Aaron Dishman
UTID: adishman
Turnin: adishman

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?
   Network Security: internet transactions(purchases, privacy, etc.)
   Physical security: police provide security against crimes
   Personal Security: own weapons for protection
   Communication security: cell phones, email, etc.

2. What do these have in common?
   They are all examples of types of protection of assets from attacks.

3. Have you been a victim of lax security?
   Obviously, the NSA knows everything I do on my phone and computer. But also, I have had my credit card number stolen from a company that processed the payments of a restaurant I ate at. Also have had my home(s) and car(s) broken into.

4. What is the likelihood that your laptop is infected? How did you decide?
   I would say that it is likely that there is some form of malware that gathers data about me and how I use the internet. This could be from the NSA, or from downloaded files like songs or videos, or websites that I have visited.

5. What security measures do you employ on your laptop?
   Even before Edward Snowden, I was worried about the ability of someone to hack into my computer and turn on my camera and watch me. This idea creeped me out to the point that I’ve made a habit of placing tape over said camera until I actually use it. I also update my OS and apps as quickly as updates are available.

6. Do you think they are probably effective?
   I don’t think that updates are 100% effective, because I don’t think that a 100% effective system exists, but I have come to accept a certain amount of risk. I do think that the tape over my camera is 100% effective at blocking any malicious attempt to use said camera to spy on me.

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

To some extent, it does overstate the case, just in the fact that it seems unlikely that if they could "challenge our country's very existence" would they not have already done so. But I think that perhaps this official was espousing about the possibility existing, and using hyperbolic rhetoric to draw attention the the slight possibility.

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

As a programmer, it would be foolish to put time and energy into a program or system that could be easily attacked and manipulated.

Lecture 2

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

Those 5 seem to cover everything that I can think of.

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

I think there is a way to enumerate "some, many, or most" bad things that might happen to a program, but impossible to enumerate "all" the bad things that might happen. This is because I don't think it's possible to anticipate every system that your program could run on and how that system will interact with said program.

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

The attacker only has to find a single vulnerability to attack a system, but a defender has to find EVERY vulnerability to protect a system. Asymmetry refers to the contrast between one and all.

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

I agree, because I believe that perfect security implies no functionality, or doesn't exist at all. In order to get anything done, you need to be able to change things, and if you can change things, you can potentially change things that should not be changed.

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

It kind of has to do with my answer for question 4. Functionality of a program implies a reduction in system security.

Lecture 3

1. Define "risk"?

The possibility that something "bad" will happen.

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: super volcano eruptions
Avoid: Skydiving
Mitigate: I lock my house and car doors when I leave them
Transfer: I buy car and home insurance

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

ALE is a good way to estimate a potential loss due to a given set of likely risks, but it doesn't take into account everything about risks.

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 of enforcing aspects of the lists on slides 2

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

It depends on the context. For my credit card data that I send to online purchases, confidentiality is extremely important. For my grades, integrity is important, I don't want my A's to be randomly changed to F's.

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

It refers to looking at different data in different contexts in order to determine what protections it needs.

4. Why might authorizations change over time?

A user might get a promotion, so therefore might need to be able to read higher level documents, or vice versa.

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

A failure of availability implies a failure of reliability.

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

Online purchases. You want to know that you are purchasing from Amazon, and you don't want Amazon to be able to say that you didn't pay them after your payment has been withdrawn from your account.

Lecture 5

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

A customers phone should always be able to make a call in an area that is covered by a cell tower. No one who is authorized to be on base will be blocked from entering the base.

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

A policy is a lower level for specific details in a specific system, whereas a metapolicy may be ambiguous.

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

faculty/staff may not use student SSNs in documents/files/postings; all older docs containing SSNs must be destroyed unless deemed necessary; documents deemed necessary must be kept in secure storage; etc.

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

Yes.

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

social security numbers of students should be protected from disclosure

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

Without understanding the general metapolicy of confidentiality, integrity, or availability, specific policy requirements may seem arbitrary or not understandable

Lecture 6

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

Because information "sensitivity" levels are different for different information. For instance, generals want to be able to know the war plan, but you don't necessarily want a private to know the whole plan. But there are also aspects of integrity and availability, for instance, you don't want the war plan to be randomly changed.

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

Information flowing down in levels.

3. Why do you think the proviso is there?

Because if we are concerned with integrity or availability, we might get results that violate confidentiality. Also, someone burning down the office and destroying the war plan might be a significant threat, but it's not a threat to confidentiality.

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

Labels contain hierarchical component and a set of categories.

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

That is concerning a different policy

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

1: not confidential, low sensitivity
2: highly sensitive
3: not confidential, low sensitivity
4: confidential
5: confidential
6: confidential

7. Invent labels for documents containing each of those facts.

1: U: {}
2: TS: {C}
3: U: {}
4: C: {P}
5: C: {P}
6: TS: {C}

8. Justify the rules for “mixed” documents.

If there is highly sensitive and not information in a single document, it would not make sense to mark it as low sensitivity, because then anyone with low read would be able to see highly sensitive information, violating BLP.
The same logic applies to multiple categories.

Lecture 7

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

Much in the same way

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

A level for humans implies how much they are trusted, a label for documents implies sensitivity of information

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

Documents are files; humans are users or processes

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

Because a person who works in crypto only shouldn’t concern themselves with nuclear secrets, and an organization wants to decrease the possibility of information leaks to as few sources as possible.

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.

They make sense because they conform to the hierarchical rules

Lecture 8:

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

To generalize the ideas behind security policies and make them easier to code.

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

x == L1
y == L2
z == S2 ⊆ S1

x >= x == L1 >= L1
(x >= y ^ y >= x —> x == y) == L1 >= L2

3. Show that dominates is not a total order.

because it's "if" not "if and only if"

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

If they are equal

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

Read access is granted to subjects that have dominance over objects

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

because there may be other factors that prevent a read from happening

Lecture 9

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

because a dominating subject being able to write to an object it dominates may open up the possibility of sensitive information being passed "down"

2. Why do we need constraints on write access?

to prevent highly sensitive information leaking "down"

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

trojan horse programs of high clearance could be written by a low clearance users and write sensitive information to be sent to low clearance sources

4. State informally what the *-Property says.

read down, write up

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

must be at the same dominance level

6. How could we deal with the problem that the General (top secret) can't send orders to the private (Unclassified)?
Give the general a separate low clearance account to send such emails

7. Isn't it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.
It is not a problem of confidentiality, just integrity. make a trusted subject.

Lecture 10:

1. Evaluate changing a subject's level (up or down) in light of weak tranquility.
An object can be raised, therefore not leaking information "down"
Lowering the level of a subject could potentially leak hi information if it retains such information before it writes.

2. Why not just use strong tranquility all the time?
Sometimes a subject may need to "give orders" or some information may be later deemed as "sensitive"

3. Explain why lowering the level of an object may be dangerous.
It could leak highly sensitive information to low levels

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.
information contained no longer deemed "secret"

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 would be high level, all objects would be low level.

2. Why wouldn't you usually build an access control matrix for a BLP system?
Because it doesn't really make sense. The matrix would be so big that it would make more sense to calculate it on the fly.

Lecture 12

1. Suppose you had hierarchical levels L, H with $\mathbf{L < H}$, 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, {}) -> Everything

(L, {A}) -> NOT (L, {})
(H, {}) -> (H, {A})
(H, {A}) can't write to anything

All of these can also write to themselves

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?
LUB = highest security level and superset
GLB = lowest security level and common subset

3. Explain why upward flow in the lattice really is the metapolicy for BLP.
Because flow of information can only go "up"

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.
because BLP doesn't allow information to flow from hi to low

2. Argue that the READ and WRITE operations given satisfy BLP.
No information from objects with high clearance is passed down

3. Argue that the CREATE and DESTROY operations given satisfy BLP.
No information from objects with high clearance is passed down

4. What has to be true for the covert channel on slide 5 to work?
The same operations must happen for low subject

5. Why is the DESTROY statement there?
So you can start over fresh again

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?
because you can't know the behavior before hand, it must work this way

8. Why does SH do different things? Must it?
Because SH can create objects at will without detrimental effects

9. Justify the statement on slide 7 that begins: "If SL ever sees…"
The metapolicy is BLP, which forbids information flow from high to low.

Lecture 14

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

Because if information is passed, it wouldn't be gathered from a covert source…the "processes" are actually communicating.

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 SH doesn't change from Send 0 to Send 1

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

within the system state

4. In Covert Channel #2?

in the ordering or duration of events on the system

5. In Covert Channel #3?

in location of disk read head

6. In Covert Channel #4?

in the control flow

7. Why might a termination channel have low bandwidth?

it might take a while for a computation to complete

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

a way to measure usage

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

a usb stick that has a power light

Lecture 15

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

because processors operate at thousands of bits per second

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

For the same reason as 100% security doesn't exist…usability suffers

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. This is intrusion detection.

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

1 Both sender
and receiver must have access
to some attribute of a shared object.
2 The sender must be able to modify
the attribute.
3 The receiver must be able to
reference (view) that attribute.
4 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.

to send sensitive information covertly

Lecture 16

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

not necessary, because either it already existed, or it does now. don't send information that you don't need to send

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

yes

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 different files would contain different information…wouldn't tell you much

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

To systematically identify potential covert channels,