**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?

   Personal information is exchanged everyday via the internet or computer programs, such as retail websites or online banking/ATMs respectively. Personal security, homeland security and communications security are a few that are relevant everyday to individuals.

2. What do these have in common?

   They all want their assets to be protected against threats. Those threats can be of many different types.

3. Have you been a victim of lax security?

   Yes. Recently many websites have had their data compromised (Heartbleed) and those have compromised my data.

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

   Pretty high. Considering how many new and unique malware samples were discovered in 2009, one can only guess five years later there are even more. Also, since there is no way for a machine to be 100% secure, and since a machine usually stays infected, it wouldn't be shocking to learn my laptop is infected.

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

   I have a firewall, anti-spyware software, a password required at login and upon awaking from sleep mode, and my data is encrypted.

6. Do you think they are probably effective?

   They are probably mostly infected, but if someone were determined to hack into my personal computer to gain access to my information, I imagine it could be done.

7. Consider the quote from the FBI official on slide 10. Do you think it overstates the

case? Justify your answer.

I don't think it overstates the case. A great deal of our country's government requires secrecy and privacy of data from both citizens and potential threats to the country. Especially concerning military plans and insecurities, exposing classified documents and data could leave the country and it's citizens vulnerable to an attack.

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

Being aware of ways information can be stolen or changed allows you to make it more difficult for a hacker or bug to attack you. Nothing is 100% guaranteed, but by making it more difficult, it lowers the percentage of attacks that leave you vulnerable.

**Lecture 2**

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

Most people are uneducated about security vulnerabilities, and the most heavily used operating systems aren't the most secure.

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

There are ways to prioritize one "bad thing" over another based on which would cause the most risk. If there is a risk that happens three times everyday and causes a company to lose $1000 every time it happens, that would take priority over a problem that could lose $100 every 20 years. On the other hand, something that is only estimated to happen every 100 years but will bankrupt the company would also be an important problem to fix.

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

There are significantly more attackers than defenders. The defender must think of every single way an attacker could possibly compromise the system while the attacker only needs one loophole.

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

I do agree that one way to completely assure computer security is to never use one. However, there are also way to make that risk minimal by educating yourself on how to protect yourself and your computer.

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

To fully equip a program or system from all attacks a defender could think of, it might require a system to run slow, or for the user to do too many security checks before use that business is lost. So the tradeoff is for usability, speed, and accessibility in exchange for heightened security.

**Lecture 3**

1. Define "risk"?

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

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

Yes.

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

Accept: I could pay for home insurance my entire life and never use it. Avoid: Not driving down the highway at 3 am on New Year's to avoid drunk drivers. Mitigate: Putting valuables out of sight when parking car. Transfer: Purchasing car/home/travelers insurance.

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

The ALE is total loss over a year based on how often a risk occurs and how much it would cost. It does a good job of putting smaller cost, high frequency risks into perspective, but diminishes risks that are rarer, but very expensive.

5. List some factors relevant to rational risk assessment.

Take actions based on the assumption a risk will happen at some point. So for the rare, but expensive threat, still make that risk a priority.

**Lecture 4**

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

The list on slide 3 (mechanisms) is ways to accomplish the list on slide 2 (goals).

2. Consider your use of computing in your personal life. Which is most important:

confidentiality, integrity, availability? Justify your answer.

Confidentiality because of personal information used on the internet, like online shopping and schoolwork

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

It means to assign a category (crypto, nuclear etc) and a clearance (top secret, secret, etc) so it's easier to control who has access to which files.

4. Why might authorizations change over time?

More people might need access, or gain/lose clearance.

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

To be available your program or website, etc must be reliable. And when your program is reliable, generally, it's available to whoever it needs to be.

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

In online retail, you want to be sure you're giving money to who you think you are, and also need the retailer to not deny they charged you.

**Lecture 5**

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

Customer's data is held as secure as possible and only viewable by those needed to do their job.

Confidential documents are shared and viewed on a need to know basis.

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

Because you need to have particular processes to accomplish your larger goal.

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

Only the registrar's office can change a grade. Students can see their own records at any time. Students cannot see other student's academic records.

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

Yes, it could. Perhaps, a business would want to see evidence of profit before investing in a certain project. That may require seeing financial records and otherwise confidential documents and now there's a conflict.

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

The goal is to keep students social security numbers confidential to prevent identity theft on the part of the university.

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

If you don't understand the motive behind a certain rule, that rule seems frivolous and unnecessary.

**Lecture 6**

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

The military is primarily concerned with who has access to their information because the wrong person with a confidential document could cost loss of lives and money. Integrity and availability are also important but is secondary.

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

A person viewing documents they're not authorized to see.

3. Why do you think the proviso is there?

To simplify the experiment.

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

There are linear confidentiality levels from top to bottom: Top Secret, Secret, Confidential, and Unclassified. Then also "need-to-know" partitioned from an unordered list: crypto, nuclear, janitorial, personnel, etc.

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

Because the labels are less important than the sensitivity of the documents and it's done by a security officer.

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

Lowest to highest sensitivity: Unclassified: 3, 1, Confidential: 4, 5, Top Secret: 6, 2

7. Invent labels for documents containing each of those facts. 8. Justify the rules for "mixed" documents.

Leisure, Human Relations, Intelligence, Armed Forces. For "mixed" documents, if someone has half the clearance (say Top Secret Crypto, but doesn't have the clearance for Top Secret Nuclear) they would see top secret information from a different department. The point of the sensitivity system is to keep sensitive knowledge as private as possible, which cannot happen if you allow documents to be viewed with only partial clearance.

**Lecture 7**

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

Humans are labeled by clearance and are authorized to view that level and below.

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

Levels for document are able to be viewed if you are cleared to that level or above. For humans, it's the opposite. You can view all documents in the category and below.

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

Files. Information.

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

This allows everyone to have all the information they need to work, while also not having any extraneous information they could leak. If a leak does occur, the number of people with access is much lower.

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 person is cleared to a level above the document in crypto. Makes sense.

2. The document is a level above the person. Makes sense.

3. The person is cleared to two levels above document. Makes sense.

**Lecture 8:**

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

   To clarify the following examples

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

   Dominates: If X1 >=X2, then X1 dominates X2.

   X1<=X1, then X1 dominates X1

   If X1 dominates X2, and X2 dominates X3, then X1 dominates X3

   If X1 dominates X2 & X2 dominates X1 then X1 = X2

3. Show that dominates is not a total order.

   Dominates is not a total order because for some pairs, neither dominate the other.

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

   (L1, C1) >= (L0, C0)

5. State informally what the Simple Security property says.

   Someone can only read a document if the persons clearance is higher or equal to the document label and classification.

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

   There may be other security constraints in place that stop you from viewing the document.

**Lecture 9**

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

   Because it only defines read permissions and write permissions are ignored.

2. Why do we need constraints on write access?

To protect the integrity of documents so they aren't changed and to make sure something isn't copied and change the labels.

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

It's easier to determine the security of one person, rather than that person and all programs running at one time.

4. State informally what the *-Property says.

A subject can write to their level or above. They can't write down.

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

It must be the exact level of the subject's clearance.

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

The biggest issue prevented by the "no write down" rule is that of subject interfering with the unclassified message to be sent. So, we're worried about programs/other subjects leaking classified information separate from the message. A way to ensure that doesn't happen is to cut out any subjects that could alter the message. So, don't send it digitally, and don't send a messenger who could change your original message. Deliver the message in person.

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

The only way to overwrite the war plan is to have access to a file which you can't read. So if you don't have permission to read the object, you also don't have access to it. (Meaning if you can't open the folder, you also can't hold/touch the folder. This way no information can be altered.)

**Lecture 10:**

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

As circumstances change, a certain object/subject may need to be changed based on how important that information is at the time or on what that subject needs to know to do their job.

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

   As time goes on, certain facts come to light (whether intentional or not) and certain information is no longer dangerous for lower level clearance to know. For example, if a document labeled "top secret" in 1925 was downgraded to secret or even classified, the chances it would adversely affect a persons livelihood is low even though that wasn't the case in 1925.

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

   The government possesses many documents could directly impact lives of soldiers or officials. Even ignoring obvious war plans and military information overseas, much of the white house operates under classified information in the event of a malicious attack. If this information was at a lower classification, this leaves white house staff and the president vulnerable.

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

   The object must not contain any information that would be harmful if downgraded. It's also not beneficial if the security is the same. The only time it's preferable to downgrade an object is if it is more beneficial (from a security perspective, not a malicious attacker's perspective) at a lower level than at a higher level.

**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?

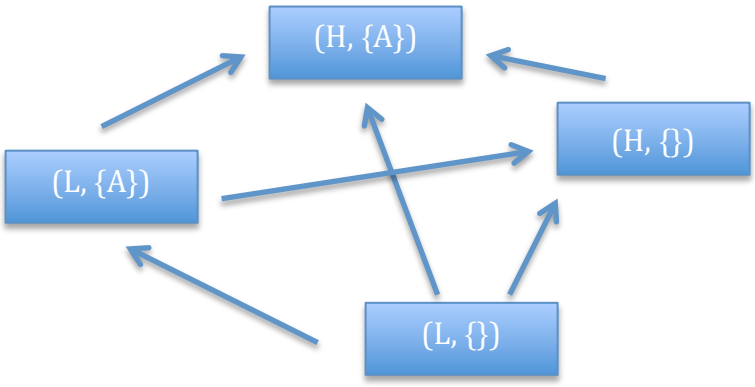
   Each subject would have H clearance in all categories, and each object would have L clearance with any combination of categories.

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

   Because the number of subject and objects would create too big of a matrix, and because the access can be computed on the fly due to simple rules which together make the matrix unnecessary.

**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?

   The GLB is the element with the most arrow tails and the LUB is the element with the most arrow heads. So in the diagram above: GLB = (L,{}) and LUB = (H, {A}).

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

   Because upward flow makes sure confidentiality is protected.

**Lecture 13**

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

   Information is only supposed to flow upwards which is equivalent to "read down" and "write up".

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

   The read instruction makes sure the object exists and that the subject dominates the object's level before returning value. If these conditions aren't satisfied, it returns 0. The write instruction makes sure the subject's level is below the objects, and only writes under these constraints. Both conditions satisfy BLP.

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

Both operations make sure to not read up, or write down.

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

The lower level subject must perform the same sequence of tasks.

5. Why is the DESTROY statement there?

To allow this process to be repeated with different information being passed.

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

Yes, in one path there exists an object F, in the other it doesn't exist.

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

SL must do the same thing in both cases because the lower subject is the control. The message can only be transmitted if the lower subject does the same thing.

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

The higher subject must do different things depending on which bit of information wants to be sent.

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

The metapolicy states that no information should leak from the top to the bottom level of a system. Through this process, a bit of information is leaked depending on whether SH creates a file, so the metapolicy is violated.

**Lecture 14**

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

Because the flow of information is not "within the system"

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 in both situations, the lower subject can't see the document.

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

Storage

4. In Covert Channel #2?

Timing

5. In Covert Channel #3?

Both

6. In Covert Channel #4?

Control flow

7. Why might a termination channel have low bandwidth?

Because it either ends or it doesn't

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

The high level subject can modify power and the low level subject can sense the power.

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

Smartcards where energy is supplied by host computer

**Lecture 15**

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

Because there can be thousands of bits per second transmitted without any impact on system processing.

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

Because there are too many ways for a covert channel to exist

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

You could change the system, make it noisy, or monitor it.

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

   Both sender and receiver must have access to some attribute of a shared object. The sender must be able to modify the attribute. The receiver must be able to reference (view) that attribute. A mechanism for initiating both processes, and sequencing their accesses to the shared resource, must exist.

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

   The sender can either create a file or not. The receiver then attempt to create the same file, write a 1 to it, then read it and destroy it. If a 0 is returned, the sender created the file. If a 1 is returned, the sender didn't create the file.

**Lecture 16**

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

   Create doesn't directly tell you that a file exists. It's implied.

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

   Because it means that someone can modify and another can reference it, meaning it has the potential to be a 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, because it would indicate different stages would have different access capabilities.

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

   It shows parts of a system that should be monitored for a possible leak of information.