     Name: Luis Delgado

     EID: LED625

     CS Login: LDELGADO

     Email: luisdelgado24@utexas.edu

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 every

day life? *Personal security, Homeland security, Communications security*

2. What do these have in common? *The protection of assets from threats*

3. Have you been a victim of lax security? *Yes, a personal computer I once had was attacked by a virus due to my negligence for not installing virus protection software*

4. What is the likelihood that your laptop is infected? How did you decide? *Very likely given that programs that run under my consent may lead to infection without me having consented it. From the moment I started using my computer it has been “at risk”*

5. What security measures do you employ on your laptop? *I try to avoid falling for pop-ups or other traps that may lead to malware. I do not install Virus Protection Software anymore given the virus-protection success rate of my OS (MAC)*

6. Do you think they are probably effective? *I think that Virus Protection Software is effective up to a certain degree. If the developers did not anticipate a certain breach then the system might still be corruptibles*

7. Consider the quote from the FBI official on slide 10. Do you think it over-states the case? Justify your answer. *Not at all, much of the country’s most-sensitive information is stored digitally, and more precisely, online. So it is at a constant risk of putting our country in serious trouble.*

8. What is the importance in learning about computer security? *You are able to improve your personal security and contribute to protecting other systems.*

Lecture 2

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

factors? *Hackers with different abilities, from all around the world unite in the task of attacking your system. It’s you against an army of hackers. Tough.*

2. Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not? *There’s no fixed number, you never know which new bug someone might find eventually.*

3. Explain the asymmetry between the defender and attacker in security. *The defender has to worry about finding all possible flaws in the system while the attacker just needs one weakness in the system to penetrate it.*

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not? *Yes, a computer system is vulnerable at all times. The only way to absolutely protect it is to not use it.*

5. Explain the statement on slide 8 that a tradeoff is typically required. *Attempting to guarantee security in a system may take a burden on performance, usability or other aspects. It might slow down some processes of the machine or it might keep certain applications from becoming available to the user in order to “protect” That’s the tradeoff.*

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? *Yes, trying to maintain functionality while assessing potential threads in whatever way is best.*

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer? *Accept: Driving, Avoid: Texting and driving, Mitigate: Carrying a spare tire, Risk transfer: Own car insurance*

4. Evaluate annualized loss expectancy as a risk management tool. *It is a powerful tool but probably deceiving at times given that it deals with probability. If you happen to be betrayed by destiny and you had gone with the “most-likely” answer from the ALE analysis you might be in dangerous grounds.*

5. List some factors relevant to rational risk assessment. *How much exposure there is to risk, level of protection, probability.*

Lecture 4

1. Explain the key distinction between the lists on slides 2 and 3. *Slide 2 shows aspects or general sub-categories of security (meta-policies), while slide 3 shows lower-level parts of security, which may form part of policies.*

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer. *None is more important than the others. I.E. I need my bank not to publish my financial information, my social networks not to allow anyone else to write on my behalf, and my online retailers to be available when I need them.*

3. What does it mean “to group and categorize data”? *To divide information onto piles, where each pile represents a level of security so that the whole pile has the same level.*

4. Why might authorizations change over time? *People might gain access to classified information due to promotions, for example.*

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related? *By contrast, unreliability leads to a lack of security given that a given moment if a user wants to access a piece of data that becomes unavailable there may be security consequences.*

6. In what contexts would authentication and non-repudiation be considered important? *For making payments you would probably want non-repudiation to not occur, given that you want the other party to acknowledge you made a payment. And authentication could come into play when it comes to logging in to a personal email account.*

Lecture 5

1. Describe a possible metapolicy for a cell phone network? A military database? *For a cell phone network the metapolicy could be to provide availability so that customers can always make calls. For a military database I think it should be confidentiality due to the sensitivity of the information*

2. Why do you need a policy if you have a metapolicy? *The policy is the actual set of mechanisms that have to happen in order for the metapolicy to take place.*

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

\* *If you want to change a student’s grades you need to log in*

*\* (After logging in) You need to submit a petition to change it, which will be approved by the department*

*\* Grades may not be changed after a certain period of time*

4. Could stakeholders’ interest conflict in a policy? Give an example. *Definitely, a student whose grades are being secured by the University’s system, might want to change them, which would conflict with any policies that have to do with integrity*

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

6. Explain the statement: ”If you don’t understand the metapolicy, it becomes difficult to justify and evaluate the policy.” *Without knowing what the big picture is, a simple policy might be senseless. Having to log in into a website might be senseless if the user does not know there is some information trying to be protected*

Lecture 6

1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability? *There are different levels of trustworthiness and the system needs to account for that. Integrity and availability may be minor compared to confidentiality in military security*

2. Describe the major threat in our MLS thought experiment. *Letting a lower-level military person gain access to higher-level information*

3. Why do you think the proviso is there? *If the subject’s level of confidentiality reaches the document’s level, then it can be read.*

4. Explain the form of the labels we’re using. *Unclassified, Confidential, Secret, and Top Secret. From lowest to highest ranking.*

5. Why do you suppose we’re not concerned with how the labels get there? *There is a system for that which is handled differently. Only people who are eligible to write and/or assign labels can do so.*

6. Rank the facts listed on slide 6 by sensitivity. *Base softball team has a game tomorrow at 3pm, cafeteria is serving chopped beef, Col. Smith didn’t get a raise, Col. Jones got a raise, British have broken the German Enigma codes, Normandy invasion is scheduled for June 6.*

7. Invent labels for documents containing each of those facts. *Recreational, Merits and Honors, Strategic*

8. Justify the rules for “mixed” documents. *You can never put a jeopardy any information that an individual is not allowed to see. So even if they can see the rest of the packet, it won’t become accessible to them because they can’t see everything that it contains.*

Lecture 7

1. Document labels are stamped on the outside. How are “labels” affixed to humans? *Each person gets an “authorization level” granting access to that-level-type information.*

2. Explain the difference in semantics of labels for documents and labels for humans. *A human label represents the degree of trustworthiness to which they have been vetted. A document label represents the security type of individuals that can read it.*

3. In the context of computers what do you think are the analogues of documents? Of humans? *Documents can be files that can be read. Humans can be programs that are trying to perform an action on those files.*

4. Explain why the Principle of Least Privilege makes sense. *Because people cannot leak what they don’t know. It’s a way of protecting information*

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 first one makes sense because that person has access to even higher-level type of information, so they get access as well to this document. For the second one, they don’t have ‘top secret’ access to crypto nor any type of access to nuclear information. So, denied. For the last one, ‘secret’ access to nuclear information is a super set of the ‘unclassified’ empty set. So they get access.*

Lecture 8:

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

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

*A category “X” dominates itself by reflexivity;*

*if A dominates B, and B dominates C, then A dominates C by transitivity;*

*A category “X” may be dominated by a superset by anti-symmetry;*

3. Show that dominates is not a total order. *Dominates is a partial order thanks to the reflexive, transitive, and anti-symmetric properties.*

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

5. State informally what the Simple Security property says. *A person can read a document if they have access to that document’s category and if they can read at that security level of information or higher.*

6. Explain why it’s “only if” and not “if and only if.” *It’s necessary that the subject-level dominates the object-level but it is not sufficient as there may be other constraints in the system that prevent the read from happening even if SS would allow it.*

Lecture 9

1. Why isn’t Simple Security enough to ensure confidentiality? *Someone with read access can write it onto an ‘unclassified’ folder, leaving it for anybody who’s clearly not qualified to read*

2. Why do we need constraints on write access? *So secret information does not end up somewhere that can be read by people who are not classified.*

3. What is it about computers, as opposed to human beings, that make that particularly important? *Some program I run may have embedded malicious logic (a “trojan horse”) that causes it to “leak” information without my knowledge or consent.*

4. State informally what the \*-Property says. *A person can write a document if they have access to that document’s category and if they cannot read at that security level of information or higher.*

5. What must be true for a subject to have both read and write access to an object? *Both, categories and classifications must match*

6. How could we deal with the problem that the General (top secret) can’t send orders to the private (Unclassified)? *The General can find a different streamline of communication to make the message get to the private*

7. Isn’t it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that. *That is a problem of integrity not of confidentiality.*

Lecture 10:

1. Evaluate changing a subject’s level (up or down) in light of weak tranquility. *Subjects and objects may change labels in a way that does not antagonize the general “spirit” of the security policy*

2. Why not just use strong tranquility all the time? *Because there may be occasions where a particular label may be changed while the system remains balanced.*

3. Explain why lowering the level of an object may be dangerous. *Because people who should not have access to read the object may now have it.*

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure. *All lower-level subjects’ level must be at least on the same level as the new level of the object (no one should gain access if they are not allowed). The meta-policy must still hold.*

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 have high-level security and all objects are low-level security*

2. Why wouldn’t you usually build an access control matrix for a BLP system? *You can compute the dominates for a particular relationship on-the-go and it is quicker*

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.)

L {} ––> L{A} ––––

▼ ▼

H{} ––––––––> H{A} *Left out reflexive arrows*

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB? *In order to find the LUB of X you find the set of labels and categories that immediately dominates X even though transitivity allows for other sets to dominate X. In order to find the GLB you find the set of labels and categories that X immediately dominates even though transitivity allows X to dominate other sets.*

3. Explain why upward flow in the lattice really is the metapolicy for BLP. *Because of the principle that information may flow up and not down due to the confidentiality restraints having to do with authorization levels.*

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1. *Simple Security takes care of allowing reads of information to be done downward (so information itself can never be flowing from H to L), and the \* property makes information writes to be done upward (L can write to L). This way the system remains balanced and confidentiality is not jeopardized.*

2. Argue that the READ and WRITE operations given satisfy BLP. *Read won’t happen unless the level of the subject dominates the level of the object, and write won’t happen unless the level of the subject is dominated by the level of the object. This satisfies BLP.*

3. Argue that the CREATE and DESTROY operations given satisfy BLP. *They satisfy BLP because the CREATE won’t succeed if a file with the same name already existed and the DESTROY won’t succeed if no file with that name existed.*

4. What has to be true for the covert channel on slide 5 to work? *The subject must have access to perform those commands*

5. Why is the DESTROY statement there? *To basically undo the creation of SL or, if it wasn’t created (meaning SL was already there) it destroys that one.*

6. Are the contents of any files different in the two paths? *It depends on whether a Create is successful or not (basically whether the file existed beforehand or not)*

7. Why does SL do the same thing in both cases? Must it? *It tries to create, write, read, and destroy an object in both scenarios to see whether it succeeds when a higher-level individual created the same object before and when they didn’t*

8. Why does SH do different things? Must it? *The high-level individual didn’t execute a “create” in the second chart. The individual can decide whether to execute it or not*

9. Justify the statement on slide 7 that begins: “If SL ever sees...” *If different things happen depending on a higher-level subject’s actions, that can allow information to flow downward meaning a lower-level subject gets access to something they shouldn’t*

Lecture 14

1. Explain why “two human users talking over coffee is not a covert channel.” *The flow is within subjects within the system. We care about using the mechanisms of the system to implement the flow.*

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 SL does not get any type of information based on what SH did. In both cases READ will fail because SL does not have access to that info.*

3. Where does the bit of information transmitted “reside” in Covert Channel #1? *The bit of information resides within the system state*

4. In Covert Channel #2? *It resides in the ordering or duration of events on the system*

5. In Covert Channel #3? *It’s not clear whether it’s a timing channel or a storage channel but q receives a value from p depending on p’s most recent read.*

6. In Covert Channel #4? *The end value of L depends on the value of H so the control flow of the program gives information based on what if statement was executed.*

7. Why might a termination channel have low bandwidth? *One possibility could be because of noise that slows down the flow of information*

8. What would have to be true to implement a power channel? *The energy that is consumed by a channel must be able to be measured*

9. For what sort of devices might power channels arise? *For devices that would benefit based on the measurement of its consumed energy*

Lecture 15

1. Explain why covert channels, while appearing to have such a low band-width, can potentially be very serious threats. *Because there may be other factors such as noise that can be threatening the channel.*

2. Why would it be unfeasible to eliminate every potential covert channel? *Too many possibilities for you to detect all of them. “You don’t know about it until you know about it”*

3. If detected, how could one respond appropriately to a covert channel? *We can eliminate it by modifying the system implementation, reduce the bandwidth by introducing noise into the channel, and/or monitor it for patterns of usage that indicate someone is trying to exploit it.*

4. Describe a scenario in which a covert storage channel exists. *If a receiver references a piece of information that based on the data returns different things, information would be flowing through a path that shouldn’t allow this.*

5. Describe how this covert storage channel can be utilized by the sender and receiver. *The receiver is always listening for when the sender makes changes in the channel while the sender has the ability to make changes at any given time.*

Lecture 16

1. Why wouldn’t the “create” operation have an R in the SRMM for the “file existence” attribute? *Because creating a file means a modification in existence, it does not have anything to do with referencing the file.*

2. Why does an R and M in the same row of an SRMM table indicate a potential channel? *Because it represents that for that attribute there is a mechanism by which someone can modified it and someone can reference it (what is needed for a covert channel to exist)*

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 the behaviors are different.*

4. Why would anyone want to go through the trouble to create an SRMM table? *It suggests place(s) where to look for covert channels (even though it does not identify them)*