Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

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 every day life?

 personal security, Corporate security, Personnel security, energy security, Homeland security, Operational security, Communication security, Network security, System security

2. What do these have in common?

 security; protection of assets against threats

3. Have you been a victim of lax security?

 Yes, my laptop was infected with trojen virus.

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

 Most likely would be infected. Virus comes thru internet(www). When it gets infected, the computer gets slower, processing things slower than before.

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

 I use virus/internet security program called Norton 360.

6. Do you think they are probably effective?

 Yes. they help me find out whether I have been infected or not and fix the problem.

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

 I think the quote is telling us truth. As you learn computer programming, you learn alot and will acquire skills that may hack into other system. A person who is not a programmer can hack too with the help of hacking tool program these days.

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

 It is important to learn about computer security, so that you know what is going on and can prepare for the coming infection.

Lecture 2

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

 The world is changing fast. Technology is one of them that changes dramatically. Its speed of getting developed is more than an exponential function. Because of the rate, the new threats occurs which we are not prepared to prevent beforehand.

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

 We may say Yes and No. We can enumerate the bad things currently exists but as I stated earlier in #1, we are not prepared for the future unknown new threats that will occurs.

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

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com
 The defender has to find and eliminate all exploitable vulnerabilities, while the attacker only needs to find one.

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

 Yes I do agree with them. Unless you do not connect to internet/use computer, the perfect security is probably impossible in any useful system.

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

 since you can never achieve perfect security, there is always a tradeoff between security and other system goals.
Functionality, usability, efficiency, time-to-market, 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 I agree. Risk management is a process for an organization to identify and address the risks in their environment. This is what security does.

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

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

- Risk acceptance : risks are tolerated by the organization. Sometimes the cost of insurance is greater than the potential loss.
- Risk avoidance : not performing an activity that would incur risk. (ex: disallow remote login)
- Risk mitigation : taking actions to reduce the losses due to a risk; most technical countermeasures fall into this category
- Risk transfer : shift the risk to someone else. (ex: most insurance contracts, home security systems.)

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

- Annualized Loss expectancy effectively computes the "expected value" of any security expenditure.

5. List some factors relevant to rational risk assessment.

- technical, economic, psychological

Lecture 4

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

- The lists on slides 3 are mechanisms for protecting one or more of the major aspects such as confidentiality or integrity.

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

- It all depends on what I do on computer. For example, if I am searching a certain item online, then Availability is more important than Integrity.

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

- If my data is not equally sensitive, then we may separate the data by rating which can be less secure and group them and categorize.

4. Why might authorizations change over time?

- because of the threat coming from outside.

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

- Yes. availability and reliability are more related to each other than availability and security. We want to make sure how reliable the sources are when I need them, not secure matter.

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

- Such as bank account, pay transaction., etc.

Lecture 5

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

- Confidentiality, integrity, and availability

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

- The metapolicy is often too general to provide adequate guidance

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

- Who can view the students' academic records, who can modify the records,

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com
who controls the whole system of students file

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

 Could be. such as authorization.

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

 Faculty/staff may not use student SSNs in documents/files/postings.

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

 Often the metapolicy will be in terms of confidentiality, integrity, and availability; the policy will be in terms of mechanisms like firewalls, encryption, locked drawers, etc.

Lecture 6

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

 The confidentiality of information - no person not authorized to view a piece of information may have access to it. For this thought experiment we are only concerned with confidentiality, not integrity or availability.

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

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

 Information at different "sensitivity" levels: the war plan, the defense budget, etc.
individuals permitted access to selected pieces of information: General, privates, colonels

3. Why do you think the proviso is there?

 For confidentiality

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

 Information is parcelled out into separate containers labeled according to their sensitivity level. The label contains both a hierarchical component and a set of catefories.

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

 Some security officer makes these labeling decision. How they are made is outside the scoop of out concern.

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

 1. The Normandy invasion is scheduled for June 6. 2.The British have broken the German Enigma codes. 3. The base softball team has a game tomorrow at 3pm. 4. The cafeteria is serving chopped beef on toast today. 5. Col. Jones just got a raise. 6. Col. Smith didnt get a raise. 7. so on

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

 Urgent, Top urgent.

8. Justify the rules for “mixed” documents.

 The document contains both sensitive and non-sensitive information

Lecture 7

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

 "labels" on humans indicate classes of information that person is authorized to access.

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

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

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

 Any subject should have access to the minimum amount of information needed to do its job. This is as close to an axiom as anything in security.

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.

 Do not make sense. Because the Sensitivity and Access do not match.

Lecture 8:

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

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

 Because the above terms are often used in the type of security policy we are constructing.

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

 (L1, S1) dominates (L2, S2) iff L1 >= L2 in the ordering on levels, and S2 subsets of S1.

3. Show that dominates is not a total order.

 There are sercurity 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?

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

 Subject S with clearance (LS , CS) may be granted read access to object O with classification (LO, CO) only if (LS , CS) ¸ (LO, CO).

 The Simple Security Property shows how to use dominates to decide whether a read access should be allowed.

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

 An individual asking to see a document must show that his clearance level dominates the sensitivity level of the document.

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

Lecture 9

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

 The Simple security property codifies restrictions on read access to documents, not write access.

2. Why do we need constraints on write access?

 Because the confidentiality will be violated

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

 Subjects in the world of computing are often programs operating on behalf of a trusted user. Some program I run may have embedded malicious logic that causes it to leak information without my knowledge or consent.

4. State informally what the *-Property says.

 Subject S with clearance (LS , CS) may be granted write access to object O with classification (LO, CO) only if (LS , CS) · (LO, CO).

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

 Control over read and write operations is needed to prevent confidentiality breaches.

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

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

Lecture 10:

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

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

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

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

Lecture 11:

1. Suppose you wanted to build a (library) system in which all subjects had

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

read access to all files, but write access to none of them. What levels could you give to subjects and objects?

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

Lecture 12

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

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,{}) -> (L.{A})
 (L,{}) -> (H, {})
 (L,{}) -> (H,{A})
(L,{A}) -> (H,{A})
 (H,{}) -> (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 metapol icy for BLP.

Lecture 13

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

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

 Read: if object O exists and LS >= LO, then return its current value; otherwise, return a zero.
 Write : if object exists O and LS <= LO, change its value to V; otherwise, do nothing.

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

 Create: if no object with name O exists anywhere on the system, create a new object O at level LS ; otherwise, do nothing.
 Destroy: if an object with name O exists and the LS <= LO, destroy it; otherwise, do nothing.

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

5. Why is the DESTROY statement there?

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

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

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

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

Lecture 14

Name: Mingu Chang
EID: mc35926
CS Login: mchang
Email: mc-kpmg@hotmail.com

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

3. Where does the bit of information transmitted “reside” in Covert Channel #1?
4. In Covert Channel #2?

5. In Covert Channel #3?
6. In Covert Channel #4?
7. Why might a termination channel have low bandwidth?
8. What would have to be true to implement a power channel?
9. For what sort of devices might power channels arise?

Lecture 15

1. Explain why covert channels, while appearing to have such a low band-width, can potentially be very serious threats.
2. Why would it be infeasible to eliminate every potential covert channel?
3. If detected, how could one respond appropriately to a covert channel?
4. Describe a scenario in which a covert storage channel exists.
5. Describe how this covert storage channel can be utilized by the sender and receiver.

Lecture 16

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

 because after this operation, you know that the file exists.

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

 SRMM doesn not identify covert channels, but suggests where to look for them.

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 any shared resource matrix is for a specific system. Other systems may have different semantics for the operations.

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