Matt Hendrickson
mjh2793
mjh2793
matthewjames@utexas.edu

Week 1 questions

Lecture 1

1. What uses of the term "security" are relevant to your everyday life?
Make sure the doors are locked and the windows are closed when I leave the house. Also at night close the blinds. The information on my facebook and bank account are password protected. At my job, the paperwork related to the cash transactions have to secure and entered in a few different places and reviewed by a few different people.

2. What do these have in common?
It prevents unauthorized access, either for stealing, changing, or simply viewing.

3. Have you been a victim of lax security?
yes, my car was broken into once.

4. What is the likelihood that your laptop is infected? How did you decide?
unsure, if it is I cannot tell. Nothing malicious seems to be going on. I don't have any unauthorized transactions on my bank account.

5. What security measures do you employ on your laptop?
none

6. Do you think they are probably effective?

Lecture 2

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

1. have to consider all the bad things that you don't want to happen
2. must know every way you can be attacked
3. concerned with defeating an actively malicious opponent
4. You have to defend against all means of attack. attacker need only find one weakness
5. find balance between functionality and security.

*6.

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

No because it all depends on the program itself and the context the program operates in

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

The defender has to protect from every avenue of attack. The attacker only needs to find one weakness

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

while I'm sure they were just being humorous, I dont agree with the quote. You don't need perfect security to have a well operating system. Just have enough security to mitigate the serious threats.

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

Because security complicates the building and implementation of the software, a tradeoff between how much security and how much functionality, ease-of-access, marketability, etc. is required.

Lecture 3

1. Define "risk"?

The probability of a threat to your system.

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

yes, you have to be able to prioritize what you want to be able to protect.

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

accept - The risk of getting into a car accident when I go driving.
avoid - The risk of lung cancer from smoking cigarettes
mitigate - baseball bat in case a burglar breaks into the house
transfer - Taking the bus downtown instead of driving myself.

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

By figuring out how much money/time/resources you will lose in a given period of time can help prioritize what you need to protect.

5. List some factors relevant to rational risk assessment.

Probability of each event happening
Estimated amount of damage that would be caused for each event
The kind of damage caused by each event happening

Lecture 4

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

The second list are ways to implement the things in the first list.

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

integrity - I don't want someone to be able to change my bank account password.

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

Group objects by their classification

4. Why might authorizations change over time?
People would get different access powers as their jobs change. people get fired or promoted, new people come into a system.
5. Some of the availability questions seem to relate more to reliability than to security. How are the two related?
Security means different things in different contexts. In the context of reliability, a user needs to be able to access th system or recieve its fair share of resources.
6. In what contexts would authentication and non-repudiation be considered important?
When I log into my bank acocunt for authentication. Even if my username and password are entered correctly that could just someone else who stole them from me. Recently my bank has required a code sent via text to be entered if i am using a new device. for non repudiationIf i made a transaction with another person via ebay and they try and say they were hacked and the transaction should be cancelled I can use nonrepudiation techniques to try and prove that they did indeed make that transaction

Lecture 5

1. Describe a possible metapolicy for a cell phone network? A military database?
Metapolicy for cell phone network -
2. Why do you need a policy if you have a metapolicy?
the policy describes the actual means of implementing a metapolicy
3. Give three possible rules within a policy concerning students' academic records.
don't let anyone change the students grades except the registrar or the students current teacher.
only the student can see his whole academic record
The teacher can only change the grades of the student for the class the teacher is teaching to the student
4. Could stakeholders' interest conflict in a policy? Give an example.
yes, Maybe the teacher makes a mistake in grading but the semester is over. That teacher should be able to go back and change the grade but according to the scenario above he/she wouldn't be able to. The student and the teacher are the stakeholders in this example.
5. For the example given involving student SSNs, state the likely metapolicy.
confidentiality
6. Explain the statement: "If you don't understand the metapolicy, it becomes difficult to justify and evaluate the policy."
if you don't have a clear objective then it will be difficult to figure out how to implement it.

Lecture 6

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

Plans must be kept secret lest the enemy find out. The leaders need to be able to make sure the plans are not changed and be able to have access to them whenever they need.

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

The leak of war plans

3. Why do you think the proviso is there?

some of the policies concerning confidentiality by itself might seem counterintuitive to overall security

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

linearly ordered

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.

1. Normandy invasion
2. Enigma codes broken

3-4 the raises
5-6 baseball/lunch schedule

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

Normandy invasion - Level 0 classified
Enigma codes - Level 1 classified
raises - Level 5 classified
basebal/lunch - public knowledge

8. Justify the rules for "mixed" documents.

Normandy invasion needs to be the highest level of security - it is crucial to the war effort that that succeed. Engima codes broken - helps the war effort a lot but if the enemy finds out and changes their codes that won't hurt the invasion of normandy. The raises are one level above public knowledge because they are not that important.

Lecture 7

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

They are inlcuded in information profile about them depending on the system.

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

labels for documents come from the linear ordered set. the labels from humans are a linearly ordered set based on importance to sensitive intelligence by job description.

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

documents to files as humans to profiles.

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

Since there's no reason to grant access thats not pertinent to the job then why grant it? Theres not point in assuming that extra risk, however small.

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.

If someone with a high access in a given subject wants to read a lower access in the same subject then sure.

The person reading does not have top secret access, only secret.

Anyone can read unclassified.

Lecture 8

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

it corresponds to the language used in our project description

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

There are combinations of subjects/objects that, given this sytem, neither would dominate the other.

3. Show that dominates is not a total order.

You could have Subject {crypto : A, B} and subject {nuclear: C} This would result in neither dominating the other, thus the system containing these two things would not be total order.

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

they are the same label

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

A subject with a certain label can only have read access if the subjects clearance is equal to or greater than the objects

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

I don't see a difference between the two.

Lecture 9

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

It doesn't have the property of secure writing.

2. Why do we need constraints on write access?

So someone with top secret access cannot write something top secret onto an unclassified folder.

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

There could be a leak in a program and the user would not even know it.

4. State informally what the *-Property says.

You can only write to your level of clearance or below.

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

The clearance levels of the user and the object must be the same.

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

Give the private access only to the top secret document he needs to complete his mission

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

modifications made by lower cleared levels must be approved by members that have clearance levels equals to the object in question

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?

not enough flexibility, it could interfere with functionality

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

It could be accessed more easily and a virus could then be hidden inside of it.

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

The subject doing the downgrade must be a equal to higher level to the object prior to downgrading.

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?

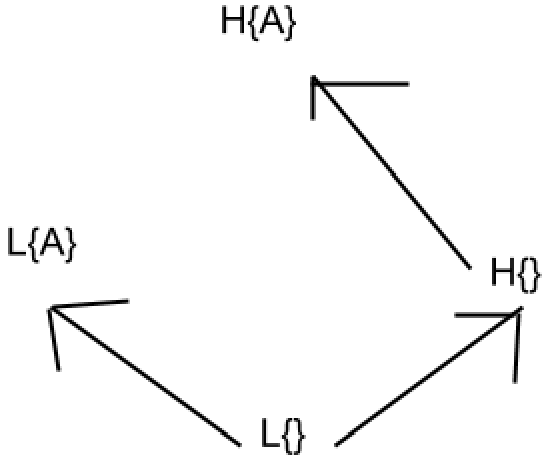
Subjects would be given the highest access clearance. Objects clearance would not matter because Subjects can read everything if they have the highest level of clearance.

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

Because it would be very large and complicated for most realistic systems.

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?

to find the GLB follow the flow of info all the way until you cannot go any farther. To find the LUB go in the opposite direction.

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

The upward flow of info is how the rules of BLP are manifested within the system.

Lecture 13

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

Low can write to high and high can read from low. Information flows up the lattice.

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

They fallow the simple security and * principle which form the basis for BLP

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

These two operations do not mention reading or writing and their definitions do not violate any of the tranquility properties that we would use in BLP so they satisfy BLP

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

The system be a BLP system.

5. Why is the DESTROY statement there?

To eliminate the object that can be traced to the covert channel. Essentially, covering your tracks.

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

NO.

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

Because the contents of the files are the same and the operations are performed in the same order.

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

Because SI is always trying to read from FO. Depending on the level of FO is how SH reacts.

9. Justify the statement on slide 7 that begins: “If SL ever sees...”
Because of the example just shown in the previous slides, SL is clearly seeing varying values dependent on SH.

Lecture 14

1. Explain why “two human users talking over coffee is not a covert channel.”
it’s in a public place
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?
Sh
4. In Covert Channel #2?
In the clock timing mechanism of objects p and q. The information transmitted can be iterpreted by q by it seeing how much time was left on the clock when p relinquished control of the processor
5. In Covert Channel #3?
Both.
6. In Covert Channel #4?
in variable h
7. Why might a termination channel have low bandwidth?
the program took up too much bandwidth and the computation terminated.
8. What would have to be true to implement a power channel?
a way to measure how much power is consumed
9. For what sort of devices might power channels arise?
power supply unit for PC’s. batteries on phones

Lecture 15

1.Explain why covert channels, while appearing to have such a low bandwidth, can potentially be very serious threats.
They transmit thousands of bits per second without affecting the perfomrance of the processor.
2. Why would it be infeasible to eliminate every potential covert channel?
too many to get rid of all. getting rid of one could create another. takes away functionality
3. If detected, how could one respond appropriately to a covert channel?
keep it monitored then close it if it becomes a problem.
4. Describe a scenario in which a covert storage channel exists.

when two entities have access to some attribute of a shared object. The sender must be able to modify that attribute and the receiver must be able to view it. There must be a way to initiate each function and syncronize their movements so that the information will get transmitted form sender to reciever.

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

above.

Lecture 16

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

It doesn't actually read the file. After the operation you only know that the object exists.

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

If there is a way to both read and write from a given area then that area is a potential covert 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?

No, They would not be from the same attribute therefore sender and reciever are not connected on that avenue.

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

It shows potential vulnerabilities in a system.