Paul Diaz
CS166 - Homework 7

1. 3. In this chapter we discussed access control lists (ACLs) and capabilities (aka C-list).
    a. **Two advantages of capabilities over access control lists (ACLs)include that it is easier to add and or delete user, and that it is easier to delegate (avoid the confused deputy).**
    b. **Two advantages of access control lists (ACLs) over capabilities include that it is easier to implement and easier to change rights to a resource**
2. 4. In the text, we argued that it's easy to delegate using capabilities.
    a. **Yes. In the textbook example (Alice, compiler, and a filename — where Alice tries to access and write something to the filename), in order to delegate using ACLs, Alice must oversee and record of what/who is acting on her behalf and use whatever permissions, this representative, in the appropriate ACLs, which specifies which entities are granted access to and what operations are allowed to use. In the textbook example, Alice invokes and uses the compiler to gain access to a file where she doesn't have access to — Alice confuses the compiler and act on her behalf.**
    b. **This scenario starts off by Alice delegating the permission of her capability list to the next person, which is Bill. Bill then does the same process to Charlie. In ACLs, the scenario gets complicated, but easier with capabilities because delegation of permission is easy in capabilities.**
    c. **Capabilities is better in delegation because it avoids the confused deputy.**
3. 10. This problem deals with covert channels.
    a. **In the textbook example, (Alice creates a file if she wants to send a message "1" to Bob, if she wants to send "0," no file exist if no message. Note that Bob cannot see the content of the file). A overt channel involving a print queue would be when we send a file in print queue and then deletes it. Print queue is used to signal information.**
    b. **Covert channel involving the TCP network protocol is TCP sequence number where the sender hides the information in the sequence number and the packet — with its source address forge to be the address of the intended recipient — is sent to an innocent server. When the server acknowledges the packet, it unwittingly completes the covert channel by passing the information contained in sequence number to the intended recipient.**
4. 11. We briefly discussed the following methods of inference control: query set size control; N-respondent, k% dominance rule; and randomization.
    a. **Three methods of inference control**
        i. **Query set size control - no response is returned if the size of the set is too small.**

ii. N-respondent, k% dominance rule - more refined form of query set size control where answer is not released if statistic of k% or more comes from N or fewer.

iii. Randomization - add small amount of random noise to data/reply.

b. Inference control methods: strengths and weakness

i. Strengths

1. **Query set size control - will have a difficulty to finding specific or precise information.**
2. **N-respondent, k% dominance rule - same as query set size control; this is due to the fact there would be no release if k% or more comes from N or fewer.**

ii. Weakness:

1. **Query set size control and N-respondent, k% dominance rule - attacks are possible.**
2. **if we want to have precise query answers, randomization would not be our be best choice because it adds random noise to the data.**