CS361 Questions: Week 1

These questions relate to Module(s) 1. Type your answers and submit them via email to the TA by 5pm on Thursday, June 12.

Lecture 1

1. What uses of the term "security" are relevant to your everyday life?

   Personal security, network security, and system security

2. What do these have in common?

   They have to do mainly with securing my technology

3. Have you been a victim of lax security?

   Yes, my car has been broken into, and I've had my computer infected

4. What is the likelihood that your laptop is infected? How did you decide?

   I'd say the likelihood is high since malware is so prevalent

5. What security measures do you employ on your laptop?

   I don't download risky files

6. Do you think they are probably effective?

   I feel as though it's not 100% effective but that it eliminates most of the threats

7. Consider the quote from the FBI official on slide 10. Do you think it over-states the case? Justify your answer.

   I feel as though any system connected through the internet has the possibility of being compromised, so yes I feel the quote from the FBI official is justified

8. What is the importance in learning about computer security?

Because computers are becoming more prevelant, and cyber security threats could greatly affect anyone personally.

Lecture 2

1. Consider the five reasons given why security is hard. Can you think of other factors?

   It's very difficult to stop a malicious user who has worked on the same type of security system

2. Is there a systematic way to enumerate the "bad things" that might happen

I think there is but only to a certain extent. You could just take every function of program of try to find any way it could possibly be compromised.

3. Explain the asymmetry between the defender and attacker in security.

The defender has no idea what the attacker could do to thwart the system or what part of the system he even intends to compromise.

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?

They're saying that it's impossible to protect a computer from every possible threat because nobody knows every possible threat.
I agree, any possible way that the computer has to share or move information can be compromised in some way, and you'll never know all the ways it could be compromised beforehand.

5. Explain the statement on slide 8 that a tradeoff is typically required.

Too much security limits functionality because the more checks you have the slower the computer runs and it gives developers less freedom to use all aspects of the hardware and software.

Lecture 3

1. Define "risk"?

Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability

2. Do you agree that software security is about managing risk

Yes, because you have to decide where an attack is most likely to occur and focus on securing those areas first

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?

   A risk I accept is that I may get sick eating out, a risk I avoid is eating out at dirty places, a risk I mitigate is washing my hands when eating out to avoid getting sick, and a risk I transfer is having someone take care of me because I'm sick from eating out.

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

   It's a good tool because it not only shows how bad each risk is, but shows how likely it is to occur, so I think it's a good tool for managing risk.

4. List some factors relevant to rational risk assessment.

   The likelihood that a risk is to occur, the damage the risk would do if it were to occur, and the ALE for the risk, meaning the loss expectancy for the risk taking into account both the damage of the risk and the probability of it occuring

Lecture 4

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

   Slide 2 has a list of functionality you want your security system to have, slide 3 has ways of accomplishing that functionality.

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

   For me it's integrity and availability since I don't store a lot of sensitive information on it, this is because I don't want to lose any files and I want access to my files whenever I need them.

2. What does it mean "to group and categorize data"?

   It means to separate it into different groups based on the sensitivity of the information the data contains. That way only people with the proper authorizations can view the data

3. Why might authorizations change over time?

   People may gain more permissions or the data may be deemed not as sensitive as it used to be and moved to a lower level of confidentiality

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

   Because if someone tampers with the data in your database it could have just as catastrophic consequences as someone stealing your data.

important.

In cases like ordering something online, where the retailer needs to make sure it's actually you ordering a product and you need to make sure that the retailer actually received the money that you sent them

Lecture 5

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

   For a cellphone network you'd want nobody to be able to intercept the communication between the phones.

   For a military database you'd want only personnel with the proper authorization to access certain files and you don't want anybody from an outside network bypassing your firewall and changing either the integrity of your data or just stealing it.

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

   Because the policy is how you're going to accomplish the metapolicy

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

   Only registrars should be able to change them.
   Students, teachers, and registrars should be able to just view them though.
   Registrars' passwords should be regenerated every week

3. Could stakeholders' interest conflict in a policy? Give an example.

   Students wanting extremely quick access to their records may complain if the records are stored in a slower but encrypted database.

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

   Students' SSNs should not be revealed unless to a specified user

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

   Because you need to know your goals in order to justify why you're using each sort of security tool to accomplish them

Lecture 6

1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?

   Because the military has many secrets it doesn't want other countries knowing. There are also aspects of integrity and availability because you don't want a soldier Changing his discharge status or a general not being to access plans on the battlefield

CS361 Questions: Week 1

2. Describe the major threat in our MLS thought experiment.

   The confidentiality of information, the wrong person having access to it.

4. Why do you think the proviso is there?

Because integrity and availability add 2 whole dimensions of policy implementation

5. Explain the form of the labels we're using.

   There are several unordered categories of personnel, within those categories there are some ordered categories detailing different security levels

5. Why do you suppose we're not concerned with how the labels get there?

   Because they're just arbitrary names for certain security levels

6. Rank the facts listed on slide 6 by sensitivity.

   Beginning with most sensitive 2,6,1,5,4,3

6. Invent labels for documents containing each of those facts.

   RecSports, Payroll, MilitaryIntelligence, Cafeteria

7. Justify the rules for "mixed" documents.

   You should use the highest appropriate label

Lecture 7

1. Document labels are stamped on the outside. How are "labels" affixed to humans?

   By the amount of trust worthiness that they have

2. Explain the difference in semantics of labels for documents and labels for humans.

   Document labels indicate the sensitivity of the contained information and human labels indicate what classes of information that person is allowed to access

3. In the context of computers what do you think are the analogues of documents? Of humans?

   In computers it's files and in humans it's memories or knowledge in the brain

5. Explain why the Principle of Least Privilege makes sense.

   Because the more access everyone has the more possibilities there are that

third column do or do not make sense.

The first makes sense because he has the correct need to know category and a higher security clearance than even required, the second makes sense because although he has the correct need to know category he doesn't have a high enough security clearance

Lecture 8:

1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?

   Because now we're going to talk about confidentiality

2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).

   This works because if there are two labels describing levels of information sensitivity , if A dominates B, then B will never dominate A

3. Show that dominates is not a total order.

5. What would have to be true for two labels to dominate each other?

   They would have to be the exact same

6. State informally what the the Simple Security property says.

   If the label of the user dominates the label of the object then the system allows the user to take action on the object

6. Explain why it's "only if" and not "if and only if."

   Because the system must verify every time absolutely that the user has the proper Authorization to alter the object

Lecture 9

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

   It only covers read access not write access

2. Why do we need constraints on write access?

   To protect confidentiality

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

   Computer files can be changed and manipulated as opposed to a person's knowledge

3. State informally what the *-Property says.

   No read up no write down

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

   He must have the same label as the object

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

   He could change the permissions on the file

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

   It's an integrity problem that we haven't yet covered, but you could lock certain files after creating them

Lecture 10:

1. Evaluate changing a subject's level (up ordown) in light of weak tranquility.

   It could violate some sort of security rule

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

   Because sometime the sensitivity of information changes

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

   It could be used to give lower users access to unauthorized information

to be secure.

It must not violate the spirit of the security policy

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?

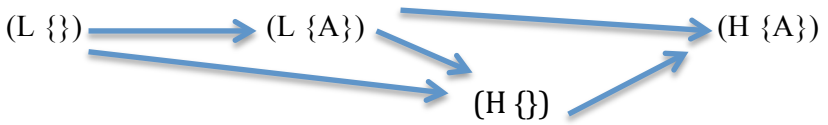
   The subjects would be (H {A, B, C}) and the objects would be (L {})

2. Why wouldn’tyou usually build an access controlmatrix for a BLP system?

   The matrix is implicit in the rules

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?

   Making a lattice

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

   Because you don't want to write down

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.

   This is because according to BLP information cant flow downward and according to the meta policy we don't want to read up or write down

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

Because once again they satisfy the premise that you aren't allowed to read up or write down, the write and read operations given allow you to write up and read down only

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

   They satisfy the BLP because create only makes something at the level of the user so it doesn't really contribute to the illegal flow of information, and DESTROY is ok because it still doesn't allow an upper level user to write downward in the hierarchy

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

   You have to have a feedback mechanism that changes depending on whether or not the high order object that you created exists

6. Why is the DESTROY statement there?

   To cover the tracks that the program was running

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

   No, just the level of user that they were created by

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

Yes because in one case it creates an object and this gives different feedback to SL Create

10. Justify the statement on slide 7 that begins: "If SL ever sees..."

    If SL ever has access to a mechanism that can see the change in an object that is created by SH, then that could be a threat by transmitting either a 1 or 0 depending on the error message

Lecture 14

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

   Because they wouldn't be utilizing system resources that were not designed to be used for inter-subject communication

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)     |

   Yes this is a covert storage channel. It's a covert channel
   because SL is reading from SH
```

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

   In the system state

4. In Covert Channel #2?

   In the system clock

4. In Covert Channel #3?

   It's a storage channel stored on the hard drive

6. In Covert Channel #4?

   In the control flow of the program

7. Why might a termination channel have low bandwidth?

   Because it's not sending data on something that happens very often

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

   You'd have to have access to the battery readings or a reader on the power supply of the computer

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

   Laptops and cell phones

Lecture 15

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

   They operate at thousands of bits per second

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

   There' no way of knowing all of them

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

   Modify the existing system implementation, reduce the bandwidth of the channel with noise, or monitor it for patterns of usage that indicate the exploit

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

   Two users have access to the same attribute that they can both read and that at least one can modify

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

   Both sender and receiver must have access to some attribute of a shared object, the sender must able to modify the attribute, the receiver must be able to reference (view) that attribute, and a mechanism for initiating both processes and sequencing their accesses to the shared resource must exist

Lecture 16

1. Why wouldn't the "create" operation have an R in the SRMM for the "file existence" attribute?

   Because it's not referencing anything looking up any information it's just modifying the current file structure by adding in a new file

2. Why does an R and M in the same row of an SRMM table indicate a potential channel?

   Because you can modify files and then read the changes

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?

   Yes because if you tried to create something and it gave you a warning if it wasn't created then you have a potential feedback mechanism for transmitting information

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

   To find covert channels