CS361 Questions: Week 3

These questions relate to Module(s) 3. Type your answers and submit them via turnin on Canvas by 5pm on Thursday, February 11, 2016.

Lecture 11:

1. Suppose you wanted to build a (library) system in which all subjects had read access to all files, but write access to none of them. What levels might you give to subjects and objects.

2. Why wouldn’t you usually build an access control matrix for a BLP system?

Lecture 12

1. Suppose you had hierarchical levels L, H with $L < H$, but only had one category A. Draw the lattice.

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?

3. Explain why upward flow in the lattice really is the metapolicy for BLP.

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 2 (flows only from L to H).

2. Argue that the READ and WRITE operations given satisfy BLP.

3. Argue that the CREATE and DESTROY operations given satisfy BLP.

4. What has to be true for the covert channel on slide 5 to work?

5. Why is the DESTROY statement there?

6. Are the contents of any files different in the two paths?

7. Why does SL do the same thing in both cases? Must it?

8. Why does SH do different things? Must it?

9. Justify the statement on slide 7 that begins: “If SL ever sees...”
Lecture 14

1. Explain why “two human users talking over coffee is not a covert channel.”

2. Is the following a covert channel? Why or why not?

```
Send 0 | Send 1
------------------------------------------
Write (SH, F0, 0) | Write (SH, F0, 1)
Read (SL, F0)    | Read (SL, F0)
```

3. Where does the bit of information transmitted “reside” in Covert Channel #1?

4. In Covert Channel #2?

5. In Covert Channel #3?

6. In Covert Channel #4?

7. Why might a termination channel have low bandwidth?

8. What would have to be true to implement a power channel?

9. For what sort of devices might power channels arise?

Lecture 15

1. Explain why covert channels, while appearing to have such a low bandwidth, can potentially be very serious threats.

2. Why would it be infeasible to eliminate every potential covert channel?

3. If detected, how could one respond appropriately to a covert channel?

4. Describe a scenario in which a covert storage channel exists.

5. Describe how this covert storage channel can be utilized by the sender and receiver.

Lecture 16

1. Why wouldn’t the “create” operation have an R in the SRMM for the “file existence” attribute?
2. Why does an R and M in the same row of an SRMM table indicate a potential channel?

3. If an R and M are in the same column of an SRMM table, does this also indicate a potential covert channel? Why or why not?

4. Why would anyone want to go through the trouble to create an SRMM table?