Tyler Kemme

UTEID: tpk266

CS ID: tpkemme

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 and network security are very relevant to my life. Personal security is obviously important because it involves the security of my personal items. A good example of personal security is the locks on my front door. Network security is important as well because I study web development and it is a key part of keeping your data and users safe.

2. What do these have in common?

   Both of these types of security involve the protection of materials/data that is important to me.

3. Have you been a victim of lax security?

   Considering how insecure email is, it is not surprising that I have been a victim to lax security through email. I have been “hacked” to the point where my email address would automatically send spam to every user in my contact list.

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

   It’s relatively easy for me to figure out when my laptop is infected. Considering most of the infections I get on my laptop are from the internet, I can usually detect much slower network speeds with infections like adware, spyware, malware, etc.

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

   I personally don’t use any anti-virus software because I have experienced exactly how useless they tend to be. I definitely employ a firewall but I also have multiple tools for removing infections after I have contacted them.

6. Do you think they are probably effective?

I think my measures are very effective. Because it is easy for me to detect infections, I only need to run the tools I have to remove them. I don't believe anti-virus software is effective in keeping your system secure and consequently, I don't use it.

7. Consider the quote from the FBI official on slide 10. Do you think it over-

states the case? Justify your answer.

The statement is slightly exaggerated, but the official is not incorrect. Many of the tools for hacking computer systems are already available online. All it takes is someone who chooses to use those tools incorrectly.

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

Computer security is incredibly important because computers are becoming an integral part to our daily lives. If these systems were not secure, we would constantly be at risk.

Lecture 2

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

Another reason that security is hard is because the more complex a security system is, the less likely it is that it will be used correctly/effectively. For instance, if it is hard for a user to remember a system-generated password, he/she might write it down on a piece of paper, making the complex password useless.

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

to a program? Why or why not?

There is really not a way to enumerate "bad things." Obviously a developer can consider all the cases of inappropriate input/user usage. However, hackers often discover vulnerabilities in systems that would never be found if not for a user looking for a malicious way to use the system.

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

Because it's almost impossible to predict where systems will be vulnerable, defenders almost always have to react to attacks. Many times, a vulnerability in a system will not be mitigated/corrected until after an attack has exploited it.

4. Examine the quotes from Morris and Chang. Do you agree? Why or why

not?

I do agree. Morris and Change are essentially explaining that vulnerabilities are inevitable as long as we continue to build imperfect systems. Considering a system can never be perfect, we should assume that perfect security is impossible.

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

A perfectly secure system implies a sacrifice to simplicity, functionality, usability, and efficiency. Because of this, developers need to find a balance between being secure and having a system that is not too complex for the user to use efficiently.

Lecture 3

1. Define "risk"?

   Risk is the probability that a vulnerability in a system will be exploited. So, there might be a very apparent vulnerability in a system, but it does not present a large risk because exploiting the vulnerability will cause very little damage to the system.
2. Do you agree that software security is about managing risk?

   Because we can assume that no software is totally secure, security is all about risk management. Software developers must take the time to decide how much risk a vulnerability presents to the system and make appropriate changes.

CS361 Questions: Week 1 2

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

one you transfer?

Risk accepted: I accept that driving to work puts me at risk for being killed in a car accident.

Risk avoided: I avoid selling illegal drugs because I understand that by not selling them, I'm avoiding the possibility of jail time for drug-related charges.

Risk mitigated: I have renters insurance so that in case my apartment does get robbed, the insurance company will help pay for my losses.

Risk transferred: I keep my money in a bank so that the task of keeping it secure lies with the bank.

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

   Annualized loss expectancy is useful as a risk management tool because it takes into account the amount of damage possible due to a vulnerability and the likeliness that the vulnerability will be exploited.

4. List some factors relevant to rational risk assessment.
   -the time needed to correct a vulnerability
   -cost of correcting a vulnerability
   -impact on the user of correcting a vulnerability
   -etc

Lecture 4

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

   The list on page 2 explains the goals of computer security. The list on page 3 details the tools used to achieve these goals.

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

Personally, availability is the most important to me when computing in my personal life. Because most of my personal data is not incredibly private or important to me, confidentiality and integrity are not as important as availability. However, if I'm trying to do a homework assignment through the internet, it is vital that the service is available to me so that I can finish my work in a timely fashion.

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

   Grouping/Categorizing data means that you go through your data and decided how sensitive it is. For instance, if the data contains credit card numbers, that data is likely to be more sensitive than a picture of someone's dog.

3. Why might authorizations change over time?

   Authorizations can change as users/employees change roles within an organization. Authorizations can also change when the underlying structure of a system changes and thus user roles change.

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

If a system is not at all secure, it is very likely that an attack can negatively affect the availability of a system. This makes the system unreliable.

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

Authentication and non-repudiation are important in the context of sending data through a network. The sender must prove he is who he says he is and if he sends a file to another user, he canot deny sending it later.

Lecture 5

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

Cell phone network: goals of a cell phone network include integrity, confidentiality, availability, and non-repudiation

Military database: goals for a military database include confidentiality, integrity, availability, authentication, and non-repudiation.

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

A metapolicy only outlines the general security goals you have for a system/network. The policy describes the actual mechanisms used to implement the metalpolicy.

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

records.

1. Student academic records should not be available to view by everyone
2. Students should be able to view their academic record at any time
3. Students should not be able to change their academic record at all.

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

   Stakeholders' interests can conflict because there are multiple groups of people with different interests at stake. Someone must decide what risks are more important to resolve.

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

   The metapolicy for this example is the achievement of confidentiality concerning student SSNs.

6. Explain the statement: "If you don't understand the metapolicy, it becomes

difficult to justify and evaluate the policy."

Basically, if you do not understand your general security goals for the system, you cannot implement tools to keep the system secure.

Lecture 6

1. Why is military security mainly about confidentiality? Are there also as-

pects of integrity and availability?

There are definitely aspects of integrity and availability in military security. However, since most of their data is a matter of national security, it is absolutely vital that their data is completely confidential.

CS361 Questions: Week 1 3

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

   The biggest threat in the MLS thought experiment is the threat to confidentiality.

4. Why do you think the proviso is there?

   The proviso is important because integrity and availability involve different policies to resolve.
5. Explain the form of the labels we're using.
   The labels used in the slides describe the sensitivity of the information found in various documents/folders/objects/files.
6. Why do you suppose we're not concerned with how the labels get there?

   Labelling objects based off their sensitivity is highly subjective. A piece of information might be very important to one company and virtually useless to another.
7. Rank the facts listed on slide 6 by sensitivity.

   2, 6, 4, 5, 1, 3
8. Invent labels for documents containing each of those facts.

   2 = (Top Secret: {WWII})
   6 = (Secret: {WWII})
   4 = (Confidential: {income})
   5 = (Confidential: {income})
   1 = (Unclassified: {baseball})
   3 = (Unclassified: {lunch schedule})
9. Justify the rules for "mixed" documents.
   When a document has mixed amounts of sensitive material, it is necessary to use the highest level of sensitivity. This is to ensure that all information is classified at least at the level it should be or higher.

Lecture 7

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

humans?

Labels are generally affixed to humans by security clearances or authorization levels. A good example of a human label would be a security badge that gave you access to a certain building or room.

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

humans.

Labels for documents explain how sensitive the information in the document is. Human labels indicate what categories and sensitivity levels that person can access.

3. In the context of computers what do you think are the analogues of documents? Of humans? Documents can be anything from directory tree to actual document files. Humans are generally users logged into the system.

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

The principle of least privilege makes sense especially in the context of systems/organizations that contain a lot of sensitive information. Because this information could be used inappropriately in the wrong hands, it is imperative that subjects can only access the minimum amount of information. This way they do not have access to information outside the scope of their working projects.

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.

1. (does make sense) Yes this human should have access because the sensitivity of the document is less than that of his/her clearance
2. (does make sense) No the human shouldn't have access because the document has a higher sensitivity than the human's clearance.
3. (does not make sense) The human shouldn't have access. Even though his security clearance is higher than the sensitivity of the document, the human does not have access to any files except those pertaining to nuclear topics.

Lecture 8:

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

actions?

These terms were introduced so we can better describe the relationships between the three.

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

3. Show that dominates is not a total order.

If dominates was a total order, then for arbitrary security label A, there would have to be a another security label B that either dominates A or is dominated by A.

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

   If two labels dominate each other, then they are equal.

5. State informally what the Simple Security property says.

The simple security property states that a human can read a document if their clearance dominates the document's sensitivity level.

6. Explain why it's "only if" and not "if and only if."
   If an object is dominated by a subject, he/she cannot necessarily have read access to it.

CS361 Questions: Week 1 4

Lecture 9

1. Why isn't Simple Security enough to ensure confidentiality?
   Simple security does not address write access, only read access.
2. Why do we need constraints on write access?
   Because someone could have security clearance to read a top secret document and if they had write access, they could copy it and change the sensitivity level on the copied document.

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

particularly important?

Constraints on write access are important in computers because if a program has faulty logic or malicious code, having access to write to any document can seriously affect the security of the system.

4. State informally what the *-Property says.

The * property basically says that if an object's sensitivity level dominates a user's clearance level, then that user has write access to that object.

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

object?

If a subject has read and write access, then their security clearance is equal to the sensitivity level of the 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.

It is a problem. In that case, we would need additional rules for integrity.

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?

You can not assume that security levels are so black and white that they would never change. For instance, as top-secret information gets older, it tends to become less sensitive.

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

Lowering the level of an object can be dangerous because if it is top secret information, this would give lower level subjects the ability to read it.

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?

To give all users read access, you would need to make their security clearance higher than that of every object. In order to keep users from writing to any of them, the categories for subjects must not be a superset of the categories of the objects.

2. Why wouldn't you usually build an access control matrix for a BLP system?
   Building an ACM for a real BLP system would take a huge amount of computations and space. It would not be realistic.

Lecture 12

CS361 Questions: Week 1 5

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.)

```
(H{A})  ←   (L{A})
  ^            ^
(H{ })   ←  (L{ })
```

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.

The upward flow of the lattice is a visual representation of the Simple Security policy and the * security policy. Thus, it represents the metapolicy.

Lecture 13

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

example on slide 1.

BLP rules permit L to write to H and H to read things at L, which are the general properties of BLP.

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

The read operation allows users to read any object as long as their security clearance dominates it. The write operation allows users to write to objects with a higher security clearance.

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

Create and Destroy give users the same options as Read and Write, despite the fact that really aren't "secure" because low-level users can destroy high level objects.

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

5. Why is the DESTROY statement there?

To illustrate that SH cannot destroy the first F0 it created.

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

If SH transmits a 0, then an extra file (SH, F0) will be created.

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

SL must do the same thing in both because otherwise it would violate BLP.

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

Yes it must do different things. If SH transmits 1, it cannot create an F0 with a higher level security clearance.

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

If SL can see bits that indicate the results of SH's actions, SL could theoretically predict/infer what activities SH is performing.

Lecture 14

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

Although talking over coffee can be considered the flow of information between subjects, there is not notion of a security hierarchy or any organized system.

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)

Yes this is a covert channel because depending on what SH write to F0, SL will see two different values.

2. Where does the bit of information transmitted “reside” in Covert Channel

   The bit of information resides in the system as an error message.

#1?

3. In Covert Channel #2?

   The bit of information in covert channel 2 resides in the process as a time unit.

CS361 Questions: Week 1 6

5. In Covert Channel #3?

The bit of information in covert channel 3 “resides” in the position of the particular cylinder. If a cylinder is very close to the read head, this essentially stores information about the process’s most recent read.

6. In Covert Channel #4?

The bit of information resides in l.

7. Why might a termination channel have low bandwidth?

   Some computations never terminate and sometimes it is impossible to predict whether they will terminate.

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

If energy was consumed at a constant rate, this could essentially become a timing channel. If the amount of power left was stored, it would be easy to discover how much energy was consumed.

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

   Any electronic device with a battery.

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?