Chapter 5 Problem 1, 2, 4,

* 1. Why is it meaningless to have compartments at the UNCLASSIFIED level (such as (UNCLASSIFIED, { NUC }) and ( UNCLASSIFIED, { EUR }))?
* 2. 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 }).
  + d. Sammi, cleared for (TOP 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 }).
* In the DG/UX system, why is the virus prevention region *below* the user region?

Chapter 14 problems: 2, 4

* 2. Alice can read and write to the file *A*, can read the file *B*, and can execute the file *C*. Bob can read *A*, can read and write to *B*, and cannot access *C*.
  + a. Write a set of access control lists for this situation. Which list is associated with which file?
  + b. Write a set of capability lists for this situation. With what is each list associated?
* 4. Explain why some UNIX-based systems with access control lists do not allow *root* to alter the ACL. What problems might this raise?

Other questions (not from the textbook)

1. “traditional” Linux access control uses abbreviations of access control that is specified by 9 letters (e.g., rwxrwxrwx gives full access). What are the letters and what do they mean?
2. What is the difference between mandatory and discretionary access control?
3. Given an example of where mandatory access control could be used and an example where discretionary access control could be used.
4. What is role-based access control? How is it different from access control based on access control lists?
5. Answer the questions on slide 19 of the power point slides for chapter 14, specifically, answer true or false and if false, explain why. Details are on slide 19. Also see the video at <http://www.eecis.udel.edu/~bohacek/IntroToCybersecurityVideos/RoleBasedAccessControl/RoleBasedAccessControl.html>
   * 1. Canexec(Ivan, code set A) = true/false ?
     2. Canexec(Sam, status project A) = true/false ?
     3. Canexec(Lisa, code set A) = true/false ?
6. (for help see: <http://www.eecis.udel.edu/~bohacek/IntroToCybersecurityVideos/WindowsACLSearch/WindowsACLSearch.html>)

Consider the ordered detailed access control list below. Give the end results and the steps taken in deciding the following requests made to the operating system

* 1. Stephan is in Group A and Group B and seeks to write to the object
  2. Linda is in Group B and seeks to execute the object
  3. Joe is in Group A and seeks to read the object
  4. Chris is in Group C and seeks to read the object

DACL

* Access denied
* Stephan
* Read, write, execute

ACE 1

* Access denied
* Group A
* Read, write, execute

ACE 2

* Access allowed
* Group B
* Write

ACE 3

* Access allowed
* everyone
* Read

ACE 4