Homework 4

Due Date: Tuesday, November 22, 2005 **Points**: 100

1. (*20 points*) Alice can read and write to the file *x*, can read the file *y*, and can execute the file *z*. Bob can read *x*, can read and write to *y*, and cannot access *z*.
   a. Write a set of access control lists for this situation. Which list is associated with which file?
   b. Write a set of capability lists for this situation. With what is each list associated?
2. (*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?
3. (*20 points*) An *intelligent bridge* is a type of firewall that analyzes messages passing through it. It associates with each network interface the names of hosts that lie on the network serviced by that interface. For example, consider a firewall with two network interfaces, the *inside* and the *outside*. Suppose host *treat* is on the inside network, and sending messages with host *candy*, on the outside network. After an exchange of messages between the two hosts, the firewall puts *treat* on the list for the inside network and *candy* on the list for the outside network.
   a. Why would the firewall track this information? That is, what types of attacks will this prevent? Please give an example.
   b. Now suppose a host is moved from one network to another. For example, suppose *candy* were moved to be on the same network as *treat*. What would the firewall do, and how would you arrange for the firewall to correct it?
4. (*20 points*) As stated in class, one of the goals of an election is to prevent people from being paid for votes, which requires them proving to the payor how they voted. But a voter would like to be able to verify that her vote was properly counted and, if it is not, complain to a county official and have the count corrected. To do this, the voter requires proof of her vote. Is it possible to enable a voter to do this and at the same time prevent people from being paid for votes? Why or why not?
5. (*20 points*) Consider how a system with capabilities as its access control mechanism could deal with Trojan horses.
   a. Consider the inheritance properties of new processes. These properties simply mean that if a user starts a process, the process is given some (or all) of the capabilities of its creator. If the creator controls which capabilities the created process is given initially, how could the creator limit the damage that a Trojan horse could do?
   b. Can capabilities protect against all Trojan horses? Either show that they can or describe a Trojan horse process that C-Lists cannot protect against.

Extra Credit

6. (*25 points*) How could Ken Thompson's rigged compiler be detected?