Homework 3

Problem 1. (25 points)
Alice can read and write to the file F, can read the file G, and can execute the file H. Bob can read F, can read and write to G, and cannot access H.
(a. 13 points) Write a set of access control lists for this situation. Which list is associated with which file?
(b. 12 points) Write a set of capability lists for this situation. With what is each list associated?

Problem 2 (20 points)
Consider data that is input to a Web form. Such data is often transferred to the server by including it in a URL. Suppose the input is validated on the client. For example, suppose the following order has been checked by the client:
http://www.things.com/orders/final&custID=112&num=55&qty=20&price=10&shipping=5&total=205
This URL is interpreted to mean that the customer with ID number 112 has ordered 20 of item number 55, at a cost of $10 each, which, with $5 shipping, gives a total cost of $205.
Show three ways in which a client named Mallory can cheat the server.

Problem 3 (30 points).
Find and point the buffer overflow in the code below. Illustrate an attack using the stack image we covered in class. Show how the buffer overflow can be eliminated.

Algorithm 1 Code snippet of a vulnerable function.
1. ...
2. char buf[64], in[MAX_SIZE];
3. printf("Enter buffer contents : ");
4. read(0, in, MAX_SIZE - 1);
5. printf("Bytes to copy:");
6. scanf("%d", &bytes);
7. memcpy(buf, in, bytes);
8. ...

Problem 4 (25 points).
What will the following code print? Why? Identify the line where the vulnerability is. Explain the vulnerability. Show how the vulnerability can be eliminated.

Algorithm 2 Example vulnerability.
1. void called (int foo){
2. if (foo = 1) printf("foo");
3. else printf("bar");
4. }
5. int main(){
6. called(2);
7. return 0;}