Homework 2

Due: May 1, 2015 **Points:** 100

Questions

Remember to justify your answers.

1. (*16 points*) Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file *alicerc*, and Bob and Cyndy can read it. Cyndy can read and write thee file *bobrc*, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file *cyndyrc*, which she owns. Assume that the owner of each of these files can execute it.

   (a) Create the corresponding access control matrix.
   (b) Cyndy gives Alice permission to read *cyndyrc*, and Alice removes Bob's ability to read *alicerc*. Show the new access control matrix.

2. (*28 points*) The proof of Theorem 1 states that we can omit the **delete** and **destroy** commands as they do not affect the ability of a right to leak when no command can test for the absence of rights. Justify this statement. If such tests were allowed, would **delete** and **destroy** commands affect the ability of a right to leak?

3. (*16 points*) Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.

   (a) The file access control mechanisms of the UNIX operating system
   (b) A system in which no memorandum can be distributed without the creator's consent
   (c) A military facility in which only generals can enter a particular room
   (d) 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. (*20 points*) 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}).

5. (*20 points*) In the footnote on p. 29 of [War70], Ware writes: "we would discourage writing a [process] that on its own initiative reaches into another [process] for information without the knowledge of the second one. We would insist that some communication require that the first module ask information from the second, and that the exchange take place in an information-exchange area within neither."[1]

   (a) How does Ware's scheme satisfy the Principle of Least Common Mechanism? (As a historical note, Ware's report preceded Saltzer's and Schroeder's work by about 5 years.)
   (b) In the Linux operating system, this interprocess communication may occur using a set of pipes between the processes. Does the use of pipes meet Ware's insistence that the exchange (communication) take place in an area within neither process?

[1] Note that Ware uses the term "subroutine" where we would use the term "process".

Extra Credit

6. (*30 points*) Prove Theorem 3. (*Hint:* Use a diagonalization argument to test each system as the set of protection systems is enumerated. Whenever a protection system leaks a right, add it to the list of unsafe protection systems.)