Name: Zhenyu Zhu

Date: 6/15/2014

EID: cike

CS loging: zhenyu

Email: zhu_zhenyu@utexas.edu

HW: #2

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?

Home security, financial security, personal security, computer security, network security, physical security

2. What do these have in common?

Assets, threats and protection methods (security policy, rules)

3. Have you been a victim of lax security?

No

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

Very likely, by tons of virus, spam, Trojan horse out there, also the increase connectivity and low threshold to access, more hacking tools make people becomes a hacker easier than before. Because of the current Internet changes and how easy computer can be hacked.

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

Install latest virus checker, spyware filter, spam filter, and constant update to the latest definition

6. Do you think they are probably effective?

Maybe, they work against known virus or security loopholes, but cannot prevent new attacks, always one step behind.

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

Probably not, it depends what type of computer system unauthorized group has accessed. If a nuclear weapon system has been hacked, then it indeed will "challenge our country's very existence".

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

Understand what security and threats are, enhance own protection, contribute to a more security cyberspace and help prevent cyber attacks.

Lecture 2:

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

    Always easy to break than to build, there might be a small group of programmer who are working on a program, but1000 times of people who will use the program, hence more people can find vulnerability than the people actually build the program. Also Technology change too fast, there might be new loopholes discover in the near future that will threat an existing program.

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

    No, because there are too many possible “bad things”, it is hard to categorize and hard to thought of all possible attack scenarios, hence hard to enumerate in a systematic way.

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

    Defender has to defend all possible vulnerabilities, while attacker only needs one vulnerability to breach in security.

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

    Yes, it is very extreme, but that is the only way if you are chasing “Perfect security”, if you don’t have an asset, then no threat can be apply, hence it is perfect secure.

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

    Efficiency definitely possible since turning on security feature can use more computer resources and have longer run time.

    Simplicity is always the case since adding codes to add security function will always make program more complex.

    Time to market is effected since you will need extra time to find all the possible vulnerabilities.

    Usability is going to be effected since you are adding extra feature for security other than the original goal of program.

Lecture 3:

1. Define “risk”?

    Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. Risk is the possibility of bad things might happen.

2. Do you agree that software security is about managing risk?

    Yes, there is always a tradeoff and limited resource, and each different risk can cause different consequences, you have to make a decision to reduce the risk and cause minimum damage if risk can not be avoided, hence software security is also about managing risk

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

    Accept: take a flight to some other city knowing plane might crash.

    Avoid: do not go to dangerous place where you might get rob.

    Mitigate: bring less cash on you when you have to go to a dangerous place, and go there during daytime.

    Transfer: ask someone else to go to a dangerous place to do something, or ask police presence.

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

It is an effective tool for risk management, but the “expected value” ALE compute should not be the only factor to make a risk management decision. Other factors should be considered as well.

5. List some factors relevant to rational risk assessment.

Technical, economical, psychological etc.

Lecture 4:

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

Lists on slide 2 are the goals, and lists on slide 3 are the mechanisms to achieving goals on slide 2.

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

Confidentiality, I don’t want anyone else to view my personal and financial information. If they can’t view my information, then they can’t change it, so integrity is less concern, and since my information is always there, so availability is less a concern for me as well.

3. What does it mean, “to group and categorize data”?

It means to separate data into different levels of confidentiality depends on its content.

4. Why might authorizations change over time?

Because assets’ content might change its confidentiality level over time. So the authorization might change according to the change in confidentiality level, either upgrade or downgrade.

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

Reliability is defined in IEEE as the ability of a system or component to perform its require function under stated conditions for a specified period time. One distinction can be reliability deals with internal functionality of a system, where security deals with vulnerability of the system. Without a reliability system, we cannot have security system and availability. A reliable system might not be secure and but it can be available. A secure system can be reliable and available.

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

Such as log in to an online retailer site and make a purchase with saved credit card linked to the account. In this case, authentication and non-repudiation will be important.

Lecture 5:

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

Cell phone network metapolicy: Availability, make sure cell phone can be used in all geographic area within USA.

Military database metapolicy: Confidentiality, Separate data into different categories with different access levels.

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

Because policy (lower level) is a set of rules to achieve a goal (high level metapolicy). Metapolicy is too general and subject to multiple interpretations, and policy provides more specific and enforceable guidelines' to the system user or developer.

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

A) University should not permit access or release student's academic record without his/her written consent.

B) The contents of a student's educational record may be challenged by the student on the grounds that the record is inaccurate, misleading, or otherwise in violation of the privacy rights of the student by submitting a written statement to the custodian of records.

C) General categories of educational records are periodically reviewed and obsolete information is removed and destroyed in accordance with an established record retention schedule.

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

Yes, student might want to change his/her academic record for a better grade while university want to keep students' record's integrity.

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

Metapolicy: To protect the confidentiality of student's SSN from identity theft. Student's SSN 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."

Because policy is a set of rules to achieve metapolicy, if you don't understand what is the overall goal you trying to accomplish, then you can't evaluate the tools or mechanism you use in the policy correctly.

Lecture 6:

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

Because you don't want everyone accessing military information, but it is not only about confidentiality, yes, there are aspects of integrity and availability as well. In this lecture, we only concerns about confidentiality for our thought experiment.

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

Confidentiality of information is breached. Unauthorized person can view the information about his/her security clearance.

3. Why do you think the proviso is there?

To simplify the MLS thought experiment for now.

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

Label is made of two components; one is in hierarchical linear order of 4 sets. (Unclassified, confidential, secret, top secret), second component is needed to know unordered categories sets. (Such as crypto, nuclear, personnel, etc.).

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

Because our security goal here is confidentiality, how label gets there is an integrity issue.

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

Baseball schedule (UN)

Normandy invasion schedule (TS)

Cafeteria menu (UN)

Col. Jones raise (C)

Col. Smith didn't get raise (C)

The British broken German Enigma Code (TS)

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

Baseball schedule (Unclassified: {recreation})

Normandy invasion schedule (Top Secret: {schedule})

Cafeteria menu (Unclassified: {cafeteria})

Col. Jones raise (Confidential: {personnel})

Col. Smith didn't get raise (Confidential: {personnel})

The British broken German Enigma Code (Top Secret: {crypto})

8. Justify the rules for "mixed" documents.

The goal here is protect the confidentiality of the information. So we need to prevent "mixed" documents with high hierarchical rank being accessed by unauthorized subjects, hence using the highest appropriate level, and use all categories associated with the mixed documents.

Lecture 7:

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

Assign appropriated clearance levels, of same form as document sensitivity level. To indicate the degree of trustworthiness and a set of need-to-know categories, that he or she is authorized to operate.

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

Labels on documents indicate the sensitivity level of the contain information.

Labels on human 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?

Of documents: file access privilege

Of human: different level of administration login rights.

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

Because if you don't give the information to someone, then they can't leak the information. The less you know, the less you can leak.

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.

Because the first component of label is in linear order for both documents and human.

Row 1: Yes, because person have high order of clearance ($S > C$) and same need to know category.

Row 2: No, because person has lower clearance level. ($S < TS$)

Row 3: Yes, because person have high clearance and more need-to-know category than document.

Lecture 8:

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

So we have same terminology and easy to have a systematic way to develop a security policy.

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

Reflexive: since same set of security label will have same hierarchical level and categories, then it satisfied both constrain definition of dominates, therefore $x \geq x$,

Transitive: if $x \geq y$ and $y \geq z$, let $x = (L1, S1)$, $y = (L2, S2)$, $z = (L3, S3)$
for hierarchical level: $L1 \geq L2$ and $L2 \geq L3$, then $L1 \geq L3$, since linear order
for categories: $S3 \subseteq S2$, $S2 \subseteq S1$, then $S3 \subseteq S1$, definition of set and subset
therefore by definition of dominate, $x \geq z$

Anti-symmetric if $x \geq y$ and $y \geq x$, let $x = (Lx, Sx)$, let $y = (Ly, Sy)$
if $Lx \geq Ly$ and $Ly \geq Lx$, then $Lx = Ly$
if $Sy \subseteq Sx$, and $Sx \subseteq Sy$, then $Sx = Sy$,
since $Lx = Ly$ and $Sx = Sy$, then $x = y$

3. Show that dominates is not a total order.

Security labels A and B such that neither $A \geq B$, nor $B \geq A$,

For example A can be (Secret: {nuclear}) and B is (Secret: {Crypto}), here we have 2 different category, that does not agree to second definition of dominate, then neither $A \geq B$, nor $B \geq A$, therefore it is not a total order.

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

That the two labels are equal, both in hierarchical level and have same category set.

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

Subject S can be grated read access to object O only if S clearance level dominate O sensitivity level. Read down.

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

Because there might be other security constraints that will prevent read access, and also because the simple security property is a necessary condition but not a sufficient condition for read access.

Lecture 9:

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

Because we also need to have proper write access to protect confidentiality, and simple security property is only apply to the read access. Such as high level person reads file and write to lower level folder, which does not violate the simple security, but breached the confidentiality.

2. Why do we need constraints on write access?

Because in the world of real life, we can trust a person with proper level of clearance but we cannot trust the program running under this person's behalf, the program might contain malicious virus that leaks or write information to a lower sensitivity level place. So we need to add constraints on write access to protect confidentiality.

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

Because computer might have embedded Trojan horse virus, we can trust a human with proper clearance level will not break protocol, but we can not trust program running under his behalf is not infested with Trojan horse virus or spy ware to leak information without his consent.

4. State informally what the *-Property says.

Write up. Subject S maybe grant write access to object O only if (Lo, Co) dominate (Ls, Cs)

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

That subject and object has the same clearance and sensitivity level.

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

By logging out from General's top secret account and re-log into his unclassified account to send the marching order information to the soldier.

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

Yes, it is a problem, but it is an integrity problem instead of confidentiality problem we concern here. We can change the high level object file access to be read only if a lower level personal trying to overwrite same file. Or maybe adding more security rules that apply to this situation in the future lectures.

Lecture 10:

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

Raise the subject level is bad which will allow subject to view more sensitive information of object and violate the security goal of the system.

Lowering the level of subject depends on if the subject contains residue high-level information of object or not. It does not violate the goal if subject is stateless subject. Otherwise lowering level with high-level information equal to write down which is bad and violate the security goal.

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

Because in real life, subjects might gain or lose trust and some information of objects might become less sensitive when time pass. With strong tranquility all the time, even when the information becomes lower level but it is still not authorized to be accessed by lower level subjects.

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

Because subject with lower level of clearance might get their hands on previously unauthorized object, hence a breach of the confidentiality. If downgrading without a very constrained rule, then lowering the level of object is dangerous.

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

Only if the object's contents are reviewed by the downgrader subject *including visual inspection by a trained human being.*

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?

System high for subjects, and any level other than system high for objects.

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

Because in real world, the ACM for large BLP system would be huge, takes a lot of rows and columns and their intersection might be blank, also since the matrix is implicit in the rules of BLP system (simple security and *-property), access permission 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.)

```
(H, {A})
   |    \
   |     \
   |     (H, {})
   |       |
   |       |
(L, {A})   |
    \      |
     \     |
     (L, {})
```

Graph skipped reflexive lines to each label itself, and transitive line from (L, {}) to (H, {A}). Also can't draw arrow with editor, here all arrow point upwards in the existing 4 lines.

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?

LUB:
a) List all the labels dominates label A in listA, including label A itself
b) List all the labels dominates label B in listB, including label B itself
c) Form a listC with the labels exist in both listA and listB
d) Sort the listC with security level; the lowest label in listC is the LUB

GLB:
a) List all the labels that label A dominates in listA, including label A itself
b) List all the labels that label B dominates in listB, including label B itself
c) Form a listC with the labels exist in both listA and listB
d) Sort the listC with security level; the highest label in listC is the GLB

3. Explain why upward flow in the lattice really is the metapolicy for BLP.

Because the metapolicy of any BLP system is to constrain the flow of information among different security levels, we use simple security and *-property rules try to achieve the metapolicy. Therefore sensitivity information should not flow “down” in the system, from a high level to low level.

The simple security would prevent lower level pulls info from high level (flow down), and *-property should prevent high level writing down to lower level (flow down). Both rules is trying to get information only flow upward in the BLP system, hence it is really the main goal, the metapolicy.

Lecture 13:

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

The metapolicy is to control the flow information only from L to H. The simple security rule only allows information flow from L to H if H dominates L by read access. The *-property only allows information flow L to H when H dominate L by write access.

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

Because the given semantics of READ is basically following the simple security rule, and the semantics for WRITE is following the *-property rule. Both of these rules are part of the BLP model, and they are specific related to read and write access.

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

Although it is stretching the simple security and *-property here for these two new operations. But at least the definition of CREATE and DESTROY does not violate the simple security and *-property rules. And for CREATE, you can always write to your own level object. Same for destroy, you are allow to modify the same level or high level object following *-property.

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

That S_L has to see varying results (during reading object F0) depending on varying action by S_H

5. Why is the DESTROY statement there?

So this piece of code and same parameter name can be reused, and this group of code can be put into a loop to pass more information.

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

No, the content of the file F0 in this example is the same with value 1.

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

Because S_L does not know that whether S_H is trying to pass a 0 or 1, it does not know which different action that SH has performed. So it must do the same thing at least until it gets the value (finding out if 0 or 1 is transmitted by S_H).

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

Because S_H have to send a 0 or 1, so the combination of binary code can be some meaningful information, that is why it needs to do different things to corresponded to the 2 different bit it trying to send.

9. Justify the statement on slide 7 that begins: “If SL ever sees...”

Because not every varying actions by S_H can be used to send a bit of information from H to L, covert channel exists or not exist depending on specific actions perform by S_H, so “if S_L ever sees varying results from…” then we know for sure that a covert channel exists.

Lecture 14:

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

Because the illegal flow of information is between the subjects within the system. Here I assuming the subjects are computer programs running on behalf of person’s security level. We can trust the human but we cannot trust the programs running under his behalf. Intuitively, human with the proper security level should know not to talk classified information to other human who is not authorized. Also the flow occurs via system resources that were not intended as communication channel. “Two human users talking over coffee” is not system resources.

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 it is not a covert channel, because if SH can write to F0, then F0 should have security level at least as high as SH, then SL cannot allow to read F0. So when SH write 0 or 1, SL would get the same result trying to read F0. If SH can not write to F0, that means F0 is has lower security level than SH, in that case, the value of F0 can not be changed by SH, no matter SH is trying to write 0 or 1, SL reading F0 has the same original content of F0. So in both case, same result instead of different result is seeing by SL no matter which different action of SH.

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

Within the system state, which is the different status of some system resource manipulated by SH

4. In Covert Channel #2?

The information is stored by in the ordering or duration of events of system.

5. In Covert Channel #3?

The information is stored by the order of cylinder read by process q depending on q’s recent read

6. In Covert Channel #4?

The information is stored by low depends on the control flow of the program, what path it take.

7. Why might a termination channel have low bandwidth?

Because termination channel only sends 1 bit of information per flow path, terminate or not terminate to represent 1 or 0 along the covert channel.

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

That both SH and SL should be able to somewhat access energy consumed by computation. In detail, SH should be able to manipulate how much energy assigned to each computation, and SL need to be able to measure energy used by computation. A mechanism for initiating both SH and SL and sequencing their access to energy consume by computation must exist.

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

Smart cards, tamper-resistant black box, integrated circuits

Lecture 15:

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

Because even if covert channel appears to transmit bit of information per illegal flow, but this piece of code can be put into a loop and with the current processor fast clock speed. In real life systems, covert channel can operate thousands of bits per second, which will send enough information with this bandwidth to cause serious threats.

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

Because not all the realistic system has high security levels, most systems contain unclassified information, also because not every covert channel can effectively transmit highly sensitive information. Sometimes eliminate certain covert channel can introduce other problems, such as DoS (denial of service) vulnerability.

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

Depends on the bandwidth of the covert channel, we can either eliminate the channel if the bandwidth is too big, or reduce the bandwidth of an covert channel by introducing noise to it, or just plain monitor and see if there is someone who is trying to exploit it.

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

In our MLS example, the use of CREATE, WRITE, READ, DESTROY, and the group of code on lecture 13 slides 5 shows a covert storage channel. SH is the sender, SL is the receiver. SH modified the attribute of F0 by creates or not creates. SL reference by read access of F0.

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

SH is the sender, it either creates an object F0 with its security level or not create the object. SL will try to create the same object right after SH's action. So for SL and with the definition of CREATE function, it either creates a lower level F0 or do nothing when F0 (high level) already exist. When SL trying to read information from F0, it will see two different results, either read success if F0 is lower level, or denial read if F0 is high level. Since SH and SL is coordinated on whether read success is 1 or 0, then 1 bit of information is passed along the covert channel. Code can be repeated used in a loop to pass more information if there is a DESTROY function to remove the object created after read access. To send information formed by letter, all you need to do is covert letters into binary code, and send the correspondent binary code in order to pass the information.

Lecture 16:

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

   Because the create function does not provides us the information of file existence attribute explicitly, we infer file existence by intuition after CREATE, and a lower level process couldn't use CREATE to get the information it would need to carry out its part of covert channel.

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

   Because the row of SRMM table is one of some system attribute, having R and M on the same row means there are some system call program command can modify and reference this same shared attribute object. Then it will meet the certain conditions must be true for a covert channel; all it need to do is some mechanism to coordinate the information bit.

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 in the column of SRMM table, we are looking at different system attributes. It violates the first must be condition of a covert channel, "Both sender and receiver must have access to some attribute of a shared object".

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

   Because we can find the potential covert channel and deal with them to close security holes if needed.