

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

**Homework 2: 30 points**

due 7 November

**Policy on collaboration:** All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the test and final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

*Any violations will be treated as violations of the Code of Academic Integrity.*

**PLEASE submit all HW on Blackboard only. Name your files:**

**CS283\_HW1\_LASTNAME\_FIRSTNAME.doc or .pdf or**

**CS172\_HW1\_LASTNAME\_FIRSTNAME.doc or .pdf**

1. (For this problem, you will need your background in undergraduate discrete math). Consider a graph with vertices  $V$  and edges  $E$ , where  $(v_i, v_j) \in E \Leftrightarrow v_i, v_j \in V$  and there is an edge from  $v_i$  to  $v_j$ .  $(v_i, v_i)$  is not in  $E$ . Suppose these vertices represent states of the system. Suppose an edge represents a possible transition, i.e. if there is no edge from  $v_i$  to  $v_j$ , the system cannot directly transition from  $v_i$  to  $v_j$  (it could, however, do so along a path through other vertices). The graph would be like the one shown in class, or like the one in the text, pg. 96, chapter 4.

A. Show that if  $V = V_1 \cup V_2$ , where  $V_1 \cap V_2 = \emptyset$ , and there is no edge from any vertex of  $V_1$  to any vertex of  $V_2$  and vice versa, the following are true:

- a. (2 points) If  $V$  is the set of secure states, the system is secure.
- b. (4 points) If  $V_1$  is the set of secure states, and  $V_2$  the set of non-secure states, the system is secure.
- c. (1 point) If  $V_2$  is the set of secure states, and  $V_1$  the set of non-secure states, the system is secure.

B. In addition to the assumptions of A, suppose that, given any  $v_i, v_j \in V_1$ , there is a path from  $v_i$  to  $v_j$ . Show that the following are true:

d. (6 points) If the set of secure states is  $V'_1 = V_1 \setminus \{v\}$  for any  $v \in V_1$ , and the set of non-secure states is  $V'_2 = V_2 \cup \{v\}$ , the system is insecure. In particular, show that it can end up in a non-secure state for any secure state it might start in.

e. (4 points) If the set of secure states is  $V'_2 = V_2 \cup \{v\}$  for any  $v \in V_1$ , and the set of non-secure states is  $V'_1 = V_1 \setminus \{v\}$ , the system is insecure. In particular, show that it can end up in a non-secure state only when it starts in a particular secure state. What state is that?

f. (3 points) Given  $V$  and  $E$ , suppose a maximal set of secure states  $V' \subseteq V$  is 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.

2. Suppose  $o(X)$  is one of TOP SECRET (TS), SECRET (S), CONFIDENTIAL (C), PUBLIC (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?
  - ii. Can  $a$  be prevented from accessing data from the compartment Slides that is classified P?
  - iii. Can  $a$  be prevented from accessing data from the compartment Slides that is classified C?
- b. Suppose further that  $u$  is  $(P, \{Slides\})$ .
  - iv. Can  $c$  be classified  $(P, \{Slides\})$ ?
  - v. Can  $c$  be classified  $(P, \{Slides, Tests\})$ ?
  - vi. Suppose further still that  $d$  is classified  $(TS, \{Tests, Slides\})$ . What is the minimum classification

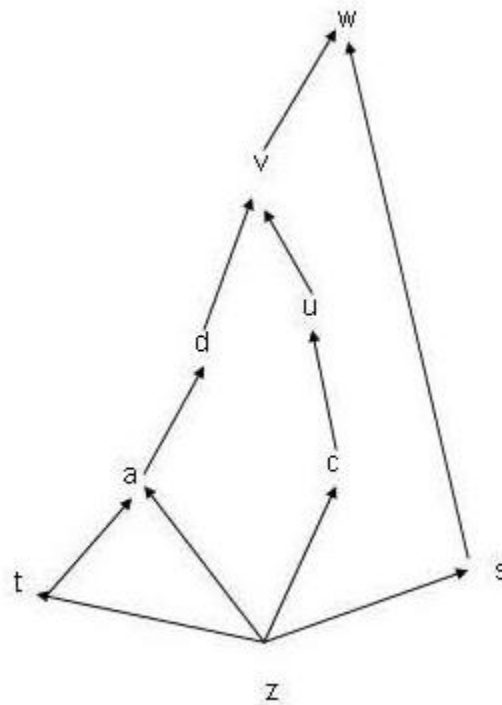


Figure 1:

of  $v$ ?

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

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?

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

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.

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