UTEID: dtn384;
FIRSTNAME: Danny;
LASTNAME: Nguyen;
CSACCOUNT: dannytn;
EMAIL: dannytnguyen91@gmail.com;

Lecture 1
1. What uses of the term “security” are relevant to your everyday life?
- Personal, communication, corporate, and network security.

2. What do these have in common?
-They deal with protection and privacy of your data and prevent others from infringing on your personal life.

3. Have you been a victim of lax security?
-Yes. Easy passcode on phone.

4. What is the likelihood that your laptop is infected? How did you decide?
-Somewhat. I torrent sometimes.

5. What security measures do you employ on your laptop?
-I try not to visit sites that seem shady or suspicious. I use strong passwords for my accounts and I also use a VPN when using public wifi.

6. Do you think they are probably effective?
- Yes, I think I am more protected and informed than the average computer user.

7. Consider the quote from the FBI official on slide 10. Do you think it over- states the case? Justify your answer.
-No. Someone could hack into our national treasury and cause financial ruin for the US.

8. What is the importance in learning about computer security?
- To help contribute security in your own personal life and in business and improve overall security in cyberspace.

Lecture 2
1. Consider the five reasons given why security is hard. Can you think of other factors?
- Security measures often take too much time and people are too lazy to properly secure their assets.

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 uncountably infinite bad things that could

happen.

3. Explain the asymmetry between the defender and attacker in security.
–The defender must protect against all possible ways to exploit a system whereas the attack only needs to find one that works

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?
– I agree with this quote. It seems virtually impossible to 100% secure your system. There freedom allowed within a system to achieve your project goals can also be used to exploit and attack it.

5. Explain the statement on slide 8 that a tradeoff is typically required.
– Since perfect security is virtually impossible to attain, we must choose how much security we want and when it is good enough. The more security we have, the less functionality and system goals we have.

Lecture 3
1. Define “risk”?
– 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, since we cannot have perfect security.

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?
– I accept the risk of injury when I play sports.
I avoid the risk of going to jail by not drinking and driving.
I mitigate the risk of
I transfer the risk of paying for a new phone by buying a protection plan.

4. Evaluate annualized loss expectancy as a risk management tool.
– It allows you to put statistics and numbers to a risk so you can better assess it and make a decision.

5. List some factors relevant to rational risk assessment.
– The cost of insurance vs cost of loss due to risk, psychological and technical factors.

Lecture 4
1. Explain the key distinction between the lists on slides 2 and 3.
– The list on slide 3 are ways of protecting the 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 because I wouldn't want people to see what I was doing and knowing my login information.

3. What does it mean "to group and categorize data"?
- You have to group data according to their sensitivity in order to protect them from unauthorized access.

4. Why might authorizations change over time?
- Access levels may change. People might require access for a certain task.

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related?
- Companies can lose money when their websites are down due to DoS attacks. Therefore, security measures must be taken in order to prevent this from happening.

6. In what contexts would authentication and non-repudiation be considered important?
- When ordering something online. You want to make sure you are ordering from a true source and they cannot deny the transaction afterwards.

Lecture 5
1. Describe a possible metapolicy for a cellphone network? A military database?
- The metapolicy for a cellphone network would be to have customers' cellular networks available so they can be reached.
The metapolicy of a military database would be to keep it confidential and out of enemy eyes.

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.
- Do not use students social security numbers in files. Destroy any documents containing SSNs unless they are deemed necessary. Necessary documents must be kept in a secure storage.

4. Could stakeholders' interest conflict in a policy? Give an example.
- Yes. They might compromise the security of a system in order to benefit themselves.

5. For the example given involving student SSNs, state the likely metapolicy.
- Keep students SSNs confident.

6. Explain the statement: ”If you don’t understand the metapolicy, it becomes difficult to justify and evaluate the policy.”
- Without understanding the security goals of a system, the rules to implement security seems arbitrary and and random.

Lecture 6
1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?
- We wouldn’t want the enemies to know our plans. There are also aspects of integrity and availability. We want the right people with the right clearance level to access the documents. They should also be readily available so they can be accessed quickly.

2. Describe the major threat in our MLS thought experiment.
- The wrong people could access highly top secret information and leak it to the enemy.

3. Why do you think the proviso is there?
- We are mostly trying to keep the highly sensitive information out of the wrong eyes (those with lower clearance).

4. Explain the form of the labels we’re using.
- They are split into hierarchical categories that reflect sensitivity and the need-to-know category that is an unordered set.

5. Why do you suppose we’re not concerned with how the labels get there?
- Because then we would have to account for the label (access level and category) of the person putting on the labels.

6. Rank the facts listed on slide 6 by sensitivity.
- From most sensitive to least:
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.
-
(Top Secret: {Management}) - The Normandy invasion is scheduled for June 6.
(Secret: {Management}) - The British have broken the German Enigma

codes.
(Confident: {Personnel}) - Col. Jones just got a raise.
(Confident: {Personnel}) - Col. Smith didn't get a raise.
(Unclassified: {General}) - The base softball team has a game tomorrow at 3pm.
(Unclassified: {General}) - The cafeteria is serving chopped beef on toast today.

8. Justify the rules for "mixed" documents.
- Different documents can contain mixed need-to-know information. You must have clearance to all of the mixed categories in order to access that particular document, otherwise you might see information you have not been cleared to see.

Lecture 7
1. Document labels are stamped on the outside. How are "labels" affixed to humans?
- Humans are assigned clearance or authorization levels

2. Explain the difference in semantics of labels for documents and labels for
humans.
- For documents the labels indicate the sensitivity of the information contained whereas for individuals, the labels indicate the authorization (clearance) to view certain classes of information.

3. In the context of computers what do you think are the analogues of docu- ments? Of humans?
- documents are analogous to the files on computer and the humans are analogous to the users with permissions.

4. Explain why the Principle of Least Privilege makes sense.
- Because the individual should be given the minimum authorization in order for them to perform their task.

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.
- pair 1 makes sense since the clearance level matches exactly the sensitivity level
pair 2 - the sensitivity level (top secret) is higher than the clearance level (secret)
pair 3 - the clearance level (secret) is higher than the sensitivity level

Lecture 8:
1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?
- To make it easier to conceptualize how security policy works in

terms of object orient programming.

2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).
- Reflexive: a label can dominate itself
(L, S) dominates (L, S)because L ≥ L and S is a superset of itself.
Transitive: A dominates B and B dominates C, therefore A dominates C
(L1, S1), (L2, S2),(L3, S3)
L1 ≥ L2 and L2 ≥ L3 therefore L1 ≥ L3.
S3 ⊆ S2 S2 ⊆ S1 therefore S3 ⊆ S1
Antisymmetric: A dominates B and B dominates C is not equal to C dominates B and B dominates C.

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?
- The labels of the subject and object must be the same.

5. State informally what the the Simple Security property says.
- A subject can read an on object only if its label dominates the subject's label.

6. Explain why it's "only if" and not "if and only if."
- Because there are other conditions that must be true as opposed to it being the only condition.

Lecture 9
1. Why isn't Simple Security enough to ensure confidentiality?
- It does not say anything about write access so someone could write something somewhere to violate confidentiality.

2. Why do we need constraints on write access?
- A cleared person could write classified information somewhere it could be accessed by unauthorized parties.

3. What is it about computers, as opposed to human beings, that makes that particularly important?
- They may have malicious logic to leak information without the user's consent or knowledge.

4. State informally what the ∗–Property says.
- Users may right to objects that have labels that dominate the user's label.

5. What must be true for a subject to have both read and write access to an object?
- The labels of the object and subject must be the same.

6. How could we deal with the problem that the General (top secret) can't send orders to the private (Unclassified)?
- Make the private have higher clearance for certain orders/documents.

7. Isn't it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.
- Require read and write access to overwrite the war plan, or have higher clearance

Lecture 10:
1. Evaluate changing a subject's level (up or down) in light of weak tranquility.
- Changing a subject's level down might compromise security since they previous had access to classified information. Changing the level up on the other hand will only give them clearance to more classified information and will not comprise security.

2. Why not just use strong tranquility all the time?
- Because some subjects may need higher access in order to do their job. Alternatively, the object's level could be lowered.

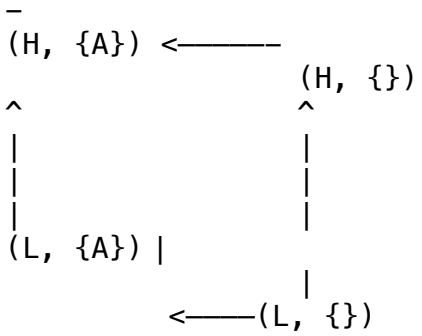
3. Explain why lowering the level of an object may be dangerous.
- Because then information that was previous classified will visible to lower level subjects, potentially violating security.

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.
- They have the same label as the object being lowered to insure that no classified information is leaked.

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?
- The subjects would have to be a higher level than the objects.

2. Why wouldn't you usually build an access control matrix for a BLP system?
- The matrix will be too big for realistic systems because there would be too many subjects and objects.

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.)



2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?
- To find the GLB, find the smallest subset of that label. Move up the path to find the LUB which is the superset of that label.

3. Explain why upward flow in the lattice really is the metapolicy for BLP.
- Information is only allowed to go from low to high (write up) and the higher level can read down.

Lecture 13
1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.
- To ensure BLP rules, you can only write up, L writes to H (∗- property), and read down, H reads L (simple security).

2. Argue that the READ and WRITE operations given satisfy BLP.
- You can only read an object if the subject’s label dominates the object’s label. You can only write if the subject’s label is dominated by the object’s label.

3. Argue that the CREATE and DESTROY operations given satisfy BLP.
- You can create only at your level to prevent leaking classified information elsewhere (read and write access).
You can only destroy an object if the object’s label dominates the subject’s label (write up).

4. What has to be true for the covert channel on slide 5 to work?
- There are two subjects, one at level H and one at level L working together in a BLP system.

5. Why is the DESTROY statement there?
- To reset and the transition process over.

6. Are the contents of any files different in the two paths?
- Yes. Depending on what the high subject does, it could be either a 1 or 0.

7. Why does SL do the same thing in both cases? Must it?
- The results on the file depends on SH creating the file. So SL's constant actions will produce a different a output on the file based on SH.

8. Why does SH do different things? Must it?
- Yes. They are the one leaking information from H to L. SL just receives it.

9. Justify the statement on slide 7 that begins: "If SL ever sees..."
- 1/0 results are used a bits to transfer information.

Lecture 14
1. Explain why "two human users talking over coffee is not a covert channel."
- A covert channel is using the system's resources in a way it was not meant to be used to convey information. A coffee shop is a social place for people to get coffee and have conversations.

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 will write F0 at H level and SL will not be able to read it.

3. Where does the bit of information transmitted "reside" in Covert Channel #1?
- From the error message SL receives by attempting to access the high level resource.

4. In Covert Channel #2?
- The time that p relinquishes the processor.

5. In Covert Channel #3?
- The order that q receives the cylinder.

6. In Covert Channel #4?
- The value of l.

7. Why might a termination channel have low bandwidth?
- You would have to wait until the channel to completely finish or terminate in order to receive information.

8. What would have to be true to implement a power channel?
- There must be a way to measure the amount of energy consumed from the low level and a way to produce a specific amount of energy from the high level.

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

Lecture 15
1. Explain why covert channels, while appearing to have such a low band- width, can potentially be very serious threats.
- Over time, the bits can be used to transmit classified information. They also 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?
- They are too many and the cost of trying to eliminate every threat will have an impact on the performance.

3. If detected, how could one respond appropriately to a covert channel?
- By eliminating it, restricting the bandwidth, or monitoring 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 receiver can reference the attribute, and based on the sender's actions, the attribute may or may not be there and indicates to the receiver a bit of information.

Lecture 16
1. Why wouldn't the "create" operation have an R in the SRMM for the "file existence" attribute?
- By creating a file, you are modifying it.

2. Why does an R and M in the same row of an SRMM table indicate a potential channel?
- Because it allows for a sender and a receiver to create a covert storage channel between 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?
- R and M should not be in the same column; it would violate the security of the system.

4. Why would anyone want to go through the trouble to create an SRMM table?
- It suggests where to look for potential covert channels.