Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

CS361 Questions: Week 1

Lecture 1

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

The uses of the term security that are relevant to my life are Personal, Physical, and Computer Security.

2. What do these have in common?

These types of security all pertain to issues that can affect me directly, and are issues that I deal with every day.

3. Have you been a victim of lax security?

I have not yet been a victim of lax security.

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

It is not very likely that my laptop is infected. I can tell if suddenly a foreign virus protector pops up, if my internet browser is unable to open suddenly, or if my computer begins to lag out of nowhere.

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

I have my firewall active, and a real-time malware protector active. I also try to stay away from sites or emails that I am unfamiliar with.

6. Do you think they are probably effective?

As of this moment, it is very effective.

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

I think that the quote is very accurate. Case-in-point, the incident with Target came out of nowhere, thousands of people were effected, and still no one knows how it happened.

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

The importance of learning about computer security is to prevent security failures.

Lecture 2

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

factors?

I also feel that because "every six months" we update our technology, and computers can become obsolete very quickly, security is like a dog chasing its tail, with new technology there is always something.

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com
2. Is there a systematic way to enumerate the “bad things” that might happen

to a program? Why or why not?

There is not a systematic way to enumerate the “bad things” because there is no way to know every single attack on a program and still have a functioning program.

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

The defender has to think like all of the attackers in the world in order for them have effective security, while the attack only has to think of the one thing that the defender would overlook or not expect.

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

not?

Computers are everywhere, in our phones, parking meters, cameras and calculators. I feel that in our time, people would not be able to live without their computers. Also, not using your computer as Morris and Chang suggest is not fixing security issues, it is ignoring the problem.

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

Your program can only use so much space, and generally other computers can only give the program so much space. It cannot be both completely and quickly functional and also completely secure.

Lecture 3

1. Define “risk”?

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?

I feel that software security is more than managing risk.

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

one you transfer?

I would accept the risk of going to college and taking out loans with the possibility that I may have bad credit or go into debt.

I would avoid the risk of driving under the influence at night because the risks outweigh the positives.

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

I would mitigate the risk of buying a new item on sale because if I don't like it, at least I didn't pay too much for it.

I would transfer the risk of email fraud by giving the user the choice to use a password.

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

ALE sounds like it takes to mitigating their risks.

5. List some factors relevant to rational risk assessment.

Technical, economic, and psychological factors are relevant to rational risk assessment.

Lecture 4

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

The lists on slide 3 is how you would do the lists on slide 2.

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

For me, confidentiality is the most important. I do a lot of things online and do not want information like credit card numbers or my ssn.

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

Some data might be more important than other data. Things that take credit card information poses a higher security risk than sites that use a password.

4. Why might authorizations change over time?

For example, if you die who has authorization to your bank accounts?

5. Some of the availability questions seem to relate more to reliability than to

security. How are the two related?

Security issues can occur if the data you need is not reliable. If the data is not reliable, then it can not be available for use.

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

important?

These would be considered important if it is mostly humans transferring data.

Lecture 5

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com
1. Describe a possible metapolicy for a cell phone network? A military database?

For a cell phone, the metapolicy would most likely be confidentiality, and for a military database, the metapolicy would will be in terms of confidentiality and integrity.

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

The metapolicy is the overall security goals and the policy is needed in order to break down the specifics of the overall goal.

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

records.

1. Students are only able to see their academic records.
2. Authorized professors are able to see specific student records and can change them.
3. Academic records should only be available to view or change for a certain amount of time.

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

If you have something to lose, then you want some say so in how the operation works.

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

The metapolicy would be to make sure that Students' ssn protected and are not made public.

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

difficult to justify and evaluate the policy."

If we do not know what the overall security goal is, it becomes hard to explain why the policies exist.

Lecture 6

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

There are important things that not everyone needs to see. Integrity is also important because we do not want just anyone to be able to change information.

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

The major threat in this experiment are those viewing information that they are not authorized to view.

3. Why do you think the proviso is there?

The person is able to view the material only if they have the authorization to do so.

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

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

The sensitivity of the data is the title and those who can access it are in the brackets.

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

The labels depend on how sensitive the data is.

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

6 & 2, 4 & 5, 1 , 3

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

War Plans, Finances, Social Events, School

8. Justify the rules for "mixed" documents.

If the war plans happen to have information about school lunches, it is okay for everyone to see the school lunch information, but not everyone can see the war plans, this is why it has to be restricted to a higher sensitivity level.

Lecture 7

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

humans?

Humans will have authorization levels or clearance.

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

humans.

Documents are labeled as how important they are while humans are by how much information they are trusted with at the time.

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

The hardware would be the analogues of documents while humans are the software.

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

So that information is not leaked by accident, it makes sense to give the individual information that they are authorized to see and only what is needed.

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.

The answers make sense that the person with "supreme" authorization can see everything, and people cannot see documents that are of higher ranking.

Lecture 8:

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com
1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?

So that they can be general terms that apply to computer security.

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

Data that dominates can be both greater than and equal to itself and other data.

3. Show that dominates is not a total order.

There exist labels that are neither greater than nor equal to each other.

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

The labels would have to be equal to each other.

5. State informally what the Simple Security property says.

I can read objects on the same level and below me.

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

There might be other security issues that might prevent a subject from reading an object, even if they are authorized.

Lecture 9

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

Someone can copy the top secret information and place it into a lesser sensitive document.

2. Why do we need constraints on write access?

We do not want information to leak without our knowledge.

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

Computers can read malicious software and leak information without knowledge.

4. State informally what the *-Property says.

Information can only be written up to higher sensitivity.

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

The subject can only read and write to an object that is exactly the same.

6. How could we deal with the problem that the General (top secret) can't send

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com
orders to the private (Unclassified)?

The General can log in as a private and send orders that way.

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

we might deal with that.

There can be a wait time in order for the information to be viewed by the higher rank before it gets overwritten.

Lecture 10:

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

We do not want to arbitrarily change the level of the subject down because they may have knowledge of important data, it might be okay to change the level up.

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

We might need to add a label, or give a subject a higher ranking.

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

The object might contain sensitive information.

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

to be secure.

They must not have knowledge of important information, or else it will be a write down.

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?

All subjects will be on the high level and objects would be on the low level.

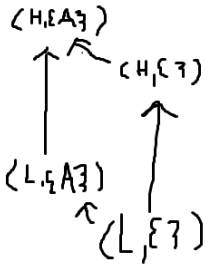
2. Why wouldn't you usually build an access control matrix for a BLP system?

You can create these permissions on the spot by using the simple security and -* property.

Lecture 12

1. Suppose you had hierarchical levels L, H with L < H, but only had one

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com



category A. Draw the lattice. .)

2. Given any two labels in a BLP system, what is the algorithm for finding

their LUB and GLB?

We simply follow the arrows in the lattice. The two labels do not dominate each other if there is no arrow between them, and the arrow points up to the dominating label.

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

We want to constrain the flow of information among different security levels.

Lecture 13

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

example on slide 1.

It is used to prevent information from flowing high to low.

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

READ satisfies that we can only read down, the subject has to dominate the object while we can only write up, the subject is dominated by the object.

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

CREATE satisfies because information is not being read or written, it is a new object. DESTROY satisfies because we can only destroy if we can write, it is just like writing over the data.

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

The low level create, read, and write have to be the same.

5. Why is the DESTROY statement there?

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

The objects can be used in a loop, created again and again using the same names.

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

The contents of the files are the same.

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

SL has to do the same thing in both cases because it has no other way to check if the value read is correct or not.

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

SH does different things because each case reads different values, it does not need to be the same because SH is already created.

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

This means that if the results of the object that is read is different, the metapolicy can be violated in order for information to travel down fix the problem.

Lecture 14

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

They are not using the system in order to make the information flow.

2. Is the following a covert channel? Why or why not?

This is a covert channel because the subject can both read and write.

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

#1?

The bit resides in p.

4. In Covert Channel #2?

The bit resides in q.

5. In Covert Channel #3?

The bit resides in p.

6. In Covert Channel #4?

The bit of information resides in l, but the value depends on h.

7. Why might a termination channel have low bandwidth?

If the channel is terminated and then fixed, the amount of memory and space used overall is low.

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

Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

To implement a power channel, you have to embed information in the power being used.

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

Phones or ipods, any device where the energy comes from another computer.

Lecture 15

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

We do not know how much information can be sent through the channel over time.

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

Some channels contain so much noise or the bandwidth is so small, it can not be detected.

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

We can eliminate it, monitor it, or introduce noise to make it hard for information to pass through.

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

A student and Professor have access to a student's exam grades and exam corrections.

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

The professor can change the grade while the student can view the grade, and also submit test corrections and the professor can change the grade.

Lecture 16

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

Create does not tell us if it had to create.

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

There is a mechanism that someone can modify it and someone else can reference it.

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?

This does not indicate a potential covert channel because the columns of the table refer to different operations, that do not pertain to the same data.

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

table?

It gives us a systematic way of looking for channels.