Name: michael truong
EID: mkt532
CS Login: mtruong
Email: mtruong92@utexas.edu

# CS361 Questions: Week 1

## Lecture 1

1. What uses of the term “security” are relevant to your everyday life?
personal security

2. What do these have in common?
they are all the "protection of assests against threats"

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

4. What is the likelihood that your laptop is infected? How did you decide?
100%; i watch a lot of porn

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

6. Do you think they are probably effective?
somewhat

7. Consider the quote from the FBI official on slide 10. Do you think it overstates the case? Justify your answer.
probably; i'm still here, aren't i?

8. What is the importance in learning about computer security?
enhance your own protection;
contribute to security in your workplace;
enhance the quality and safety of interpersonal and business transactions;
improve overall security in cyberspace;

## Lecture 2

1. Consider the five reasons given why security is hard. Can you think of other factors?
you can never achieve perfect security

2. Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not?
no; as technology grows, the number of "bad things" that might happen to a program grow

3. Explain the asymmetry between the defender and attacker in security.
the defender has to find and eliminate all exploitable vulnerabilities; the attacker only needs to find one

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?
yes; you can never achieve perfect security

5. Explain the statement on slide 8 that a tradeoff is typically required.
typically, a tradeoff is necessary between security and other important project goals: funtionality, usability, efficiency, time-to-market, and simplicity

## 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

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?
every time you drive on the streets, there's always a risk that you'll have an accident, because the alternative is stay at home and not do certain things that you want to do;
don't drive on highways or don't drive at night;
drive old chenvy instead of bentley, because you know if you're in an accident there, it's going to cost you less to get it fixed;
buy an insurance policy, install a home security system and then you put a placard in your front yard that says that you have a security system, it sort of transfers the risk to your neighbor, who doesn't have a security system, because someboy coming along who's going to break into the house is going to say "well i'm going to skip this guy's house and i'm going to go over here instead"

4. Evaluate annualized loss expectancy as a risk management tool.
you are supposed to look at the annualized loss expectancy and spend your security money where the maximum loss might occur

5. List some factors relevant to rational risk assessment.
technical, economic, psychological, etc.

## Lecture 4

1. Explain the key distinction between the lists on slides 2 and 3.
the list on slide 3 are mechanisms for protecting one or more of the major aspects on the list on slide 2

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.
confidentiality; someone could control my life if they had my information

3. What does it mean “to group and categorize data”?
if all your data is not equally sensitive, then how do you parcel out your data into the various pots so that this one receives a great deal of protection, this one maybe not so much, and this over here not at all

4. Why might authorizations change over time?
promotion, demotion

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

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

# Lecture 5

1. Describe a possible metapolicy for a cell phone network? Amilitary database?
availability; confidentiality

2. Why do you need a policy if you have a metapolicy?
the metapolicy is often too general to provide adequate guidance.
the metapolicy may be subject to multiple interpretations
there may be multiple acceptable policies that accomplish the security goals
the policy provides specific and enforceable guidelines to the system user/developer.

3. Give three possible rules within a policy concerning students’ academic records.
there should be a hierarchy of people that should be allowed to see some records but not others;
there should be a hierarchy of people that should be allowed to change some records but not others;
students' academic records should always be available

4. Could stakeholders’ interest conflict in a policy? Give an example.
the school wants to preserve the integrity of my grades; i don't

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.”

the policy only makes sense in service to a metapolicy

# Lecture 6

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

2. Describe the major threat in our MLS thought experiment.
the confidentiality of information - no person not authorized to view a piece of information may have access to it

3. Why do you think the proviso is there?
to simplify the problem

4. Explain the form of the labels we're using.
one part of the label is taken from a linearly ordered set;
there are also "need-to-know" categories, from an unordered set, expressing membership within some interest group

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

6. Rank the facts listed on slide 6 by sensitivity.
the normandy invasion is scheduled for june 6
the british have broken the german enigma codes
col. jones just got a raise
col. smith didn't get a raise
the base softball team has a game tomorrow at 3pm.
the cafeteria is serving chopped beef on toast today

7. Invent labels for documents containing each of those facts.
crypto, finance, sports, cafeteria

8. Justify the rules for "mixed" documents.
a folder with "mixed" information must be labeled to protect the information at the highest hierarchical level and protect all categories of information

# Lecture 7

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

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 the 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; programs

4. Explain why the Principle of Least Privilege makes sense.
if you don't give information to somebody, they can't leak it

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.

secret >= confidential; {crypto} ⊆ {crypto}

secret < top secret;

secret >= unclassified, {nuclear} ⊆ {}

## Lecture 8:

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

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

l1 >= l1; s1⊆ s1; (l1, s1) >= (l1, s1); dominates is reflexive;

if (l1 >= l2) and (l2 >= l3) then (l1 >= l3); if (s1 ⊆ s2) and (s2 ⊆ s3) then (s1 ⊆ s3); (l1, s1) >= (l3, s3); dominates is transitive;

if (l1 >= l2 >= l1) then (l1 = l2) and if (s1 ⊆ s3 ⊆ s1) then (s1 = s3) then (l1, s1) = (l2, s2); dominates is antisymmetric;
dominates is a  partial order

3. Show that dominates is not a total order.
there are security labels A and B, such that neither a >= b nor b >= a

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

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

6. Explain why it’s “only if” and not “if and only if.”
it's a necessary condition but it's not a sufficient condition, because there may be other security constraints which are in place

## Lecture 9

1. Why isn’t Simple Security enough to ensure confidentiality?
suppose someone with access to a top secret document copies the information onto a piece of paper and sticks it into an unclassified folder

2. Why do we need constraints on write access?
a higher-leveled subject can leak information down to a lower-leveled subject

3. What is it about computers, as opposed to human beings, that makes that particularly important?
some program you run may have embedded malicious logic (a "trojan hose") that causes it to "leak" information without your knowledge or consent

4. State informally what the *-Property says.
write up

5. What must be true for a subject to have both read and write access to an object?
(ls, cs) = (lo, co)

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

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

## Lecture 10:

1. Evaluate changing a subject’s level (up or down) in light of weak tranquility.
subjects and objects should not change labels in a way that violates the "spirit" of the security policy

2. Why not just use strong tranquility all the time?
what if a user needs to operate at different levels during the course of the day

3. Explain why lowering the level of an object may be dangerous.
the ability to change levels arbitrarily can subvert security

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.
it is safe for the information to be downgraded

## 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?
subjects - high;
objects - low

2. Why wouldn't you usually build an access controlmatrix for a BLP system?
the matrix would be huge for most realistic systems;
the matrix is implicit in the rules (simple security and the *-property), so access permissions can be computed 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.)

$$\begin{tikzcd}
(h, \{a\}) & (h, \{\}) \arrow[l] \\
(l, \{a\}) \arrow[u] & (l, \{\}) \arrow[l] \arrow[ul] \arrow[u]
\end{tikzcd}$$

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?
lub = (max_level, set_of_all_categories)

glb = (min_level, {})

3. Explain why upward flow in the lattice really is the metapolicy for BLP.
the real security goal (metapolicy) of any mls scheme is to control the flow of information in the system. i.e., sensitive information should not flow "down" in the system, from a high level to a low level;
we only want information to flow "upward" in the lattice of security levels. equivalently, information may flow from l1 to l2 only if l2 >= l1

# 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.
if object o exists and ls >= lo, then return its current value; otherwise, return a zero;
if object o exists and ls <= lo, change its value to v; otherwise, do nothing

3. Argue that the CREATE and DESTROY operations given satisfy BLP.
create and destroy are basically write operations

4. What has to be true for the covert channel on slide 5 to work?
sh has vary it's actions (create (sh, f0), do nothing)

5. Why is the DESTROY statement there?
because in both cases the object was destroyed, they can easily go back and do this again;
if sl and sh can coordinate their activities, sh can transfer arbitrary amounts of information to sl, given enough time

6. Are the contents of any files different in the two paths?
no

7. Why does SL do the same thing in both cases? Must it?
sl doesn't know what action sh has performed; yes

8. Why does SH do different things? Must it?
to signal one bit of information to sl by varying its behavior; yes

9. Justify the statement on slide 7 that begins: “If SL ever sees...”
it's enough to show that blp cannot guarantee that the metapolicy is satisfied

# Lecture 14

1. Explain why “two human users talking over coffee is not a covert channel.”
a convert channel is a path for the illegal flow of information between subjects within a system

2. Is the following a covert channel? Why or why not?
no; if you could modify the contents of a file and then have the lower-level user see that, that would just be in violation of either simple security or the *-property

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

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

5. In Covert Channel #3?
the order of which cylinder is currently closest to the read head

6. In Covert Channel #4?
the control flow of a program

7. Why might a termination channel have low bandwidth?
computations are fast and cheap?

8. What would have to be true to implement a power channel?
that the low-level process can sense how much energy is consumed by a particular computation and the high-level process can modulate that

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

# 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?
typically, a tradeoff is necessary between security and other important project goals: funtionality, usability, efficiency, time-to-market, and simplicity

3. If detected, how could one respond appropriately to a covert channel?
we can elimate 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.
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 modifies the attribute of a shared object
the receiver references the attribute of a shared object

# Lecture 16

1. Why wouldn’t the “create” operation have an R in the SRMM for the “file existence” attribute?
it's not important that you know something about the attribute; what's important is that the operation tells you something about the attribute

2. Why does an R and M in the same row of an SRMM table indicate a potential channel?
for that attribute there's a mechanism by which someone can modify it and and someone can 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; a mechanism for accessing some attribute of a shared object must exist

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

to investigate potential covert channels