neq v$. Then $y \in V_2$. Hence there is no path from y to V_1 , and hence from y to V_1' , which is a proper subset of V_1 . Hence there is no path from y to an insecure state. Hence the system can end up in a non-secure state only when it starts in a particular secure state, v .

f. (3 points)

Given V and E , define a maximal set of secure states $V' \subseteq V$ as a set of states such that (a) the given system is secure with respect to it, and additionally, (b) when any vertex v not in V' is added to V' , the system is insecure. Show that V_2 is a maximal set of secure states. You may use any of the results derived above.

We have shown in part A(c) above that if V_2 is defined as the set of secure states, and its complement,

V_1 as the set of insecure states, the system is secure. Further, in B(e) we show that, if a vertex from its complement is added to V_2 , the system is not secure. Hence V_2 is a maximal set of secure states. If, on the other hand, there were a vertex z in the complement of V_2 , say a vertex $z \in V_1$ such that there was no edge from this vertex to any other (in V_1 or V_2), its addition to V_2 would not result in an insecure system and V_2 would not be maximal.

2. Suppose $o(X)$ is one of TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), PUBLIC

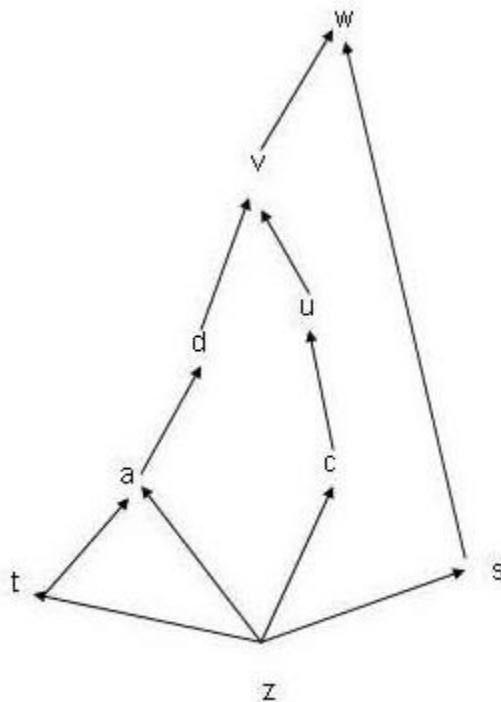


Figure 1:

(P); and $TS > S > C > P$. Suppose further that the compartments in the database are: Tests, Solutions, Grades, Slides. Figure 1 shows the domination relationships among the various nodes, for example, v dominates u . The arrows are directions of allowed information flow in the Bell-La Padula model. Let $(o(x), U(X))$ be the pair denoting the position of X in the access hierarchy, where $U \subset \{Tests, Solutions, Grades, Slides\}$. Answer the following (1 point each)

a. Suppose z is $(P, \{Slides\})$.

i. Can u access data from the compartment Slides that is classified P?

Yes.

ii. Can a be prevented from accessing data from the compartment Slides that is classified P?

No.

iii. Can a be prevented from accessing data from the compartment Slides that is classified C?

Yes

b. Suppose further that u is (P, {Slides}).

iv. Can c be classified (P, {Slides})?

Yes

v. Can c be classified (P, {Slides, Tests})?

No.

vi. Suppose further still that d is classified (TS, {Tests, Slides}). What is the minimum classification of v?

(TS, {Slides, Tests}).

c. Suppose s is classified (P, {Slides}).

vii. Ignoring the previous given values of u and d, and taking into consideration only the value of z, are all the possible domination relationships shown in the graph?

No.

viii. If not, what three other edges representing these relationships would provide all the required information in graphical form?

viii. Directed edges from: s to t, s to c, and s to z.

d. Assuming (a), (b), (vi) and (c), i.e. the given values for z, u, d and s

ix. Redraw the graph so that vertices with the same pairs are collapsed into one node bearing the names of all the vertices corresponding to it.

(See below)

x. Provide one possible pair of o and compartments for each of the vertices on the new graph.

See Figure. (Vertices in bold have to be exactly so. For the others, many solutions are possible).

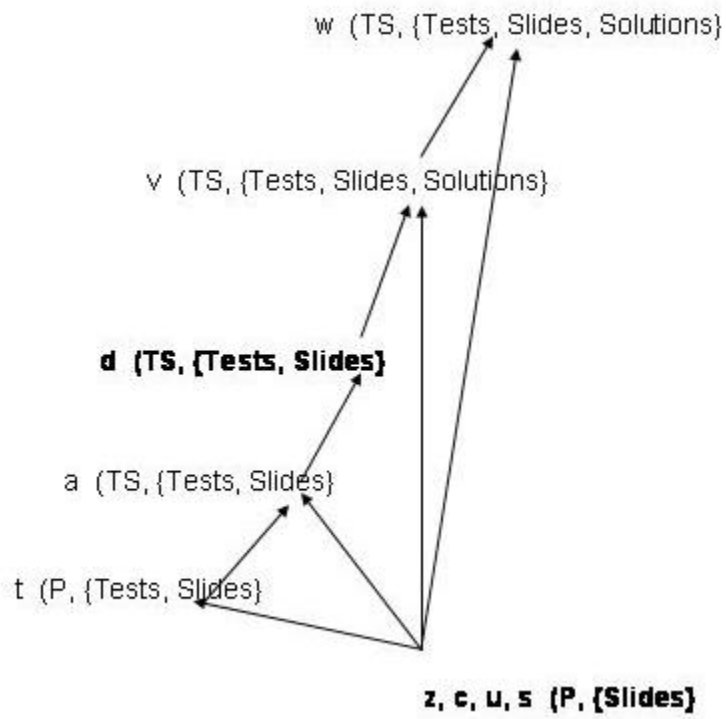


Figure 2: Solution