Homework 2

Due: October 17, 2016 **Points:** 100

Questions

Remember to justify your answers where appropriate.

1. (*30 points*) The PostScript language [1] describes page layout for printers. Among its features is the ability to request that the interpreter execute commands on the host system.

   (a) Describe a danger that this feature presents when the language interpreter is running with administrative or root privileges.

   (b) Explain how the principle of least privilege could be used to ameliorate this danger.

2. (*20 points*) In *delete_queue* in the "Robust Programming" handout, the *free* statement is not protected by an *if* that checks to see whether *queues*[*cur*] is **NULL**. Is this a bug? If not, why don't we need to make the check? (Exercise 12 of the "Robust Programming" handout)

3. (*20 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. (*30 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 }).

Extra Credit

5. (*15 points*) Write a Ponder instance authorization to allow a professor to read an assignment submitted to a drop box between 7:00am and noon.

References

[1] Adobe Systems, Inc., *PostScript Language Reference*, Addison-Wesley Professional (Mar. 1999). ISBN 0201379228.