# CS414 SP 2007 Assignment 6

1. Which of these is an example capability system, and which is an ACL-based approach?
(a) You give your friend a key to your apartment
(b) A fancy club has a list of approved guests
(c) Some dorms at Cornell have card-swipe access, where the magnetic code on the card is matched against a list of residents
(d) Your car has a parking permit, listing where you're allowed to park.

2
(a) Discuss the strengths and weaknesses of implementing an access matrix using ACL that are associated with objects.
(b) Discuss the strengths and weaknesses of implementing an access matrix using capabilities that are associated with domains.

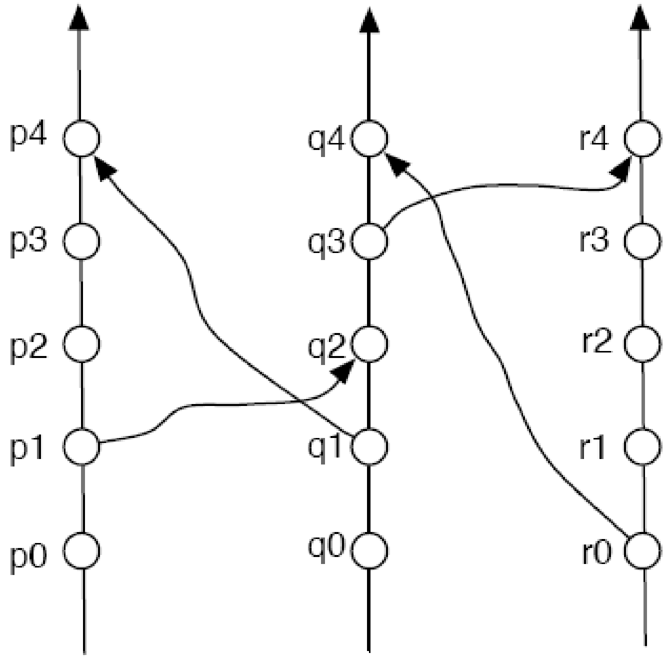
3. Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Discuss these solutions.

4. One mechanism for resisting replay attacks in password authentication is to use one-time passwords. A list of passwords is prepared, and once password[*N*] has been accepted, the server decrements *N* and prompts for password[*N-1*] next time. At *N*=0 a new list is needed. Outline a mechanism by which the users and the server need only remember one master password *mp* and have available locally a way to compute password[*N*] = *f* (*mp*, *N*). (Hint: make use of one-way hash functions)

5. In any distributed coordination problem, it is necessary to be able to determine the order in which two events occurred. In a distributed system it is sometimes impossible to say which of two events occurred first. The happened-before relation is used in obtaining a total ordering of events in a distributed system. The happened-before relation (denoted by ->) is defined as follows: first, if A and B are events in the same process, and A was executed before B, then A -> B. Second, if A is the event of sending a message by one process and B is the event of receiving that message by another process, then A -> B. Third, if A -> B and B -> C then A -> C .

(a) In a centralized system with a single core processor, it is always possible to determine the order in which two events occurred, but in a distributed system this is not always possible. Why?

(b) From the diagram below of relative time for three concurrent processes, what can you say about the relationship between q0 and p2? What can you say about the relationship between p0 and r4? (diagram attached)



6 Consider the following failure model for faulty processors. Processors follow the protocol but might fail at unexpected points in time. When processors fail, they simply stop functioning and do not continue to participate in the distributed system. Given such a failure model, design an algorithm for reaching agreement among a set of processors. Discuss the conditions under which agreement could be reached.