Name: Ali Pasha
EID: aap2493
CS Login: alipasha
Email: alipasha@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 everyday life?
   Protection from any harm to one's family, person, and property.

2. What do these have in common?
   Protection of assets against some threat.

3. Have you been a victim of lax security?
   I don't feel comfortable answering this question.

4. What is the likelihood that your laptop is infected? How did you decide?
   Very likely since my computer has lately been moaning.

5. What security measures do you employ on your laptop?
   Open-source anti-virus software.

6. Do you think they are probably effective?
   Yes. But my downloading habits are probably not.

7. Consider the quote from the FBI official on slide 10. Do you think it overstates the case? Justify your answer.
   As the other slides mentioned, no practical system can be completely risk-free. Therefore, risks certainly exist. However, I doubt our adversaries have such easy access to them, for, if they did, we would have to admit that we are blessed by having such generous, merciful, and foolish adversaries.

8. What is the importance in learning about computer security?
   Enhance our own protection, contribute to security in the workplace, and improve overall cybersecurity.

Lecture 2

1. Consider the five reasons given why security is hard. Can you think of other factors?
   No.

2. Is there a systematic way to enumerate the "bad things" that might happen to a program? Why or why not?
   No. Given the complexity and diversity of programs, there cannot exist a systematic way to enumerate "bad things" in a program such that all "bad things" in that program can be enumerated, for all programs.

3. Explain the asymmetry between the defender and attacker in security.
   The defender has to find and protect all weak points, while the attacker needs to find and attack a single weak point.

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?
   I agree because I don't know enough of this subject to disagree.

5. Explain the statement on slide 8 that a tradeoff is typically required.
   It means that there is a negative linear relationship between the security of a program and its functionality.

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.

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?
   You accept the risk of a car accident by driving a car. You avoid the risk of a car accident by not getting into any car. You mitigate the risk of a car accident by observing all safety rules and regulations such as driving at or below the speed limit relative to the appropriate road conditions. You transfer the risk of the financial cost of a car accident through the purchase of car insurance.

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

It is a good tool, but limited nonetheless. In the bank example, if a SWIFT fraud occurs, then the bank is out of business altogether, yet that is only second in security dollars allocation. (The probabilities of the incidences occurring do not add to 1.)

5. List some factors relevant to rational risk assessment.
Technology, economy, and psychology.

Lecture 4

1. Explain the key distinction between the lists on slides 2 and 3.
Slide 2 states the goals which the mechanisms on slide 3 are attempting to achieve.

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.
Most important would be integrity since I'm not doing any classified work, such as this homework, and would not care if any other person, classmate or not, saw this document. However, I would most certainly care if this document was to be altered in a way to earn me a bad grade. Second would be availability since not having access to my work, such as this homework, would be more of a nuisance, and possibly hazardous to my grade, than someone spying on my work. Third, then, would be confidentiality for the reasons already mentioned.

3. What does it mean "to group and categorize data"?
It means to divide data into groups and categorize them.

4. Why might authorizations change over time?
Some people might be granted increasing access with time.

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related?
Security weeds out the weak points in a program that might cause it to be unreliable.

6. In what contexts would authentication and non-repudiation be considered important?
In a commercial setting, where transactions, especially monetary ones, are taking place.

Lecture 5

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

A cell phone network and a military may both have a matapolicy, the overall security goals of its system, which emphasizes confidentiality.

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

The metapolicy is often too general to provide adequate guidance, and may be subject to multiple interpretations.

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

a. Faculty/staff may not use student SSNs in documents/files/postings.
b. Documents containing SSNs must be destroyed unless deemed necessary.
c. Documents containing SSNs and deemed necessary for retention must be kept in secure storage.

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

Yes. In the students' academic records, students are stakeholders, and would certainly like to access their own records to change their grades for the better, against the policy's rules. However, the school itself is also a stakeholder, and for its own reputation and integrity would like the records to not be tampered with against policy rules.

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."

It means that if you don't understand why you're implementing a certain security mechanism, then it will be difficult, if not impossible, to gauge whether your mechanism is working, which then will be difficult to explain the need for.

Lecture 6

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

The military security is mainly about confidentiality because they don't want their super duper secret top official plans to be viewed by any unauthorized party. There are issues of integrity such as someone overwriting one of those super duper secret top official plans. Availability is an issue if the one of the super duper top secret official official can't get to his or her super duper secret top official plans.

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

The major threat is that a low level person gets access to high level information i.e. information beyond the scope of that person's clearance.

3. Why do you think the proviso is there?
   Because there are measures we can take to adequately safeguard confidentiality that would at the same time have serious integrity and availability issues.

4. Explain the form of the labels we're using.
   The form of the label is an ordered pair, the first part of which is an element of a linearly ordered set, and the second part is a subset of an unordered set.

5. Why do you suppose we're not concerned with how the labels get there?
   Because we're only concerned with issues relating to confidentiality.

6. Rank the facts listed on slide 6 by sensitivity.
   By decreasing order of sensitivity:
   a. The Normandy invasion is scheduled for June 6.
   b. The British have broken the German Enigma codes.
   c. Col. Jones just got a raise. Col. Smith didn't get a raise.
   d. The base softball team has a game tomorrow at 3pm.
   e. The cafeteria is serving chopped beef on toast today.

7. Invent labels for documents containing each of those facts.
   a. (Top Secret, {Overlord})
   b. (Secret, {Enigma})
   c. (Confidential, {Pay})
   d. (Unclassified, {Game})
   e. (Unclassified, {LunchMenu})

8. Justify the rules for "mixed" documents.
   It's ok for a higher level person to view lower level documents, but no ok for a low level person to view higher level documents.

Lecture 7

1. Document labels are stamped on the outside. How are "labels" affixed to Humans?
   Each individual has a hierarchical security level indicating the degree of trustworthiness to which he or she has been vetted, and a set of "need-to-know categories" indicating domains of interest in which he or she is authorized to operate.

2. Explain the difference in semantics of labels for documents and labels for humans.
   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?
Programs, systems, databases, files etc.
Users, processes, etc.

4. Explain why the Principle of Least Privilege makes sense.
Giving more information than a person needs to successfully perform their work, regardless of the level of the person's trust, is an unnecessary risk.

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.
Column 1: Makes sense since a person with a higher level should be able to read down at a lower level.
Column 2: Makes sense since a person with a lower level should not be able to read anything above their level.
Column 3: Same reason as column 1.

Lecture 8:

1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?
To be clear of any ambiguity when referring to information containers, entities, and operations.

2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).
Suppose L1 > L2 and S2 is a proper subset of S1. Then neither of the labels (L1, {S2}) and (L2, {S1}) dominate the other i.e. there is no ordering for these two labels. However, the label (L1, {S1}) dominates the label (L2, {S2}).

3. Show that dominates is not a total order.
Suppose L1 > L2 and S2 is a proper subset of S1. Then neither of the labels (L1, {S2}) and (L2, {S1}) dominate the other i.e. there is no ordering for these two labels.

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

5. State informally what the the Simple Security property says.
A subject may be granted read access only if the subject has a label that dominates the label on the object.

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

Because we want it to be necessary, but not sufficient. That is, for a subject to gain access to read an object, it is necessary for the subject to have a label that dominates the label on the object, but it is not sufficient i.e. the subject can still be denied access

Lecture 9

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

Simple Security doesn't protect against the possibility of a higher level subject making a write to a lower level object.

2. Why do we need constraints on write access?

Simple Security doesn't protect against the possibility of a higher level subject making a write to a lower level object.

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

Humans can be trusted not to write classified information where it can be accessed by unauthorized parties. Subjects in the world of computing are often programs operating on behalf of a trusted user (and with his or her clearance).

4. State informally what the *-Property says.

A subject may be granted write access to an object only if the label of the object dominates the label of the subject.

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

The labels of both subject and object must be equal.

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

We get a general that can.

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

Only allow writes to those subjects that have a label of equal value to the objects.

Lecture 10:

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

Allow a subject to go down, but not up.

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

It would be very inefficient for several reasons. For example, if a subject's level needs to go up, then a duplicate of the subject with the upgraded label would be required.

3. Explain why lowering the level of an object may be dangerous.
Lowering the level of an object allows those subjects read access that did not have it previously, violating confidentiality.

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.
It must not violate the conditions of simple security, the *-property, and the weak tranquility property.

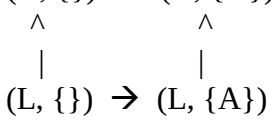
Lecture 11:

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?
The label of the lowest subject would be higher than the label of the highest object.

2. Why wouldn't you usually build an access control matrix for a BLP system?
The matrix would be too huge for most realistic purposes.

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 label that dominates the other is the supremum while the other is the infemum.

3. Explain why upward flow in the lattice really is the metapolicy for BLP.
The metapolicy of any BLP system is to constrain the flow of information among the different security levels. Upward flow means that higher level information cannot be seen by lower level subjects. A flow in any other direction would violate the metapolicy.

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.
   Information flow is permitted from L to H, but not vice versa.

2. Argue that the READ and WRITE operations given satisfy BLP.
   READ allows a subject to read an object only if the subject has a higher or equal level than the object.
   WRITE allows a subject to write to an object only if the subject has a lower or equal value than the object.
   Hence, as required by BLP, read goes down, and write goes up.

3. Argue that the CREATE and DESTROY operations given satisfy BLP.
   CREATE allows a subject to create an object of the same level as the subject.
   DESTROY allows a subject to destroy an object that is at the same level or higher. This is allowed simply by the "write-up" rule.

4. What has to be true for the covert channel on slide 5 to work?
   SL must do the same thing in every situation.

5. Why is the DESTROY statement there?
   To loop continuously.

6. Are the contents of any files different in the two paths?
   The contents are the same in both paths.

7. Why does SL do the same thing in both cases? Must it?
   If SL did not do the same thing, it would be impossible for SL to infer anything from the messages it receives. Therefore SL must do the same thing.

8. Why does SH do different things? Must it?
   SH must do different things in order for SL to receive different messages, thereby allowing SL to obtain higher level information.

9. Justify the statement on slide 7 that begins: "If SL ever sees..."
   If SL can indirectly observe SH's actions, then SL can infer (i.e. obtain information) about objects at a higher level than SL, thereby violating the metapolicy.

Lecture 14

1. Explain why "two human users talking over coffee is not a covert channel."
   Supposing that the two humans are not talking illegally within some system, and using coffee as way to utilize the resources of the system in a way they were not designed to be used, then the two people talking over coffee does not fit the definition of a covert

channel, which is a path for the illegal flow of information between subjects within a system, utilizing system resources that were not designed to be used for inter-subject 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)
```

This is a covert channel since SL will be receiving different message depending on SH's varying behavior, allowing SH to communicate down (illegally) to SL.

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

It resides in the message "Resource not found" and "Access denied" which is done by the information stored in the system by SH. Depending on SH's actions, SL can obtain the bit of information of whether or not there exists a certain confidential file above his/her level.

4. In Covert Channel #2?

The bit of information resides in the allocation time that each process transmits to the other. Depending on how long one process is taking, the other process can note any variability in times.

5. In Covert Channel #3?

The bit of information resides in the value that p sends to q. Depending on the value, q can figure out what p's most recent read was.

6. In Covert Channel #4?

The bit of information resides in the value l takes, which depends on h. Since l's value is dependent on h, l can know what h is up to.

7. Why might a termination channel have low bandwidth?

Because it doesn't terminate.

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

Energy would have to be consumed.

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

Many sources that have a power source.

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, with no appreciable impact on system processing.

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

First, theoretically, there can possibly be an infinite number of such channels unknown to anyone. Second, practically, as the previous slides mentioned, increasing security has a negative linear relationship with functionality, so that increasing security to such a degree as to attempt eliminating every covert channel would render the program itself useless.

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

We can eliminate it by modifying the system implementation.
We can reduce the bandwidth by introducing noise into the channel.
We can 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.

A sending an electronic message to B through the internet.

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

The sender can modify the shared attribute, and the receiver can view the modifications.

Lecture 16

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

Because the operation "create" doesn't explicitly say that the file exists, we can only infer that it does, while for the receiver, it would be impossible to infer event that.

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

Because it fulfills the necessary condition that both sender and receiver must have access to some attribute of a shared object such that either of one can modify it, and the other can reference it. But this condition is not sufficient 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 a column only represents a single operation, that is, a sender. A column has no potential receiver.

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

To look systematically for covert channels.