Homework 3

Due: November 6, 2023 **Points:** 100

1. (*10 points*) IAn X.509 certificate revocation list contains a field specifying when the next such list is expected to be issued. Why is that field present?

2. (*20 points*) The Web site *www.widget.com* requires users to supply a user name and a password. This information is encoded into a cookie and sent back to the browser. Whenever the user connects to the Web server, the cookie is sent. This means that the user need only supply a password at the beginning of the session. Whenever the server requests re-authentication, the client simply sends the cookie. The name of the cookie is "identif."

   (a) Assume that the password is kept in the clear in the cookie. What should the settings of the secure and expires fields be, and why?

   (b) Assume that the name and password are hashed and that the hash is stored in the cookie. What information must the server store to determine the user name associated with the cookie?

3. (*20 points*) Consider Multics procedures p and q. Procedure p is executing and needs to invoke procedure q. Procedure q's access bracket is (5, 6) and its call bracket is (6, 9). Assume that q's access control list gives p full (read, write, append, and execute) rights to q. In which ring(s) must p execute for the following to happen?

   (a) p can invoke q, but a ring-crossing fault occurs.

   (b) p can invoke q provided that a valid gate is used as an entry point.

   (c) p cannot invoke q.

   (d) p can invoke q without any ring-crossing fault occurring, but not necessarily through a valid gate.

4. (*20 points*) Suppose a user wishes to edit the file *xyzzy* in a capability-based system. How can he be sure that the editor cannot access any other file? Could this be done in an ACL-based system? If so, how? If not, why not?

5. (*14 points*) The Mysterious Mortgage Company announced it has upgraded the authentication required of its website users to two-factor authentication. Amy, a mortgagee, wants to log into her account on the web site. She enters her login name and password. Instead of showing her a screen with her account information, the next screen asked her to re-enter her login name and password. After she does so, she is then given the account page. Is this two-factor authentication? Why or why not?

6. (*16 points*) In the Janus system, when the framework disallows a system call, the error code **EINTR** (interrupted system call) is returned.

   (a) When some programs have read or write system calls terminated with this error, they retry the calls. What problems might this create?

   (b) Why did the developers of Janus not devise a new error code (say, **EJAN**) to indicate an unauthorized system call?