CS361 Questions: Week 1

These questions relate to Module(s) 1. Type your answers and submit them on Canvas.

Lecture 1

1. What uses of the term “security” are relevant to your everyday life?
2. What do these have in common?
3. Have you been a victim of lax security?
4. What is the likelihood that your laptop is infected? How did you decide?
5. What security measures do you employ on your laptop?
6. Do you think they are probably effective?
7. Consider the quote from the FBI official on slide 10. Do you think it overstates the case? Justify your answer.
8. What is the importance in learning about computer security?

Lecture 2

1. Consider the five reasons given why security is hard. Can you think of other factors?
2. Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not?
3. Explain the asymmetry between the defender and attacker in security.
4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?
5. Explain the statement on slide 8 that a tradeoff is typically required.

Lecture 3

1. Define “risk”?
2. Do you agree that software security is about managing risk?
3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?

4. Evaluate annualized loss expectancy as a risk management tool.

5. List some factors relevant to rational risk assessment.

**Lecture 4**

1. Explain the key distinction between the lists on slides 2 and 3.

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.

3. What does it mean “to group and categorize data”?

4. Why might authorizations change over time?

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related?

6. In what contexts would authentication and non-repudiation be considered important?

**Lecture 5**

1. Describe a possible metapolicy for a cell phone network? A military database?

2. Why do you need a policy if you have a metapolicy?

3. Give three possible rules within a policy concerning students’ academic records.


5. For the example given involving student SSNs, state the likely metapolicy.

6. Explain the statement: ”If you don’t understand the metapolicy, it becomes difficult to justify and evaluate the policy.”

**Lecture 6**

1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?
2. Describe the major threat in our MLS thought experiment.
3. Why do you think the proviso is there?
4. Explain the form of the labels we’re using.
5. Why do you suppose we’re not concerned with how the labels get there?
6. Rank the facts listed on slide 6 by sensitivity.
7. Invent labels for documents containing each of those facts.
8. Justify the rules for “mixed” documents.

Lecture 7

1. Document labels are stamped on the outside. How are “labels” affixed to humans?
2. Explain the difference in semantics of labels for documents and labels for humans.
3. In the context of computers what do you think are the analogues of documents? Of humans?
4. Explain why the Principle of Least Privilege makes sense.
5. For each of the pairs of labels on slide 6, explain why the answers in the third column do or do not make sense.

Lecture 8:

1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?
2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).
3. Show that dominates is not a total order.
4. What would have to be true for two labels to dominate each other?
5. State informally what the the Simple Security property says.
6. Explain why it’s “only if” and not “if and only if.”
Lecture 9

1. Why isn’t Simple Security enough to ensure confidentiality?

2. Why do we need constraints on write access?

3. What is it about computers, as opposed to human beings, that makes that particularly important?

4. State informally what the *-Property says.

5. What must be true for a subject to have both read and write access to an object?

6. How could we deal with the problem that the General (top secret) can’t send orders to the private (Unclassified)?

7. Isn’t it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.

Lecture 10:

1. Evaluate changing a subject’s level (up or down) in light of weak tranquility.

2. Why not just use strong tranquility all the time?

3. Explain why lowering the level of an object may be dangerous.

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.

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 could 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. (Use your keyboard and editor to draw it; it doesn’t have to be fancy.)

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 1.

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?

   \[
   \begin{array}{c|c}
   \text{Send 0} & \text{Send 1} \\
   \hline
   \text{Write (SH, F0, 0)} & \text{Write (SH, F0, 1)} \\
   \text{Read (SL, F0)} & \text{Read (SL, F0)} \\
   \end{array}
   \]

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?