IS2510/TEL2810 Introduction to Security

Homework 2

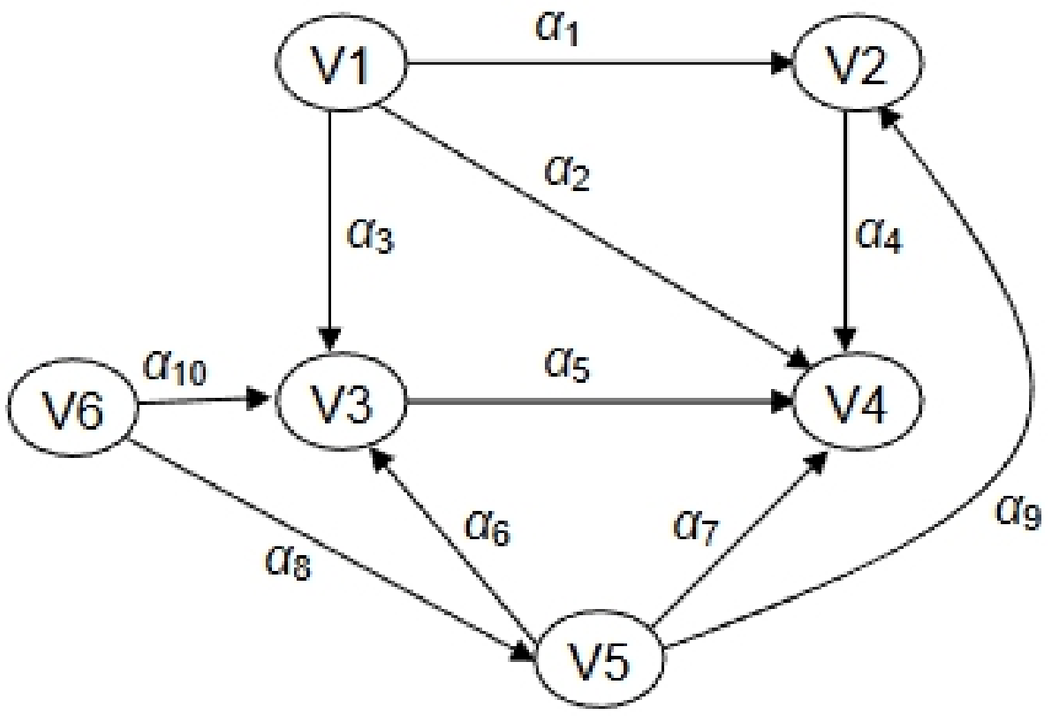
Total Points: 100

Due Date: Oct 14, 2011

1. **[20 Points]**
   The proof of Theorem 3–1 states the following: Suppose two subjects s_1 and s_2 are created and the rights in $A[s_1, o_1]$ and $A[s_2, o_2]$ are tested. The same test for $A[s_1, o_1]$ and $A[s_1, o_2] = A[s_1, o_2] \cup A[s_2, o_2]$ will produce the same result. Justify this statement. Would it be true if one could test for the absence of rights as well as for the presence of rights?

2. **[15 + 15 + 10 = 40 Points]**

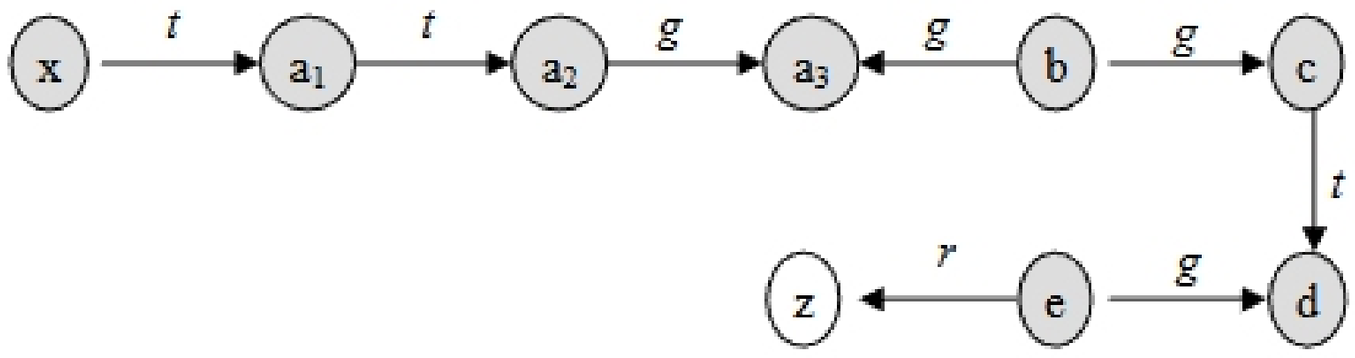
   (a) Reconstruct the following graph using the graph reconstruction technique used in the proof of theorem 3-11. Show transformed graphs for each of the three steps and label edges appropriately.



   (b) Consider the graph below which is a modified version of the graph of Figure 3-4 in the book (Brown one). For each graph, compute the following

   1. *Access set*,
   2. *Delete set*,
   3. *Conspiracy graph*,
   4. *Conspirators set* and
   5. *Witness*

   to the theft of right r by x and a_1. If the stealing is not possible, give reasons.



(c) Prove or disprove: The claim of Lemma 3–1 (related to the Take Grant model) holds when x is an object.

3. **[20 Points]**
Consider a Turing Machine with the following specification

1. Set of states: $\{k_0, k_1, k_2, k_3\}$
2. Tape symbols: $\{A, B, C\}$
3. Final (or halting) state is k_3
4. Transition Functions:

$\delta(k_0, A) = (k_1, B, R)$;

$\delta(k_1, A) = (k_2, B, R)$;

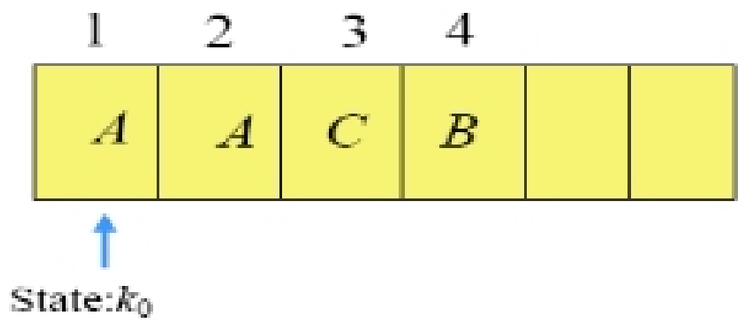
$\delta(k_1, B) = (k_1, A, R)$

$\delta(k_2, C) = (k_3, A, L)$;

$\delta(k_3, B) = (k_1, A, L)$;

Assume your TM's initial configuration is as shown below.

1. Show the mapping of the elements of this TM to a protection system.
2. Show all possible transitions, indicating each new TM configuration reached (i.e., state, head position and the symbols in each cell) and its corresponding protection state (the entries in the Access Control Matrix).



4. **[20 Points]**

(a) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

a. Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).

(b) In the DG/UX system, why is the virus prevention region below the user region and the administrative region above the user region? Explain clearly?

(c) Suppose a system implementing Biba's model used the same labels for integrity levels and categories as for security levels and categories. Under what conditions could one subject read an object? Write to an object?