```
Name: Ali Khan
EID: aak849
CS Login: alikhan@cs.utexas.edu
Email: alikhan2010@live.com
```

CS361 Questions: Week 1 - Ali Khan; aak849

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?*

   Security is relevant to my everyday life in terms of financial security, protection from harm, and security of my information

2. *What do these have in common?*

   They all involve the "protection of assets against threats"

3. *Have you been a victim of lax security?*

   Given my prudence to manage my finances, taking care of my health, and constantly changing my passwords I have not yet been a victim of lax security

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

   It is likely my laptop is infected given the duration that infections last once they happen and the silent nature of some of these infections. Additionally, millions of malware are being produced every year

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

   Linux based security which allows me to have control over what applications are being run on my mac.

6. *Do you think they are probably effective?*

   They are more effective than PC protection that has a myriad of even more viruses that can infect them but not sufficient enough to protect me from downloading an application I authorized which may carry some infection

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

   I think it does not exaggerate that fact that if a dozen of able programmers got together (if willing) could cause a lot of trouble. Every security system has a weakness and sufficiently determined programmers can crack that weakness. What might be exaggerated is the willingness of people to do such thing

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

A) Personal awareness to keep oneself protected from threats that are avoidable via good security practice and B) as an aspiring engineer who wants to learn about how computer security works

Lecture 2

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

   In addition to the 5 reasons, security tends to be difficult because it can double the technical overhead of any given project. This is both in terms of cost and time

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

   No; bad things happening tend not to happen in a systematic or methodical way. To prevent bad things from happening, one must calculate what is unpredictable

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

   The defender must cover all possible weaknesses to create a perfectly secure system whereas the attacker simply needs to find one weakness to exploit

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

   Yes; inasmuch as your computer is turned on and likely to be connected to the internet, a local area network, or even to another computer (which is also subject to the same conditions) there is some way to access your computer (both legally and illicitly)

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

   The tradeoff between security and often times performance is an intuitive one. A secure system might have to forgo some aspect of its functionality (i.e. efficiency in terms of both time and user experience) to account for security. Ultimately, its a meta-evaluation of what is important to the business or individual

Lecture 3

1. *Define "risk"?*

   Risk is 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; because security is imperfect, designing a robust security system involves evaluating and managing different risks

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

I accept the health risks associated with sleep deprivation in completing this assignment; I avoid the risks associated with texting and driving; I mitigate the risk of an accident by driving my Camry as opposed to our Sienna (van); I transfer risk when I let my dad run a late night errand in a dangerous neighborhood

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

   It is an effective risk management tool because an ALE tabulates possible losses, their likelihood, and the potential cost for an average year. Consequently, it equips you to make a decision on which risks are worth protecting from given the product of frequency and cost.

5. *List some factors relevant to rational risk assessment.*

   As per ALE, rationally assessing risk involves compounding probability and magnitude. How frequently something happens in addition to its cost should guide which risks take priority over another

Lecture 4

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

   Slide 2 articulates the goals and meta-policies of security whereas slide 3 articulates the mechanisms by which we achieve the goals mentioned in slide 2

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

   Integrity of my data is most important to me personally. I do not want to be victim to someone changing, altering, or damaging my data. I am less interested in people viewing my information and more concerned about what people can potentially do once they have that information i.e. identity theft

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

   It means to assign and stratify different data to some value given some standard. In this case, it means to assign data various levels of sensitivity

4. *Why might authorizations change over time?*

   More parties might gain privilege to see certain pieces of information i.e. a military individual getting promoted or one getting married and consequently sharing some information

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

   Security is related to the protection of assets and consequently the availability of some service might be the biggest asset of some given company or individual i.e. Amazon having their services comprised to a breach represents a severe violation of their security

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

Both of these might be relevant in the context of handling different pieces information that has various levels of sensitivity. Consequently, establishing identity is important to see that information and the ability to discernibly see who changed any piece of information is important i.e. CIA

Lecture 5

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

   A potential meta-policy for a cell phone network would be confidentiality. When two people are talking on the phone, they are under the assumption that their conversation is private and it ought to be held as such. A potential meta-policy for a military database authentication as it important that only people who have established their identity and rank that should be allowed to see sensitive information

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

   A policy is the mechanism by which you achieve the meta-policy

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

   A student should be able to view their own grades

   A student should not be able to change the outcome of their grades

   The student should be the exclusive viewer their grades

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

   A stakeholders' interest of a streamlined and quick interface might compete with the seemingly cumbersome security demands for users to access a website.

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

   Documents containing SSNs need to be kept secure given the sensitivity of an SSN and as such the meta-policy is confidentiality

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

   The meta-policy guides how the security system ought to be designed and more relevantly becomes the metric for whether a security system is effective. Consequently, absent a meta-policy, a policy becomes difficult if not impossible to evaluate

Lecture 6

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

The military is mainly about confidentiality because there is information with various sensitivity levels that only people with certain clearance levels can see. Integrity is also important in that you want to control who or what can modify this information and availability is important (although less important) in that you want the information to be accessible when needed

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

Aspects of this thought experiment include necessary elements of a secure system but are not sufficient. In other words, establishing various sensitivities for objects and clearances for subjects is only one of many aspects that are needed. Authentication is also important because you do not want someone posing as a commander with the appropriate clearance to see highly sensitive information. Other important aspects would how to protect the integrity of the information that can be seen.

3. Why do you think the proviso is there?

The proviso that there is a major threat to MLS makes sense because a) every system has a vulnerability and b) the MLS system has only one of many necessary but insufficient elements of a secure system (confidentiality)

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

The form of the label we are using entails a certain sensitivity accompanied by objects that have that sensitivity i.e. (Secret: {Nuclear, Crypto})

5. Why do you suppose we're not concerned with how the labels get there? 6. Rank the facts listed on slide 6 by sensitivity.

We are not concerned with the labels because those are decided beforehand and we presuppose that these labels accurately describe the sensitivity. With this information we can parcel out the different object into various categories.

In increasing order of sensitivity:

- **The cafeteria is serving chopped beef on toast today; {Unclassified}**
- **The base softball team has a game tomorrow at 3pm; {Unclassified}**
- **Col. Smith didn't get a raise; {Confidential}**
- **Col. Jones just got a raise; {Confidential}**
- **The British have broken the German Enigma codes; {Secret}**
- **The Normandy invasion is scheduled for June 6; {Top Secret}**

7. Invent labels for documents containing each of those facts. 8. Justify the rules for "mixed" documents. **See above for labels; For mixed documents it seems appropriate to upgrade the level of security. This makes sense because you do not want to risk divulging sensitive information to someone who has a lower security clearance**

Lecture 7

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

   "Labels" are affixed to humans because they help us categorize and organize different pieces of information. Consequently, a label attached to the front of a file helps us immediately identify its contents and sensitivity

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

   The semantics of labels for various documents may be organized by the sensitivity of its contents. Humans may create labels that relate more to the content of the documents and more about who the documents are meant to be read by i.e. "the manager's file" or "Quarterly earnings"

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

   In the context of computers, the analogue of a document object might be who or what has the authority to parse the document in addition to its contents and where it would be stored. The analogue of a document to a human is similar in that the contents, permissions to view the document, and where it is stored is relevant

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

   This principle makes sense because it minimizes the risk that unauthorized individuals get there hands on sensitive information. Security leaks are always a risk and the less people who have access to a given piece of information the less likely it will be leaked to unauthorized personnel

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.*

   Line one make sense because the secret label is greater than the confidential label and the subjects set of documents (crypto) is a superset of the object (crypto)

   Line two also makes sense because secret label is less than the top secret label and consequently access is not allowed from the subject to the object

   Line three also makes sense because secret label is greater than unclassified and Nuclear is a superset to {}.

Lecture 8:

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

   This terms provide a framework and uniform language to describe various elements and behaviors of a security system

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

   Dominates is a partial order because not all security labels are subject to a domination relationship. In other words, there exists security labels such that neither A>=B nor B>=A have to be true

3. *Show that dominates is not a total order.*

   Dominates is not a total order because there exists security labels such that neither A>=B or B>=A do not have to be true. This practically means there could be a label that exists in isolation that neither dominates or is dominated but simply defines access to a subset of authorized individuals

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

   If two labels dominate each other both ways implies that both labels are the same. A>=B and B>=A would be true if A=B

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

   Simple security basically means that if a person has clearance that is equal to or greater than the document and authorization to see the pertinent document or more documents than the object, then he or she is allowed to see the documents

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

   “Only if” is an indication that a certain element is necessary but insufficient. “If only and only if” would imply that it is necessary and sufficient. Simple security is only one aspect of a security system that may be necessary but it definitely not sufficient

Lecture 9

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

   Simple security is necessary but not sufficient because it does not articulate who has the authority to change the contents of data. Ignoring this element would defeat the spirit of a secure system

2. Why do we need constraints on write access?

   Constraints on write access are necessary to protect the integrity and usefulness of data. Absent any restriction on write access would defeat the usefulness of data as anyone can modify it.

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

   Computers are always at risk to have hidden clients, applications, or infections running that could harm the integrity of data

4. State informally what the *-Property says.

   The star property simply says that subjects of lower clearance can write up whereas subjects of higher clearance cannot write down

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

   The subject has a label equal to the label of the object and the documents of the subject are equal to the set of documents in the object (L,S) = (L,S)

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

   You restrict the general’s access but disallowing write down

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

Yes this is a flaw with the star property; we can allow writing privileges that adds to the contents and does not *overwrite the contents* in addition to documenting who made these changes

Lecture 10:

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

   All subjects can change any label but are expected to act in such a way that supports the "spirit" of the security policy. This strategy is predicated on everyone acting in that spirit

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

   Sometimes subjects and objects are constantly being promoted or demoted which would make a strong tranquility system too rigid

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

   Lowering the level of an object is risky because it assumes 100% of the content is approved for the viewing of less authorized individuals. This assumption is a bold and challenging one to uphold. Furthermore, you have substantially increased the pool of people who can view this object which increases the likelihood of vulnerability

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

   A) That are you approve the new pool of individuals B) to see ALL the contents of the downgraded object

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?

   Then all labels and levels for subjects and objects would be the same. You can give everyone unclassified access to all unclassified objects

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

   The matrix would be huge for most realistic systems

Lecture 12

CS361 Questions: Week 1 5

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,{A})———————> (H,{A})

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.*

   Upward flow in the lattice describes information flow that is legitimate in BLP. A person of level higher can read the information provided by the level is pointing to the higher level. Conversely, the lower level can write up to the higher level that it is pointing to.

Lecture 13

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

   Given L<H and L—->H; If this represents a BLP lattice, then information flow is permitted from L to H, but not vice-versa. This captures the metapolicy of this simple system.

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

   Read (S,O) accomplishes BLP because a subject's label must still be greater than the object's label and the subject must still have contents that are the superset of the object's contents.

   Write still upholds the write up doctrine of BLP in that the label of the subject must be less than the label of the object.

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

   Create seems to satisfy BLP in that it only allows the subject to instantiate a new object at the level the subject operates.

   Destroy satisfies BLP because it still subscribes to the write up doctrine in that the label of the subject must be less than the label of the object.

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

   Every attempt to access any given object from a subject should always return something

5. *Why is the DESTROY statement there?*

   To remove the object created for the sole purpose of signaling

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

   No, they are they same. They are simply instantiated by two different actors

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

   Because the same value is written to SL in both cases; Yes

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

   SH is uniquely created in case 1 whereas it does not exist in case 2

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

   Signaling by SH to SL violates the metapolicy because it represents information flow of the opposite direction

Lecture 14

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

   Because they are using a legitimate channel of communication to converse

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; no meaningful information is being conveyed because of a lack of create and destroy

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

   The error message: resource not found or access denied

4. In Covert Channel #2?

A bit is being sent between the processes using its total allocation or relinquishing the processor immediately. Information is recorded in the ordering or duration of events on the system

CS361 Questions: Week 1 6

5. In Covert Channel #3?

The order that p accesses the disk drive could be an avenue of channeling to q

6. In Covert Channel #4?

The condition of l depends on the value of h

7. Why might a termination channel have low bandwidth?

It is simply a check of whether a computation terminated

8. What would have to be true to implement a power channel? 9. For what sort of devices might power channels arise?

Some kind of energy tracker is needed i.e. a power meter coupled with a software that tracks the power usage

Lecture 15

1. Explain why covert channels, while appearing to have such a low band- width, 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 despite the seemingly slow nature of such channels

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

   It is always possible to use legitimate channels of communication for illegitimate information flow.

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

   We can eliminate the covert channel by modifying the system implementation and also reducing the bandwidth by introducing noise into the channel

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

   A military file in which the lower level is able to write up and the higher level is able to read down

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

   The sender is able to modify an attribute and the receiver is able to reference the modified attribute

Lecture 16

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

   Creation of a new object does not necessarily render the creator authority to read it

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

   Because it fulfills the conditions necessary for a covert channel. A sender is able to modify an attribute and the receiver is able to reference it

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 does not meet the preconditions for a covert channel

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

   To identify potential covert channels and to outline specific operations that each subject is able to do