Homework 2

Due: October 30, 2014 **Points:** 100

Questions

1. (*12 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.

2. (*16 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 }).

3. (*12 points*) Declassification effectively violates the *-property of the Bell-LaPadula Model. Would raising the classification of an object violate any properties of the model? Why or why not?

4. (*20 points*) Assume that the Clark-Wilson model is implemented on a computer system. Could a computer virus that scrambled constrained data items be introduced into the system? Why or why not? Specifically, if not, identify the precise control that would prevent the virus from being introduced, and explain why it would prevent the virus from being introduced; if yes, identify the specific control or controls that would allow the virus to be introduced and explain why they fail to keep it out.

5. (*40 points*) This problem asks you to implement a buffer overflow attack on a program. In the Homework area of Desire2Learn (or the Homework area of the nob.cs.ucdavis.edu class web site) is a program *bad.c*. This program contains a buffer overflow vulnerability; see the call to *gets*(3) at line 13. Your job is to exploit the overflow by providing input to the running process that will cause the program to invoke the function *trap* (which, you may notice, is not called anywhere else). You will know you've succeeded when you run the program, give it your input, and it prints "`Gotcha!`" Please do this on the CSIF systems. These run Fedora Linux, and are named "pc*nn*.cs.ucdavis.edu", where *nn* is an integer less than or equal to 60. You can see the status of the systems at `http://angel.cs.ucdavis.edu/cgi-bin/status.cgi?hostgroup=all&style=hostdetail`.

   The following questions will help guide you. Please turn in your answers to them, a hex dump of the input you use to call *trap*, and a typescript or screen shot of you running the program *bad*, giving it your input, and showing its output.
   (a) What is the address of the function *trap*()? How did you determine this?

(b) What is the address on the stack that your input must overwrite (please give both the address of the memory location(s), and their contents)? How did you locate this address?

(c) What is the address of *buf*?

(d) The *sled* is the input you give to alter the return address stored on the stack. What is the minimum length your sled must be?

Extra Credit

1. (*10 points*) How could Thompson's rigged compiler be detected?

2. (*20 points*) Develop a construction to show that a system implementing the Chinese Wall model can support the Bell-LaPadula Model.