

The most general construction of a MAC model is a reference monitor since it is program with a general purpose programming language. It is also undecidable.

The lattice based models have decidable properties, but because their security properties are enforced everywhere they are inflexible. However, the lattice models are extensible meaning that categories and compartments can be added after the system goes live without violating existing properties.

Type Enforcement is derived from the access matrix. The access matrix is of fixed sized, with domains as rows and types as columns. Each program is a member of a domain, and each object has a type. TE provides selective enforcement of security properties, and the construct of protections not possible with lattices such as assured pipelines.

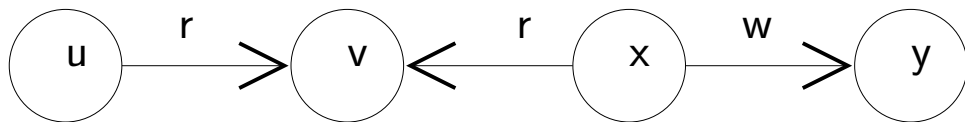
Role-Based Access Controls (RBAC) associate all permissions with roles, or groups. The hallmark of RBAC are their administrative controls which enable the modification of ordinary privileges. However, RBAC models used in practice and that support administrative controls are undecidable.

Finally, we describe Security Property Based Administrative Controls (SPBAC) in which security properties are selectively enforced. Administrative approval is needed only if the security properties in the current configuration are violated in the proposed change. SPBACs have decidable security properties. SPBACs are expressive, robust, and have decidable information flow security properties.

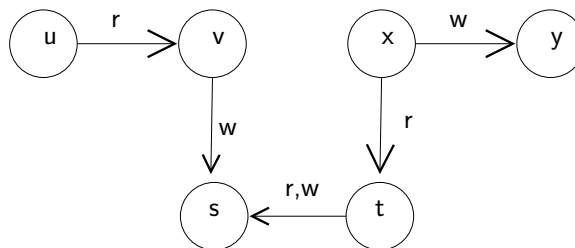
## 7.5 Exercises

1. Given a Reference Monitor, describe a situation in which the reference monitor would need to update:
  1. process descriptor
  2. object
2. **(Fall 2003)** In the Lampson's Access matrix, show what configurations enable:
  1. A permission to be copied to another domain.
  2. A permission to be removed from a domain.

3. In Lampson's Access matrix, describe all the ways that a permission can be removed from the access matrix for a given domain.
4. Capabilities. Consider a system in which the `init` process holds all the capabilities, and then passes them to processes that need them. Describe how the user processes gets the capabilities that the user can access.
5. List the differences between Lampson's and HRU's Access matrix. Do the HRU results apply to Lampson's Access matrix.
6. For the HRU Turing machine simulation, write the commands for left movement of the head over the tape.
7. **(Fall 2003)** Given the following Take-Grant configuration: can `u` `w` `y`? (Show the sequence of steps or explain why not).



8. Take-Grant. Can `u` `r` `y` in the following:



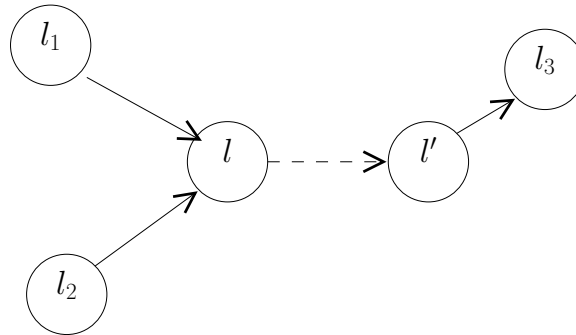
9. DAC Models.
  1. Is change of ownership a security issue? Explain.
  2. Describe a situation in which delegation of grant authority is useful.
10. **(Fall 2003)** Show how Type Enforcement can implement Bell-LaPadula without using any (explicit) lattice.

11. Type Enforcement.
  1. Show how to implement static separation of duty with Type Enforcement.
  2. Describe how TE can be used to update a user's password without super user privilege.
  3. Show how to allow only flows from  $a$  to  $b$ ,  $b$  to  $c$ , or  $b$  to  $d$ , where  $a, b, c, d$  are types.
12. Role-based access controls. Show an RBAC 96 configuration in which:
  - There are three different roles: High, Medium and Low.
  - High role has permissions  $r_h, r_l, w_l$  and  $w_h$ .
  - Medium rule has permissions  $r_h$  and  $r_l$ .
  - Low has  $r_l$  and  $w_l$  permissions.
  - Alice can take on the High role; Bob and Carol can take on the Medium role; and Carol and Darcy can take on the Low role.
13. (**Fall 2003**) Group management in SPBAC.
  1. Describe all the information to create a group set where all user are in exactly one of group A, B, or C.
  2. Describe all the information to create a group set with supervisors and workers, which are mutually exclusive and employees which contain both.
14. SPBAC groups. Design a group which has three classes of users: SeniorSysAdmins, JuniorSysAdmins, and Ordinary. New users are classified as Ordinary.

SeniorSysAdmins can relabel any user to any category. JuniorSysAdmins can relabel between JuniorSysAdmins and Ordinary.

In addition, what conditions are required so that there can be sufficient number of administrators.
15. SPBAC groups. Given the following group, is it possible for  $c$  to be non-empty? If so, describe the set of operation which makes its non-empty, if not, describe why not.

- $P_a = \{C\}, P_b = \{B\}, P_c = \{C\}$
  - $\text{Relabel}(A,B) = a, \text{Relabel}(B,C)=b$
  - new user rule: none
  - initial group labels:  $\langle u_0, A \rangle$
16. SPBAC groups. Given the following group, is it possible for  $c$  to be non-empty? If so, describe the set of operation which makes its non-empty, if not, describe why not.
- $P_a = \{C\}, P_b = \{B\}, P_c = \{C\}$
  - $\text{Relabel}(A,B) = a, \text{Relabel}(B,C)=a$
  - new user rule: none
  - initial group labels:  $\langle u_0, A \rangle$
17. SPBAC Groups. Show how two represent the RBAC healthcare hierarchy example in Figure 7.12 as an SPBAC group.
18. SPBAC. Show a group structure and associated permissions to implement Chinese Wall.
19. SPBAC information flow. Consider the following groups
- $P_a = \{A\}, P_b = \{B\}, P_c = \{C\}$
  - $\text{Relabel}(A,B) = a, \text{Relabel}(A,C) = a$
  - New User Tag:  $A$
- Let  $r(l) = a$  and  $w(l') = a$ . Then does creating  $\text{mayFlow}(l, l') = b$  create a can-flow path from  $l$  to  $l'$ ? Explain.
20. SPBAC information flow. What can-flow paths could be induced by the  $\text{mayFlow}(l, l')$  in the below diagram, assuming that the group membership does not prevent flows?



21. SPBAC information flow. Consider the definition of a  $mayFlow(l, l')$ . Can a can-flow path which does not include the subpath  $[l, l']$ .
22. SPBAC information flow. Give a configuration in which  $ac(l)$  approval is needed.
23. SPBAC information flow. Give a configuration in which  $ai(l)$  approval is needed.
24. DAC derived from SPBAC. A DAC label  $d$  derived from a MAC label  $m$  is written  $d/m$ . Assuming the permissions are read and write, what are the constraints on
  - $d$  to  $m$  information flow,
  - $m$  to  $d$  information flow, and
  - reading and writing  $d$ .
25. Approvability. Show a SPBAC configuration for approvability in which:
  1. An analyst creates a report
  2. It is approved by a manager and sent to the director or a manager request revisions and sends it back to the analyst
  3. The director either approves it or sends it back to the manager with requested revisions who must pass it to the analyst.

