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 }))?
    - If a compartment is UNCLASSIFIED, then anyone can have read and write access,, which adds no security layers and doesn't change access control.
- 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 }).
        - Paul can neither write nor read to this document.
    - b. Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
        - Anna can neither write nor read to this document.
    - c. Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
        - Jesse can read from this document but cannot write to this document.
    - d. Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
        - Sammi can read this document, but cannot write.
    - e. Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL,{ B }).
        - Robin can write but not read.
- In the DG/UX system, why is the virus prevention region *below* the user region?
    - This is a security mechanism which prohibits write downs. This allows user programs to read and execute programs in the virus prevention region, but not write.

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?
        - A ={(Alice : read/write),(Bob: read)}
        - B ={(Alice : read),(Bob: write)}
        - C ={(Alice : execute)}
    - b. Write a set of capability lists for this situation. With what is each list associated?
        - Alice capablilites:
            - A : read,write
            - B: read
            - C:execute

        - Alice = (A, read/write), (B, read), (C, execute)
    - Bob' capabilities
        - A:read;
        - B:read,write;
        - Bob = (A, read), (B, read/write), (C, -)

- 4. Explain why some UNIX-based systems with access control lists do not allow *root* to alter the ACL. What problems might this raise?
    - Some UNIX-based systems do not allow *root* to alter the ACL because if *root* is compromised then the exploiter can change the ACL, which compromises the security of the system. By changing the file permissions, for example, read only -> writable, important data may be lost. It is also possible that a *root* user changes file permissions by mistake, creating the same potential problem, but without any malice.

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?
    a. The letters stand for read, write and execute. There are 3 groups of rwx, each for user, group and world. The values of r, w and x are either 1 or 0, then each of the three groupings is translated to decimal notation. For example, lets say the 0d value is 700. The 7 corresponds to the user group, 7 in binary is 111, this means that r, w and x are all 1, so the user group can read, write and execute. The other two groups are 0 so they cannot read, write or execute.
2. What is the difference between mandatory and discretionary access control?
    a. In discretionary access control, the owner of an object controls the access rights of other users. In mandatory access control, the system specifies the access privileges.
3. Give an example of where mandatory access control could be used and an example where discretionary access control could be used.
    a. MAC would be used in a situation which requires high levels of security, with varying levels. For example, users are usually given a security clearance (secret, top secret, confidential, etc.) and data is given a security classification. When an access control decision is being made by the system, it checks the security clearance to the security classification. MAC would be used in the military or government.
    b. Most operating systems use DAC. This is most useful because a user can control what access privileges they can give to other users (rwx) for a file they created.
4. What is role-based access control? How is it different from access control based on access control lists?
    a. Role based access control restricts network access based on the roles of individuals in an enterprise. Essentially letting employees have access rights to only the information they

need to do their job, and excludes them from information which doesn't pertain to them. An employee's status in an organization determines the access rights that individual has. This ensures that lower-level employees can't access sensitive information or perform high-level tasks.

b. Permissions and privileges are assigned to each role, and users receive them via their role. The system will test the user for membership in a specific role, and grant or deny access. The acl allows a user or admin to define an ACL for a specific object.

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
    i. Canexec(Ivan, code set A) = true/false ?
        1. True
    ii. Canexec(Sam, status project A) = true/false ?
        1. True
    iii. Canexec(Lisa, code set A) = true/false ?
        1. False because Lisa is a tech lead in group B which only gives access to code set B, not A.
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

a. Stephan is in Group A and Group B and seeks to write to the object
    i. Go to ACE 1
    ii. See Access Denied (rwx) for Stephan
    iii. Thus Stephan's request is denied
b. Linda is in Group B and seeks to execute the object
    i. Go to ACE 1
    ii. No listing for Linda
    iii. Go to ACE 2
    iv. No listing for Linda
    v. Go to ACE 3
    vi. See listing for group B
    vii. Only gives permission to write, not execute
    viii. Thus Linda's request is denied.
c. Joe is in Group A and seeks to read the object
    i. Go to ACE 1
    ii. No listing for Joe
    iii. Go to ACE 2
    iv. See listing for Group A
    v. Access denied for rwx
    vi. Thus Joe's request is denied

d. Chris is in Group C and seeks to read the object
    i. Go to ACE 1
    ii. No listing for Chris
    iii. Go to ACE 2
    iv. No listing for Chris
    v. Go to ACE 3
    vi. No listing for Chris
    vii. Go to ACE 4
    viii. See listing allowing everyone to read
    ix. Thus Chris' request is approved.