**Vincent Nguy vn2863**

**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?

Financial Security, Personal info Security, and Health.

1. What do these have in common?

They are seems to mean something like “protection of assets against threats”

1. Have you been a victim of lax security?

Most Likley Yes, just don’t have an example on the top of my head.

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

Maybe. I only use a free firewall off cnet & the free version of Malwarebytes. So I decide by if they tell me I’m infected or not.

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

Honestly. Almost nothing, I have a password for my user-profile, a firewall, some anti-virus software, and Malwarebytes.

1. Do you think they are probably effective?

Yes. I feel like they give me enough Security to preform day to day tasks on my laptop and information I have on my laptop.

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

No not at all. If that’s the case than it’s really serious. The Information stored on Computers in the wrong hands could jeopardize someone’s life. Computers run our Country.

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

To protect our personal information better, contribute to security in your workplace, and overall security in cyberspace.

# Lecture 2

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

Ya you can’t protect against everything. People are coming up of new ways to break Security every day.

1. Is there a systematic way to enumerate the “bad things” that might happento a program? Why or why not?

No Not all “bad things” is known to every single programmer who does Security, and new “bad things” pop up everyday.

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

Defender trys to prevent bad things from happening.

Attacker will use any available means to subvert the security of a system

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

Well if we want to be sure the information on our system is completely secure then sure. But the information on my computer isn’t that important to take those measures.

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

Security can sometimes get in the way of the function of the program. Sometimes it’s necessary to trade performance for a better Security.

# Lecture 3

1. Define “risk”?

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

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

Yes. Assessing my assets vs risks and vulnerability and how to prioritize counter measure options.

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

A Risk I accept is not allowing my bike in my room and leaving it at the bike rake outside.

A Risk I avoid is not ever driving drunk because the risk is too high.

A risk mitigation would be having car insurance.

A risk transfer is my homes security system.

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

Amount

Write down what your risks are, Write down the potential downside of the risk being actualize ,and fine the probability it actually occurring.

1. List some factors relevant to rational risk assessment.

Technical factors, economic factors, and psychological.

# Lecture 4

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

Confidentiality, Integrity, and Availablity are the 3 major aspects of security. And the things on slide 3 is just mechanisms to achieve those major asepcts.

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

Mostly just Integrity I have data on my Computer I feel its integrity is important. I have data on my PC where I need to protect and know who I can let modify.

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

To split data into groups and categorizes of difference access levels.

1. Why might authorizations change over time?

You might need give access to data to work on projects but only for certain periods of time

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

Yes reliability is important if something isn’t operating correctly then it is just as compromised .

1. In what contexts would authentication and non-repudiation be consideredimportant?

To protecting Banking and personal information would be important to authentication, and buying things online would require non-repudation.

# Lecture 5

1. Describe a possiblemetapolicyfor a cell phone network? A military database?

For a phone network who can write, or modify information on a users phone account, integrity

For a military is having different security levels of access for people and objects. confidentiality

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

Because the metapolicy is too general.

1. Give three possible rules within a policy concerning students’ academicrecords.

Faculty may not use students SSN in documents or postings.

Documents containing SSNs must be destroyed unless deemed necessary.

Documents containing SSNs and deemed necessary for retention must be kept in secure storage.

1. Could stakeholders’ interest conflict in a policy? Give an example.

Yes if like Secret answers to retrieve lost passwords, many people sometimes forget them and have a harder time in retrieving their forgotten account’s.

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

Protecting the Integrity of who can access and modify important documents

1. Explain the statement: ”If you don’t understand the metapolicy, it becomesdifficult to justify and evaluate the policy.”

Policies are just mechanisms to build your metapolicy if you don’t understand the metapolicy you might not be building it with the correct Policies

# Lecture 6

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

Because in the military there is information that is sensitive and can ruin operations if in the wrong hands. Yes all three has aspects in military security. You need ways to protect the integrity of data and you need availability for the networks that runs the systems.

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

Confidentiality

1. Why do you think the proviso is there?

Because this Policy should only be focused on confidentiality it wouldn’t be as effective if we try to do everything here.

1. Explain the form of the labels we’re using.

It reflects the sensitivity of the information contained within that folder. Containing a hierarchical component and a set of categories.

1. Why do you suppose we’re not concerned with how the labels get there?
2. Rank the facts listed on slide 6 by sensitivity.
3. Normandy Invasion.
4. British has broken the German Enigma codes
5. Col.jones didget a raise, Col. Smith didn’t get a raise.
6. The cafeteria is serving chopped beef on toast today., and the baseball game schedule.
7. Invent labels for documents containing each of those facts.

(Top Secret {WarPlans})

(Secret {Spies})

(Confidential {Personnel})

(Unclassified {})

1. Justify the rules for “mixed” documents.

This allows for just giving a limited and just enough amount of information to people to get their jobs done. Which is good for security.

# Lecture 7

1. Document labels are stamped on the outside. How are “labels” affixed tohumans?

It indicates the degree of trustworthiness to which a person has been vetted. And gives clearance to certain information.

1. Explain the difference in semantics of labels for documents and labels forhumans.

A label for a document indicates the sensitivity of information contained.

For a Human labels indicates the authorization to view information.

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

A document is data stored, and A human is a variable passed in

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

If you try to keep as much information from not being read by people then the chances of it being leaked is lower.

1. For each of the pairs of labels on slide 6, explain why the answers in thethird column do or do not make sense.

It makes sense. The first one Secret is a higher security level then Confidential and both labels are Crypto so yes. The 2nd the Subjects clearance is lower then the object so no access. The third Subject level is higher then object level and subject label is a superset then the objects so yes.

**Lecture 8:**

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

Because

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

There are Objects and Subjects that don’t dominate each other. i.e. a object with a the label {Spy} and Subject{Nuclear}.

1. Show that dominates is not a total order.

There are security labels A and B, such that neither A>=B nor B >=B

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

They are on the same Security level.

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

If Subject Dominates the Object it can read the Object.

1. Explain why it’s “only if” and not “if and only if.”

This is only a necessary condition but not sufficient enough.

# Lecture 9

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

It only deals with reading information. Suppose someone with access to a Top Secret document copies the information onto a piece of paper and sticks it into an Unclassiﬁed folder. It’s ok with Simple Security but violateds confidentiality.

1. Why do we need constraints on write access?

Using example from above. Suppose someone with access to a Top Secret document copies the information onto a piece of paper and sticks it into an Unclassiﬁed folder. It’s ok with Simple Security but violateds confidentiality.

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

Subjects in the world of computing are often programs operating on behalf of a trusted user.

1. State informally what the \*-Property says.

If the Object dominates the Subject it can write.

1. What must be true for a subject to have both read and write access to anobject?

They both dominates each other, on the same clearance level.

1. How could we deal with the problem that the General (top secret) can’t sendorders to the private (Unclassified)?

Have him use a lower clearance account for that.

1. Isn’t it a problem that a corporal can overwrite the war plan? Suggest howwe might deal with that.

That is a violation of integrity we would have to build a policy to deal with that.

**Lecture 10:**

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

Its ok to change as long as it doesn’t violate the security Policy, not \* Property and Simple Security.

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

if a user needs to operate at different levels during the course of the day.

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

Then that destroys the idea of information should only flows up anyone can access any information.

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

It must not violate the \* Property and Simple Security.

**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?

Make all Subjects High and all Objects Low with High dominates Low.

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

No there could be thousands of objects and subjects and this could be compute the accesses faster with \*prop and simple security.

# 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.)

H{A}

^

|

L{A}

1. Given any two labels in a BLP system, what is the algorithm for findingtheir LUB and GLB?
2. Explain why upward flow in the lattice really is the metapolicy for BLP.

If information flows any other way it would indicate a violation of the securities goals.

# Lecture 13

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

Info flow from L to H is the metapolicy. We can read down which doesn’t affect info flow from L to H. and only being able to write up still keeps info flowing up and Strong tranquility.

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

Reading can only work is Subject >= Obj so its Ok

Writing can only work if Subject <= Obj so its Ok.

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

Objects can only be created at your level does not make information flow down

Destorying Objects higher then your level does not make information flow down

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

The operations by SL must be the same on both sides.

1. Why is the DESTROY statement there?
2. Are the contents of any files different in the two paths?

Yes

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

For the operation to be constant if SL did something different this would be inconclusive.

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

To show that 1 bit flows from high to low

1. Justify the statement on slide 7 that begins: “If SL ever sees...”

There can be features in a System that can be used to send information where it shouldn’t called Covert Channels

# Lecture 14

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

This does not use resources within a system that violets the security to send information

1. 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)

No.

1. Where does the bit of information transmitted “reside” in Covert Channel #1?

The error message sent to the low level Subject

1. In Covert Channel #2?

The time that elapsed between the two processes can be measured.

1. In Covert Channel #3?

The Read Head of the Disk Drive depending on p and q’s last read.

1. In Covert Channel #4?

The value of l is influenced by the value of h

1. Why might a termination channel have low bandwidth?

It doesn’t stop until the operation is terminated

1. What would have to be true to implement a power channel?
2. For what sort of devices might power channels arise?

A cellphone.

# Lecture 15

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

Covert channels on real processors operate at thousands of bits per second,

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

That may just not be possible and may end up hindering your program.

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

You can introduce noise in the system to reduce bandwtih

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

A user on a computer is sharing a harddrive with another user. One person writes to some shared resource and another reads from it.

1. Describe how this covert storage channel can be utilized by the sender andr receiver.

One person writes to some shared resource and another reads from it. Would allow them to send information between each other.

# Lecture 16

1. Why wouldn’t the “create” operation have an R in the SRMM for the “fileexistence” attribute?

You don’t get the information directly that the object is created.

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

Someone can send information and someone can modify it which you need for a covert channel

1. 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 .Someone can send information and someone can modify it which you need for a covert channel

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

To see the possible covert channels in their system