Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

CS361 Questions: Week 1

Lecture 1

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

Home security and Personal information security are what is most relevant to my every day life. I am always making sure that nothing happens to our house and to keep it safe as well as important information and documents.

2. What do these have in common?

What they have in common is to being aware that something my happen and to do something to prevent that from happening.

3. Have you been a victim of lax security?

I do not think I have ever been a victim of lax security.

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

The likelihood that my laptop is infected is not very high because I do take care of my laptop and maintain it clean and with antivirus protection. At the same time there have been times that I do wonder if my computer is infected because of popups or activity that might be a sign of bugs in my system.

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

I have antivirus protection, I clean the disk every night and while on the internet I always try to visit pages that are know so that I can avoid viruses entering my system.

6. Do you think they are probably effective?

I do think that most antivirus protection are very effective because I have not had any problems with my computer regarding malicious software or any kind of bug that might put my computer in danger.

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

I agree because even though there exist really secure systems, there is always a way to hack and access other's computers. So by the FBI official warning us about cyber-adversaries against the US its true and it can happen.

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

Computer security is very important because in today's society we are more technological advanced and the risks of having a computer out in the open can give a lot of possibilities to individuals that know how to do great and malicious things to society. Knowing how to properly secure our computers is very essential.

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

Lecture 2

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

Perfect security is simply difficult to achieve because there are always ways to break that security. A factor that is also important other than the five reasons given is that most of the time, programmers only know how to program what they are specified to do without even thinking about how secure it should be so there are many programmers that might not know how to program a secure system.

2. Is there a systematic way to enumerate the "bad things" that might happen to a program? Why or why not?

I don't think there is a systematic way because the problem about security can be for any numerous reasons. If we consider one point to be very important for informational security, the same point might not be as important as another type of security. So I think that it varies according to the classification of security.

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

The defender has to find all the weakness where an attack can happen and the attacker only needs to find one to accomplish the hack against its secure system.

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

I agree in some extent because it is true that if we want to ensure computer security we need to follow those rules from Chang and Morris but that would mean that everybody will go back to reading newspapers, regular mail, getting information from the TV and so on. But in today's society having a computer is very important now and even though there are ways to properly secure our computers, there are many ways can be used to harm the security of our computers so perfect security is probably impossible in any computer system.

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

What it means is that since one side-effect is often to prevent useful things from happening, sometimes is required to focus on security less so that some other goal can be accomplish.

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?

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

Software security is there to protect us from harm but in order for software security to protect it does need to identify possible threats and risks there are within our society. So it is about managing risks.

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

Risk acceptance: Not buying phone insurance.
Risk avoidance: Buying phone insurance in case something happens to it.
Risk mitigation: Wearing a seatbelt to reduce greatest risks of injuries if accident happens
Risk transfer: Paying a company for the protection of our home.

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

ALE is a table of possible losses, their likelihood, and potential cost for an average year. It can be better explained as the expected loss of an asset due to a risk over a one year period.

5. List some factors relevant to rational risk assessment.

Some factors relevant to rational risk assessment can be technical, economical and psychological.

Lecture 4

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

In slide 2, the list has to do with Aspects of security which are major topics in security. In slide 3, the lists pertains to mechanisms to protect those major aspects in slide 2.

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

In my personal life, confidentiality is the most important because even though I do not have information for companies or anything like that, I do store personal information that is very important and if it is visible to other users then it could be used against me.

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

It means that data needs to be organized in a way that certain users can see certain data and so that it can also be easier to find and read.

4. Why might authorizations change over time?

It might change over time for better security. If it would stay the same, then other users would have the ability to have access since they know that the authorization never change.

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

Availability and reliability are both related in the sense that everything needs to be done within a certain time period so that it can be protected and better secure and at the same time be reliable to whoever is wanting that information.

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

6. In what contexts would authentication and non-repudiation be considered important?
When it is about having a contract, where they cannot deny the authenticity of their signature on a document.

Lecture 5

1. Describe a possible metapolicy for a cell phone network? A military database?
A metapolicy for a cell phone network can be to have an overall security between phone users. A metapolicy for a military database is to have a secure way to keep all data confidential.

2. Why do you need a policy if you have a metapolicy?
Because the policy provides specific and enforceable guidelines to the system user and often the metapolicy is too general to provide adequate guidance.

3. Give three possible rules within a policy concerning students' academic records.
1. Faculty and staff may not use student's SSN in documents, files, posting, etc.
2. Documents containing SSNs must be destroyed unless they are necessary for retention.
3. Document containing SSNs that are needed for retention must be stored securely.

4. Could stakeholders' interest conflict in a policy? Give an example.
Yes, because sometimes stakeholders are only looking to benefit themselves and would not care about the security of the students.

5. For the example given involving student SSNs, state the likely metapolicy.
Protecting the confidentiality of students SSNs.

6. Explain the statement: "If you don't understand the metapolicy, it becomes difficult to justify and evaluate the policy."
Because the metapolicy makes the users think about rules to protect what they are trying to secure, in other words without knowing what the larger goal is (metapolicy), it will be difficult to come up with rules (policies).

Lecture 6

1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?
Because the military tends to have confidential data that not all personnel have access to which is very important in the military. Yes, there are also aspects of integrity and availability.

2. Describe the major threat in our MLS thought experiment.
The major threat is the confidentiality of information.

3. Why do you think the proviso is there?
Because later in the course there will be some counterintuitive results that will require integrity and availability.

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

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

The forms of labels that we are using are according to their sensitivity level, for example Unclassified, Secret, Top secret. And need-to-know categories which can be under each important secure folder.

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

Because it probably pertains to people who are rank higher than everyone else and only have access to getting the labels there with the information.

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

From more sensitive to least sensitive: 6, 2, 4, 5, 1, 3.

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

Games schedule, cafeteria's menu, pay rates, invasion dates.

8. Justify the rules for "mixed" documents.

When a document contains both sensitive and non-sensitive information, it's always better to use the highest appropriate level so that it can only be seen by people authorized at that level of security. When it contains information relating to two different categories, we would separate them into their own categories, and that is for the same reason of security, users that are authorize to see one might not be authorize to see the other document and vice versa.

Lecture 7

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

Labels on humans indicate classes of information that person is authorized to access.

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

Labels for documents are label with sensitivity levels and labels for humans with clearances or authorizations levels.

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

Documents are treated as object because of the information they contain. In humans that they are the subjects and are the one who read and/or write to those objects.

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

Because if an individual has more access than what its job requires, that individual might leak the information accidentally or freely

.

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.

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

They make sense because in the first and third row, an individual has clearance for secret and the sensitivity level for that document is confidential and unclassified respectively, so logically it makes sense because of their higher rank in clearance.

Lecture 8:

1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?
Because it helps to better understand and classified things when we are using general terms like objects, subjects and actions.

2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).
(L1, S1) >= (L2, S2) only if L1 >= L2 and S1 is a superset of S2. So If we have (L1, S1) >= (L2, S2) then the rules would not apply and it will make it false.

3. Show that dominates is not a total order.
(L1, S1) >= (L2, S2) and so if we have (L2, S2) >= (L1, S1) then dominates will be false. That is why is only a partial order.

4. What would have to be true for two labels to dominate each other?
If the subject and object are both the same.

5. State informally what the Simple Security property says.
That subject S may be granted read access to object O only if subject S's clearance dominates object O's classification.

6. Explain why it's "only if" and not "if and only if."
Because the simple security property gives you a hurdle hat you have to get over to gain access but it doesn't mean that you necessarily gain access. It is a necessary condition but its not sufficient condition.

Lecture 9

1. Why isn't Simple Security enough to ensure confidentiality?
Because the simple security property codifies restrictions on read access to documents and not write access.

2. Why do we need constraints on write access?
Because we need to keep information from flowing via the writing mechanism.

3. What is it about computers, as opposed to human beings, that makes that particularly important?
Because computers can be programmed insecurely and that can cause information to leak when having write access.

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

4. State informally what the *-Property says.

That Subject S may be granted write access to object O only if the level of the subject it's dominated by the level of the object.

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

A subject must have the highest of the levels to be able to read and write to an object.

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

The General would need to log out of his top secret account and log in into his unclassified account so that there won't be any top secret leaks into an unclassified account.

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

We would need to incorporate the rules that would be about violation of integrity since that is what the corporal is doing and the sets of rules that we have pertain only to confidentiality.

Lecture 10:

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

By changing the subject's level up its bad because then a low-level subject could view high-level information just by raising its level. And if we lower the label of the subject then it's also bad because that subject may have high-level information that can carry down to the low level.

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

Because there can be times where an object is at the low-level and might move up to a high-level so that would need to change in order for subject at a high level to be able to read and not by low-level subjects.

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

Because lowering from a top secret Crypto to secret Crypto, information that once was top secret would now be available for a lower level subject to see.

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

The information that is at the higher level is not longer confidential and can be read by other subjects.

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

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?

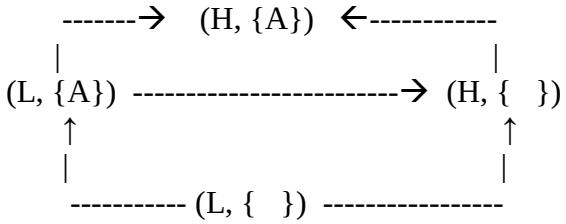
For the subjects, since they have access to all read files, thy can have Top Secret access, being able to read everything. And since they cannot have write access to anything in the library, they will have Top Secret as well and that's because high level subject cannot have write access to lower lever information.

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

Because we may have thousands of subjects and thousands of objects and so we are going to have a matrix with a lot of intersections and most of them are going to be empty because most subject won't have access to most objects.

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?

If Hs > Ls, Hs else Ls.

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

Because we only want information to flow upward and if it flows any other way then it would violate the security goals. To secure information, going up the lattice will be the metapolicy for BLP.

Lecture 13

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

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

Because a BLP lattice will have information flow from Low to High and not the other way around. So the BLP rules are put in place, simple security and the star property to prevent information from flowing high to low, which is a violation of the metapolicy.

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

Both read and write satisfy BLP because in READ, the level of the subject dominates the level of the object. In WRITE, the level of the object dominates the level of the subject.

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

They both satisfy BLP because they don't seem to violate the principles or the desired goals of BLP.

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

The level of the subject has to be at the same level as the level who is creating the object.

5. Why is the DESTROY statement there?

In case an object with name O exists and the level of the object dominates the level of the subject then it will destroy it.

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

No, the contents are the same, but depending on the subject level it may see different contents.

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

It has to do the same thing in both cases because that is the only way it can see what the object file contains.

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

It does different things because like in the example, it create it an object the first time and the second time it did not, so SH does not do the same things like SL.

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

Like the example on slide 5, a high level subject was used to send a bit of information to a low level subject by manipulating the system making easy for a low level subject to read the information and violating the metapolicy.

Lecture 14

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

Because the flow of information between the two human users is not within the system and they are not utilizing 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
```

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

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

This example is not a covert channel because the lower level subject cannot read, in both cases, the object information of the higher level subject.

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

It resides within the state of the system which in this case is the status of that resource which is used as the vehicle for sending that information.

4. In Covert Channel #2?

It resides within the timing or sequencing of events of the system.

5. In Covert Channel #3?

It resides in the most recent read of P because then q can have access to its information.

6. In Covert Channel #4?

It resides from variable H to variable L when computing the piece code.

7. Why might a termination channel have low bandwidth?

Because it only requires so little time for a termination channel to be destroyed.

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

The amount of energy that is consumed by a particular computation.

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

By using cell phones or video game systems.

Lecture 15

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

They can send thousands to millions bits of information with such a low bandwidth.

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

Because covert channels on real processors operate at thousands of bits per second making hard to eliminate every single one.

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

We can eliminate it by modifying the system implementation. We can reduce the bandwidth by introducing noise into the channel. And we can monitor it for patterns of usage that indicates someone is trying to exploit it..

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

Luis C. Lopez
LL9338
LL9338
Lclg21@utexas.edu

A low level subject tries to access a high level object and in return a high level subject sends a denied message.

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

The sender is the one that modifies the object so that the receiver can read the message sent. Through that message, information can be transmitted and that's why is called a covert storage channel.

Lecture 16

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

Because we don't know for sure that the file exists so we have to infer it by using an M instead of R.

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

Because the R and the M on a particular row says that for that attribute there is a mechanism by which someone can modify it and someone can reference it and that is what we need for a covert channel to exist.

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?

No because it only depend on the calls. For example, if the column READ some have R and M, then it only says that it can be read but not access to write, or create, etc. so it would not work.

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

Because it can help with the identifying of covert channels and dealing with them appropriately.