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?

The first and foremost form of security in my everyday life would have to be identity security: protection of credit information, social security information, etc. As an individual with little-to-no credit yet, identity theft has the potential to completely ruin my future. Another form of security would be physical-personal security: protection of myself and my physical belongings. For instance, hiding things in my car rather than showing them visibly hopefully reduces the chances of my car getting broken into. The final major form of security would be virtual-personal security: protection of my online accounts and my stored data. These are pretty self-explanatory but in today's age a breach in certain online accounts can practically cause breaches into other accounts if you are not practicing good security.

2. What do these have in common?

They all are intended to ensure the well-being of my future. Identity security and online security both fall relatively close in the confidentiality of my information. Personal security helps reduce harm to myself either physically or financially through reduction of actual crimes being committed against me.

3. Have you been a victim of lax security?

Yes, just recently my mother had my birth certificate and social security card in her purse. She left her purse in her car and it was stolen. The combination of a valid birth certificate and social security card is incredibly scary when it comes to identity theft. I immediately subscribed to identity protection and daily credit checks to make sure my identity is not stolen.

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

Minimal. Answer to second question is in #5.

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

I have pretty stringent security policies for my laptop. First, I run one of the least used major operating systems for everyday consumers (linux); this is my operating system for most of my day-to-day use. I use Windows typically for games or windows-specific applications. While this doesn't actually make me *secure*, it reduces my chances due to less consumers actually using it. Hopefully I'm not infected with Hand of Thief. Considering most of my interaction with the day-to-day world is through the internet, I by-default have javascript disabled for websites and require permissions for java applets to be run; additionally, I attempt to avoid areas of the internet that promote virus transmission. And finally, I keep a minimal amount of personal data on my computer and bi-annually wipe the operating systems and use fresh installs.

6. Do you think they are probably effective?

For all intents and purposes they are effective enough. These measures don't limit my

usability incredibly and as long as I practice common sense when browsing the internet.

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

I think that technical experts on the matter probably have a better sense of the situation than I do. However, as previously a DoD researcher for 1.5 years that worked on classified material, I am almost positive there are systems people could not access. Computer systems with no internet access, heavily encrypted, and security-hardened in vaults with no phones allowed, cameras, or even mp3 players are most likely untouchable by adversaries. Even if a virus is brought in, the information would have a tough time getting out. Of course there are situations where information could be leaked; air gap jumping viruses would especially be an issue. I think the quote from the FBI is describing the fact that it is *possible* not actually probable.

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

I think that at the very least understanding the hazards that come with computers is incredibly important in order to protect yourself. How can you protect yourself from vulnerabilities if you don't even understand what they are?

Lecture 2

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

Additionally, one could say that a determined person with nefarious intentions can study your system from the outside for as long as they want. The five reasons covered everything else rather well though.

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

No. Learning about security and understanding the inherent vulnerabilities to certain types of systems helps you enumerate *some* of the bad things; however, one cannot *practically* know everything that could happen: computer systems are too complex from hardware all the way up to software.

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

The defender has to think of every possible vulnerability with a system in order to keep it safe. An attacker has to only find one vulnerability in a system in order to conduct malicious activities. Defenders also typically don't spend all their time combing over the system for vulnerabilities; however, a dedicated attacker has virtually unlimited time to spend.

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

Yes and no. Preventing *all* possible attacks is impossible because there is simply too many parts to a computer and the system that is built on top of it. From physical vulnerabilities to virtual vulnerabilities, it is impossible to protect completely. It is *probably* possible to protect against all practical attacks. For example, people probably won't storm your building with ak47s as it is not practical; however, people may try and enter your building by just walking in.

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

If you increase the amount of interfacing with a system (functionality increase), you also increase the amount of vulnerabilities that a user could possibly exploit because there are more sections of the system that they have access too. Additionally, adding more checks, encryption, etc increases bloat and therefore decreases efficiency to complete tasks.

Lecture 3

1. Define “risk”?

The possibility of a system being exploited by a user with malicious intent and the losses that are associated with said exploit.

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

Yes, as stated by the ideas of risk acceptance, risk avoidance, risk mitigation, and risk transfer. Essentially, having a completely secure system is impractical and resource expensive; however, building security to reduce losses and simply accept the remainder of said losses can be O.K. For instance, losing the personal information of a million users to an attacker is *very* bad and should be avoided at all costs; however, software pirating is normally tolerated as an accepted loss and therefore many high end studios (read: Adobe) don’t care very much as long as it is on a personal level.

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

I accept that my packaged software will probably be ‘cracked’ and released for free; as long as corporations don’t operate under those pretenses I don’t care. Therefore, I don’t put incredibly sophisticated and expensive DRM on my software. I want to avoid having my customers’ information released to unauthorized users and therefore restrict remote logins and use a whitelist for IP access. I encrypt customer’s information because if it is stolen the losses will still be mitigated. I use services like CloudFlare to reduce my chances of denial-of-service attacks taking down my online services. This transfers some of the risk to the external service.

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

The probability of something bad happening isn’t necessarily a good risk management tool because something with a large immediate loss can be a *lot* worse than something with a small long term loss.

5. List some factors relevant to rational risk assessment.

Are the potential losses high enough that it could impact me more than the costs it would take to prevent the security measure? This includes PR issues, direct financial loss, technical loss, etc. In reality, there are a multitude of factors that are involved in risk assessment and it completely depends on the context.

Lecture 4

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

Slide 2 discusses the goals of security; slide 3 discusses the methods used to achieve said goals.

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

Typically, for the everyday consumer, confidentiality is the most important. I don't want my social security information, credit information, etc released to those that I do not authorize to have it.

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

To group data that is associated in some way. For instance, if pieces of material are related to the same topic or sensitivity then they would be under the same category.

4. Why might authorizations change over time?

Authorized users leave or step down from positions, new people can join, etc.

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

There are exploits that can deny availability; the goal is to secure the system from these exploits.

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

Non-repudiation and authentication would be especially important in any sort of e-commerce situation. I do not want users to be able to deny that they purchased items if they really did AND I do not want unauthorized users making purchases with my customers' accounts.

Lecture 5

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

A cell phone network doesn't a nefarious user destroying the integrity of the system. For example, they do not want someone hijacking the cell towers and broadcasting a message to local cell phones. Therefore, a metapolicy would probably be "uphold the integrity of the cell tower system". A military database is particularly worried about confidentiality of the data; for example, intelligence data gathered is something that the military wants to keep confidential. Therefore, a metapolicy would probably be "disallow the leak of critically sensitive information".

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

A metapolicy really just describes the goal of security, whereas the policy describes how you plan on implementing the metapolicy.

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

1. Any grade change after final grades have been posted must have explicit approval from the dean of students. 2. Any release of information of a student's academic records must be done with the explicit approval from the student himself/herself. 3. Professor's only have authority over the grades of a student within their own class.

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

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

Students critically sensitive personal information should not be viewed by unauthorized users.

6. Explain the statement: "If you don't understand the metapolicy, it becomes difficult to justify and evaluate the policy."

The metapolicy describes the goal you want to achieve. If you don't understand what you want to achieve, then how could you implement a policy to achieve it?

Lecture 6

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

The military does not want the schematics and experimental data about their technologies to be released. Such a release could result in effective countermeasures against their technologies. Additionally, any intelligence that has been gathered could be considered useless if an unauthorized user gains access to it. Regarding integrity, the military does not want anyone writing new launch codes to their missiles or writing commands to a drone. Availability would be in regards to communications; soldiers deployed in the field want to be able to securely communicate with command in case of any emergencies.

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

An unauthorized user gaining access to information they should not be able to see.

3. Why do you think the proviso is there?

Adding integrity and availability into the mix complicates the thought experiment and doesn't allow us to fully flesh out the issues with confidentiality.

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

The labels consist of 2-parts. The first part is taken from a linearly ordered set of sensitivity levels. The second part compartmentalizes the information based on the category of the information.

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

How the labels get there would be a part of integrity. Currently, we are concerned just about access to the information (confidentiality).

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

LEAST SENSITIVE -> MOST SENSITIVE

{1, 2},{4,5},{2},{6}

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

1. { Unclassified, {} }
2. { Top Secret, { War Plan } }
3. { Unclassified, {} }
4. { Confidential, { Personnel Records } }
5. { Confidential, { Personnel Records } }
6. { Top Secret, { Intelligence } }

8. Justify the rules for "mixed" documents.

Documents that are mixed should adhere to the highest level of sensitivity contained within it because someone should not be able to see information in a document that isn't appropriate to their level. Someone with the highest sensitivity in the document would be cleared to see all of it anyway. Documents with different categories should also only be shown to those that are need-to-know for all of the categories.

Lecture 7

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

ID Badges, Thumprinting that correlates to a database, etc. Some form of identification and authentication.

2. 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.

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

Files, systems, databases, anything that you would need a certain permission level to access.

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

Individuals should not be given more power than needed. Even if they never plan on using it, a nefarious individual can exploit that individual into given them information. Leaks will always happen, the more information a user has access to the worse the leaks would be.

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.

1. The user should have access because they are need-to-know on crypto and they have equal or higher clearance compared to the document. 2. the user should not have access because even though they are need-to-know on crypto they do not have equal or higher clearance compared to the document. 3. there is not need-to-know category and the user has equal or higher clearance.

Lecture 8:

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

actions?

To create concrete terms in order to establish a relationship between them in the context of security.

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

dominates is reflexive because it includes “or equal to” for clearance and a set can be a superset of itself. dominates is transitive because if a dominates b and b dominates c, then a dominates c. dominates is antisymmetric because two documents cannot dominate each other unless they have equivalent labels.

3. Show that dominates is not a total order.

Dominates cannot be a total order because two documents have the possibility for neither to dominate each other. For example, if a document is {H, {A,B}} and another is {L, {B,C}}, neither document dominates.

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

The two labels are equivalent.

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

If the subject’s clearance dominates the object’s clearance, then the subject has read access to the document.

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

if and only if actually takes two conditionals while only if takes one. IFF is bidirectional

Lecture 9

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

Simple security doesn't take into account write access. If someone with top secret clearance writes top secret information and puts it into a lower clearance folder then confidentiality is violated.

2. Why do we need constraints on write access?

Individuals are ideally supposed operate under the assumption of proper writes. However, we need constraints for computer systems to make sure it doesn't happen. If a program has a malicious piece of code, we need a system to disallow a write from high level to low level.

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

Computers follow commands blindly, humans have the ability to reason.

4. State informally what the *-Property says.

A subject can only write to clearance levels equal or higher to their own.

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

Both the object and the subject must dominate each other.

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

Have a separate system for classifying orders and sending it down the chain that is separate of document control.

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

Yes it is a problem, however that is integrity control. Simply implement a version of MLS for integrity in addition to confidentiality.

Lecture 10:

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

According to the weak tranquility property, a subject's level can go up and down because it doesn't violate the spirit of the security policy.

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

Subjects may require higher or lower levels of security as time passes. If the military is operating under the principle of least privilege, the privilege may change often.

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

Objects can contain highly sensitive information that shouldn't be downgraded even if the rest of the

document should.

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

All of the information must be cleared to be able to go down a level OR information must be redacted.

Lecture 11:

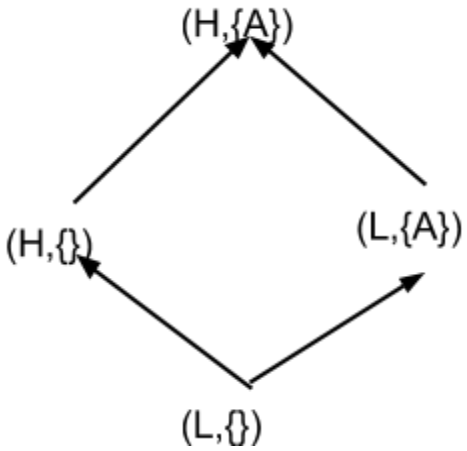
1. Suppose you wanted to build a (library) system in which all subjects had read access to all files, but write access to none of them. What levels could you give to subjects and objects?

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

The access control matrix would be really large and it would be much more efficient to compute the access on the fly.

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?

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

The metapolicy is what we really care about, and the metapolicy for any BLP system is to constrain the flow of information among the different security levels. Therefore, if information only flows upwards than that is the metapolicy.

Lecture 13

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

example on slide 1.

The idea behind BLP rules are to enforce the metapolicy. BLP rules are used to restrict the flow fo information.

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

READ operations satisfy BLP because no information is given to a lower level subject if they request a READ. They do not even get a response that could tell if object O exists. WRITE operation satisfies BLP because information is only flowing upwards.

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

CREATE operation only "creates" information at the subjects level. DESTROY operation only modifies information higher than its level.

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

The lower level subject has to perform the exact same steps in order to verify the data that they received from the higher level subjects before doing anything else.

5. Why is the DESTROY statement there?

So the process can be indefinitely repeated.

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

The contents are not necessarily different. The read operation is what gives the different return value. High level subject can write a 1 to the file; however, the lower subject will read a 0 because it doesn't have acess.

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

Because SL can't receive what SH did until they perform the exact steps given.

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

Yes it must. SH does different things to signify different bits.

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

Communication is essentially registering differences between information; therefore, differences in observable actions can be used as communication.

Lecture 14

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

Covert channels by definition use system resources that were not designed for communication

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)

No because the lower level subject can't detect a difference as they will always just receive a zero when attempting to read the file.

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

The bit of information resides in the different error messages.

4. In Covert Channel #2?

Within the timing of tasks on the processor.

5. In Covert Channel #3?

Within the order of the requests on the disk drive from SH and the order of requests processed on the disk drive for SL.

6. In Covert Channel #4?

Whether a branch is taken or not is used to communicate a bit.

7. Why might a termination channel have low bandwidth?

It requires a longer amount of time to communicate a bit of information as if it doesn't terminate then you have to wait for the whole process to start back over again. so instead of thousands of bits per second, you are looking at maybe 1 bit per second or so.

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

A change in power based on computations of SH and access to the power levels for SL.

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

Hardware devices that change power consumption based on the computation. smart cards, etc.

Lecture 15

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

Covert channels can have minimal impact on the system and transfer at almost thousands of bits per second.

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

The more attributes you remove from being referenced by the receiver or remove from being modified by the sender, the less your system can actually do.

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

Modify the system implementation, reduce bandwidth by introducing noise, monitor for patterns that indicate someone is trying to exploit it.

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

A Sender has the ability to modify a system attribute that a receiver has the ability to reference. The attribute is continuously changed and the receiver notes the differences.

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

See answer 4.

Lecture 16

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

Because the file either already exists or it will exist after the create operation. therefore, no reference to file existence.

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

The ability to note a change in an attribute {R} along with the ability for a higher level subject to modify the attribute {M} means that there is the possibility for a channel to happen.

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 a receiver cannot reference the same attribute that has the potential to be modified.

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

To identify potential covert channels.