Assignment #4

Due: October 27

Problem 1 (30 pts) Access Control Mechanisms Please read the chapter on Access Control Mechanisms (chapter 14 or 15 depending on the version of the book)

a)Both ACLs and C-list entries use ”owners” (users) rather than individual processes. Why?

b) Alice can read and write to file x, can read to file y, and can execute the file z. Bob can read x, can read and write to y, and cannot execute z.

1. Write a set of access control lists for this situation. Which list is associated with which file?
2. Write a set of capability list for this situation. With what is each list associated?

c) Suppose a user wishes to edit a file xyzzy in a capability based. 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?

Problem 2 (15 pts) The Dribble Corporation authenticates users on their computers using a password. However, the computers are not accessible from outside their building, and gaining entrance to the building requires showing a company-issued picture identification badge to a guard.

a) For each of the following types of authentication describe how their system requires it (in one sentence or less), or state that it does not require it.

i) Entity knows something.

ii) Entity has something.

iii) Entity is something.

iv) Entity is someplace.

b) For the authentication method of requiring the picture on the badge to match the person holding the badge, describe the authentication method formally. I.e., what is the authentication information, complementary information, etc . . .

Problem 3 (15 pts) The Dribble Corporation’s website requires that its customers supply a user name and a password before shopping for widgets on their site. To make things easier for the user this information is encoded in a cookie and sent back to the browser. Whenever a user connects to the site, the cookie is automatically sent. This means the user needs to only supply a password when first visiting the site. Each page that is visited by the user, the browser automatically sends the cookie in response to the server’s request for authentication.

a) Assume the password is kept as ASCII text in the cookie. What should the settings of the secure and expires fields be, and why?

b) Assume the name and password are hashed using SHA-256 and the hash is stored in the cookie. What information must the server store to determine the user name associated with the cookie?

c) Is the cookie storing state or acting as an authentication token, or both? Explain.

Problem 4 (40 pts) The following protocol was devised by the Dribble Corporation to establish session keys between users. Trent is a trusted third part that shares keys with both Alice and Bob. Let $E_X(\cdot)$ be the encryption of $\cdot$ with the key X. All ciphers are symmetric, or shared key.

1	Alice	$\xrightarrow{A, B}$	Trent
2	Alice	$\xleftarrow{E_A(K, E_B(K, A))}$	Trent
3	Alice	$\xrightarrow{E_B(K, A)}$	Bob
4	Alice	$\xleftarrow{E_K(R_b)}$	Bob
5	Alice	$\xrightarrow{E_K(R_b - 1)}$	Bob

In step 2, Trent randomly creates a session key K that is computationally infeasible to brute force. Steps 4 and 5 are to establish that the session key is fresh and not a replay of another run of this same protocol.

a) Describe an attack on this system that would allow an attacker, Mallory, to read all messages between Alice and Bob. Assume that Mallory has full control over the communication channel. You can also assume that this protocol is run often, and that Mallory is someone that Alice and Bob might normally communicate with. Reference steps from the protocol to help describe the attack.

b) What simple change could be made to the above protocol to make it resistant to your attack?