

1. Revisit the example of one student copying another student's homework assignment. Describe three other ways the first student could copy the second student's homework assignment, even assuming that the file access control mechanisms are set to deny him permission to read the file.
2. A noted computer security expert has said that without integrity, no system can provide confidentiality.
  - a) Do you agree? Justify your answer.
  - b) Can a system provide integrity without confidentiality? Again, justify your answer.
3. Classify each of the following as an example of a mandatory or discretionary controlled policy, or a combination of thereof. Justify your answers.
  - a) The file access control mechanisms of the UNIX operating system.
  - b) A military facility in which only generals can enter a particular room.
  - c) A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.
4. 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 or both) 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}).
  - d) Sammi, cleared for (SECRET, {A,C}), wants to access a document classified (CONFIDENTIAL, {A}).
  - e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).
5. Give an example that demonstrates that the integrity level of subjects decreases in Biba's low-water-mark policy. Under what conditions will the integrity level remain unchanged?
6. Consider using mandatory access controls and compartments to implement an ORCON control. Assume that there are  $k$  different organizations. Organization  $i$  will produce  $n(i, j)$  documents to be shared with organization  $j$ .
  - a) How many compartments are needed to allow any organization to share a document with any other organization?
  - b) Now assume that organization  $i$  will need to share  $n_m(i, i_1, \dots, i_m)$  documents with organizations  $i_1, \dots, i_m$ . How many compartments will be needed?

7. Someone once observed that “the difference between roles and groups is that a user can shift into and out of roles, whereas that user has a group identity (or identities) that are fixed throughout the session.”
- a) Consider a system such as a Berkeley-based UNIX-system, in which users have secondary group identities that remain fixed during their login sessions. What are the advantages of roles with the same administrative functions as the groups?
  - b) Consider a system such as a System V-based UNIX system, in which a process can have exactly one group identity. To change groups, users must execute the *newgrp* command. Do these groups differ from roles? Why or why not?