UTEID: aji272;

FIRSTNAME: Alex;

LASTNAME: Irion;

CSACCOUNT: alex10;

EMAIL: alexirion10@gmail.com;

**CS361 Questions: Week 1**

**Lecture 1**

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

Personal, network, communication, homeland, and system security are all relevant to me.

1. What do these have in common?

All of the types of security are protecting assets against threats

1. Have you been a victim of lax security?

Yes, I have had a twitter password stolen and my house broken into before

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

My laptop is very unlikely infected right now. I have a mac, which has noticeably less viruses and haven’t downloaded anything off of the Internet that was suspicious lately.

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

I run adblockers on the web, make sure to be careful what I click on, make sure I visit secure web sites, and make sure I know and understand everything I download

1. Do you think they are probably effective?

I think my measures are effective, but most likely not perfect

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

Yes, I think it is possible. It would be extremely difficult to do with updated security measures. No security wall in computers has been perfect or without a flaw.

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

It is important to know how to protect data and information online, especially when your attacker is in physical contact.

**Lecture 2**

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

Often times you have no idea who the attacker is or where it is coming from. As said by Robert Morris, the only way to truly have security is to disconnect from everything. Some attacks are even indictable, I might not even be aware someone is trying to get into my system.

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

No. You can fix the security to patch up an issue after the fact, but there is no way to systematically cover/foresee all “bad things”. The defender has to find and eliminate all exploitable vulnerabilities; the attacker only needs to find one.

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

 As stated in the answer above, the defender has to find and eliminate all exploitable vulnerabilities; the attacker only needs to find one. The defender must consider all possible vulnerabilities, while the attacker only needs to fine one.

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

In a sense they are over-exaggerating, some computers and systems are very difficult to attack. However, to truly insure 100% security one must essentially completely disconnect the computer and power it off.

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

Usually when security is made much stronger, it also prevents certain actions within the system. For example, if all users of a system had the same security access they could work as a more functional team, but if security access had a hierarchy for safety purposes the efficiency of the team may decrease.

**Lecture 3**

1. Define “risk”?

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

Also stated as a potential threat to a system.

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

Yes. A system cannot completely prevent attacks, but they can certainly manage the amount of risks involved. You can identify threats and manage the overall vulnerability of the system

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

Risk you accept = risks tolerated by the organization. Ex. The cost of making a security measure is more expensive that the potential value lost

Risk you avoid = not performing an activity that would incur risk. Ex. Not allowing remote logins

Risk mitigation = taking actions to reduce the losses due to a risk. Ex. Creating a complex login portal or encrypting information

Risk transfer = shift the risk to someone else. Ex. Using a home security system to prevent a break in, using external money transfer options instead of creating your own

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

The bank should spend more money on teller theft security prevention since it has the highest annualized loss expectancy. Next it should attempt to secure SWIFT\* fraud even more since the ALE is very high as well.

1. List some factors relevant to rational risk assessment.

Technical, economic, and psychological risk factors

**Lecture 4**

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

Slide 2 is the meta-policy (overall goal of the system) and slide 3 is the policy (mechanisms/methods to achieve the meta-policy)

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

Confidentiality. In my personal life, my most important things include preventing others from reading my computer files, passwords, or online information.

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

You place similar data items in similar places and categorize each group based on its sensitivity. Only authorized people will be able to access certain groups of data. Not all data is equally as sensitive, therefore leading to different levels of restrictions.

1. Why might authorizations change over time?

Authorization might change in a promotion/demotion, or a need to access new information. This could change the availability of certain data

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

Without a reliable system to get you information, you system isn’t secure, and without security the reliability of the system may be worse. They depend on each other.

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

 In the military, a system would need to authenticate users to make sure only the right people are accessing information. Non-repudiation could also be important incase a certain action was accidently initiated (you would need a way to cancel an action).

**Lecture 5**

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

Protect the integrity of information transmitted.

Keep information confidential and only allow access to authenticated people.

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

You need the policy to implement and achieve the metapolicy. The metapolicy can often have multiple interpretations, and multiple possible policies to accomplish the meatpolicy. The policy provides specific and enforceable guidelines to the system user.

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

Faculty and staff cannot use students SSN. Documents containing SSN should be destroyed. Documents kept with SSN must be put in secure storage.

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

 yes. Some stakeholders may want complete confidentiality, while others may desire availability. For example, teachers may want to keep some academic records for integrity and legal purposes while students want them destroyed for protection of their SSNs.

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

 Protect students personal SSNs.

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

Without understanding the over reaching goal/ what you are trying to accomplish, the policy doesn’t have any purpose or solve any metapolicy.

**Lecture 6**

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

The militaries main goal is keeping their information private from the public. There are aspects of availability and integrity in still allowing the military officials to get the data they need and making sure all info is only changed by those that should have access.

2. Describe the major threat in our MLS thought experiment

 How do we determined who is authorized to what? A major threat arises in that just because we are keeping certain people out, doesn’t mean that we are in any way limiting what they can do once inside.

3. Why do you think the proviso is there?

  Implementing integrity and availability is a much more complex system and requires many different styles of use.

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

The labels is a linear ordered set of dominance. Ranging from bottom to top: unclassified, confidential, secret, top secret.

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

The labels are placed upon the creation of a document, we just need to keep certain people from viewing documents they don’t have authorization to.

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

The British have broken the German enigma codes. The Normandy invasion is scheduled for June 6. Col. Jones got a raise. Col. Smith didn’t get a raise. The cafeteria is serving chopped beef on toast today. The baseball team has a game tomorrow at 3pm.

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

Military/secret (first 3), personnel (raises), general info (daily activities/last 2)

8. Justify the rules for “mixed” documents.

Any document with mixed levels of information should be placed in the highest appropriate level.

**Lecture 7**

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

People only see the documents that are equal to or less than their personal label. A person’s label symbolizes the trustworthiness and need-to-know domain he/she has been vetted.

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

Labels on documents indicate the sensitivity of the contained information, labels on humans indicate classes of information that person is authorized to access.

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

The operating system, hardware in the computer, programs, and various file folders on the computer.

Organs essential to living (heart/brain), organs that help regulate (stomach, nervous system), form organs (muscles, fat, bones)

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

People don’t need information above their clearance to understand do their proper job. If further information is required than what is given, then they should consult a person in a higher position.

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

Row 1: secret > confidential, and they both have crypto

Row 2: secret < top secret

Row 3: secret > unclassified, and t he unclassified doesn’t have a category of clearance

**Lecture 8:**

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

They are the different physical things interacting with each other. Since there are 3 categories we can establish a relationship between them

1. Prove that dominates is a partial order (reflexive, transitive, anti-symmetric).

With security labels A and B, neither A>=B or B<=A is always true. Even though the clearance might have a higher level, the order relation depends on special labeled categories.

1. Show that dominates is not a total order.

Top Secret {crypto} | Secret {Nuclear} = No dominance

Just because the first access is top secret doesn’t mean that they can access all of the secret files.

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

For two labels to dominate each other they would have to be equal (the same level)

1. State informally what the Simple Security property says.

 Person S with clearance (Ls, Cs) has read access to object O with classification (Lo, Co) only if (Ls, Cs) >= (Lo, Co). The person has to have a higher or equal security clearance of the object and the document classification must be a subset of the persons

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

It is a dominance relationship, so one must have access equal or higher than the one labeled. If and only if assumes that the two clauses must be equivalent

**Lecture 9**

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

Simple security isn’t enough because a person of high clearance can violate confidentiality by writing important information to a lower level.

1. Why do we need constraints on write access?

So that confidentiality isn’t broken. Someone in top secret shouldn’t be able to write important information to unclassified.

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

Human beings are trusted not to write classified info where unauthorized people can access it, however malicious programs can leak information without human knowledge or consent.

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

Write access is granted to people writing objects to levels where the objects clearance dominates the persons.

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

They must be equal clearance levels.

1. How could we deal with the problem that the General (topsecret) can’t send orders to the private (Unclassified)?

Covert channels could help them communicate.

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

Yes. Even though it is a “write up” order, since this is a dominance relation the war plan should be classified to something that the corporal doesn’t have access to still.

**Lecture 10:**

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

Over time the classification of a document might change. There are times where a classification needs to be changed as a safety measure, but it can also cause a lot of harm if done incorrectly. Changing needs to be done in good spirit.

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

Because the inability to access some documents might hinder workflow of some people. If a document weren’t moved to a lower level, then workers would have to consult their manager to get that information.

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

 A person could potentially move a top-secret document to unclassified, spilling war plan secrets (something that shouldn’t happen)

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

 Subjects and objects do not change labels in a way that violates the “spirit” of the security policy. They can move subjects/objects up and down unconditionally as long as it is in good spirit.

**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?

Give all subjects Top Secret access with all classifications {crypto, nuclear, etc.}, and give the subjects access lower than top secret and subsets of the classifications

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

They can be huge! With many categories and access levels the matrix can be expensive. Instead you can just make a few rules for the entire matrix to follow.

**Lecture 12**

1. Suppose you had hierarchical levels L, H with L < H, but only had one category A. Draw the lattice.

L{} 🡪 L{A} 🡪 H{A}

 

H{}

1. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?

Greatest lower bound: L1 <= L2  <= …. <= Lx

Lowest upper bound: Lx >= Lx-1  >= …. >= L1

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

Upward flow is the metapolicy because any subject can write upwards and the subject should be able to read downwards if there is an upwards path. If no path exists upwards, then  the simple security and star property should prevent read and write accesses.

**Lecture 13**

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

Information is allowed to flow from Low to high, but not vice versa

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

You can only read if the object level is below/equal the subject level, and you can only write if the object is greater/equal to the subject

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

Create starts a new file if one with the same name doesn’t already exist, destroy deletes a file if the object file is higher than the subject

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

The two subjects have to be on different levels (high and low). Also, you need the create, destroy, read, and write commands.

1. Why is the DESTROY statement there?

You need to destroy so that the next time you transmit a value, the file isn’t there and you can create the file again. You can only create a file if it doesn’t already exist.

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

No, the contents are always the same. It just depends on what the Low subject sees based on what the high subject creates

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

 The Low subject simply sees what files the high subject is creating. Low does nothing other than observe files.

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

 Yes the high subject must do different actions to send a different bit. Depending on which files he creates determines which bit is seen by the low person.

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

The low subject may not ever have information channeled to him. This would only happen if a high subject was trying to transmit data downwards.

**Lecture 14**

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

Because two humans talking over coffee isn’t an illegal channel and is not in violation of the metapolicy.

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, this is not a covert channel because the Low-level subject will not be able to read the file. In both cases there will be an error message

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

In the error message.

4. In Covert Channel #2?

The processor clock

5. In Covert Channel #3?

The read head in the disk drive.

6. In Covert Channel #4?

in the code variable l, which depends on the value of h.

7. Why might a termination channel have low bandwidth?

Because they take up way more time to complete.

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

Power on/off a machine, file, or piece of hardware.

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

Radio or wave transmission. Sending a TV receiver a power or station change signal.

**Lecture 15**

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

 On real processors they can transmit thousands of bits per second! Also they leave no impact on the system.

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

No, it is infeasible for systems to eliminate all covert channels.

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

We could eliminate it by modifying the system implementation, reduce the bandwidth by introducing noise into the channel, or monitor it for patters of usage that indicate someone is trying to exploit it (intrusion detection).

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

 In creating/destroying files, or trying to create a file to see whether or not it exists.

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

The sender must be able to modify the attribute and the receiver must be able to view that attribute.

**Lecture 16**

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

It only provides information about the file and some attributes; it doesn’t actually allow you to read the object. It’s not important that you know something about the attribute; what’s important is that the operation tells you something about the attribute.

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

 Because that indicates that people from different access levels can reference and modify a piece of the system. It would signal a potential channel for communication.

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?

No, because the file existence, file size, and file level are all unrelated to each other, where as read, write, destroy, and create are related.

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

To help identify where potential covert channels might be. This would allow you to close, restrict, or monitor covert channels.