Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

Lecture 1

1. What uses of the term "security" are relevant to your everyday life?

Home, Food, School, Personal, Network, Computer

2. What do these have in common?

They all protect against threats.

3. Have you been a victim of lax security?

It depends on the context of lax.

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

90 percent, given that I surf the web very often and there is a recent study by Consortium saying that out of 32,000 Website, nearly 97% of sites carry a severe vulnerability.

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

Authentication
Use antivirus software(mitigate)
Avoid threatening websites
avoid storing confidential information

6. Do you think they are probably effective?

They are "probably effective" but they are still vulnerable

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

No, I think this quote is entirely true. Confidential information about defense weapons, nuclear arms, or infrastructure are vulnerable to fall onto the hands of terrorists.

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

Educating yourself about computer security can enhance own- protection, contribute to security in your workplace, enhance the quality and safety of interpersonal and business transactions, and improve overall security in cyberspace.

Lecture 2

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

Sometimes security is out of your hands, it depends on what others do and that is impossible to control. If security is about ensuring that bad things never happen, it is impossible that every individual cares about security. For example, someone or something always betrays the system.

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

No, the quote in answer 2 says " "A good attack is one that the engineers never thought of". By logic this is impossible to enumerate.

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

The defender has to make to effort to find all possible vulnerabilities that they can think of, however by answer 2 it is impossible to enumerate all of them, then there has to be at least one vulnerability that the attacker can exploit. The asymmetry is many to one.

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

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

Agree. It is impossible to achieve perfect security. Even taking the steps that Chang mentioned would not protect it from somone finding that computer.

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

If you care mostly about some particular part of a project you will always make risk to achieve the goal that you mostly desire in your software. For example, if you want to sell your software it will take you an extra step to make it more beautiful maybe make the product more aesthetically appealing although it takes to decrease security measures and efficiency.

Lecture 3

1. Define "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. Some results are worth the risk

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

(Acceptance) Car driving accident- I accept it because I need to go to work and school otherwise I will not have anything to eat.

(Avoidance) Running a red light- I avoid it to prevent accidents and fines.

(Mitigation) Car maintainance- Reduce the risk of having an accident.

(Transfer) Car insurance- Transfer the cost of fixing my car to an insurance company.

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

The expected monetary loss that can be expected for an asset due to a risk over a one year. ALE = SLE * ARO, where ALE is the annualized loss expectancy, SLE(single loss expectancy) and ARO(annualized rate of occurrance).

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 list on slide 3 such as cryptography are mechanisms used for achieving the goals in the list of slide 2. They 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.

Since I don't have top secrets to hide, confidentiality is not a problem for me. I am the only person who uses my computer so I have no issues of someone else modifying my data.

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

The most important aspect is availability of resources, since I need assignments to be done on time.

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

In other words how do I organize the data so that I can distinguish the levels of confidentiality and availability.

4. Why might authorizations change over time?

Maybe a person or a process is no longer in the system or doesn't exist so modification of authorizations must be done. Someone has been promoted to handle more confidential data.

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

Threats to availability are often called denial of service so many virus and worm attacks are DoS attacks which cost businesses an billions of dollars.

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

When a product is ordered online through an online store we want to make sure that the person ordering it is legitimate and the product will be shipped to the corresponding address.

Lecture 5

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

In cell phone network the metapolicy is that all of the calls are received to the correct recipient and the calls are not interrupted.

For a military database we want all data to be secret so that only authorized personnel can access it.

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

A policy is a refinement of an existent metapolicy.Policy is a mechanism to achieve the goals of a metapolicy.

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

- Faculty/staff may not use student SSNs in documents/files/postings
- Documents containing SSNs must be destroyed unless deemed necessary
- Documents containing SSNs and deemed necessary for retention must be kept in secure storage

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

Yes,

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

All students' confidential information must be kept in secure storage.

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

It will not become clear what are the priorities or main aspects to be protected and from there it will not be evident which policies best protect the interest of the metapolicy.

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

Lecture 6

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

Because of of various sensitivity levels and individuals having various degrees of trustworthiness such as the war plan, the defense budget, the base softball schedule, etc. For individuals we have access to selected pieces of information such as privates, colonels, secretaries, janitors, spies, etc. No aspects of integrity and availability.

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

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 emphasize the importance of confidentiality as the mos important.

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

Information is parcelled out into separate containers (documents/folders/objects/files) labeled according to their sensitivity level.

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

This falls in the aspect of integrity.

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

- The British have broken the German Enigma codes.
- The Normandy invasion is scheduled for June 6.
- Col. Smith didn't get a raise.
- Col. Jones just got a raise.
- The cafeteria is serving chopped beef on toast today.
- The base softball team has a game tomorrow at 3pm.

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

- Top Secret
- Confidential
- Confidential
- Confidential
- Unclassified
- Unclassified

8. Justify the rules for "mixed" documents.

1. Need to protect information from being accessed from unauthorized individuals.

2. We need to protect that no other individuals can view other categories not permitted.

Lecture 7

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

Each individual has a set of "need to know categories" indicating domains ofinterest in which he or she is authorized to operate.

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

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

Labels for documents are hierarchical security level indicating the degree of trustworthiness to which he or she has been vetted;
Labels for humans are a set of “need-to-know categories” indicating domains of interest in which he or she is authorized to operate.

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

Processes are analogous to humans and documents is analogous to data/files.

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

In order to have better control of the flow of information it is convenient that individuals know the least sufficient amount of information. It is harder when to take control of the flow of information if more individuals have access to information not needed.

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.

For the first row it makes sense that some individual with higher level of confidentiality such as secret and crypto can view anything below it such as confidential and crypto.

Second row does not make sense since someone with secret clearance should not be able to have access to something higher than secret, in this case something with top secret sensivity

Third row makes sense because an individual with secret clearance has a higher level of confidentiality than any unclassified information.

Lecture 8

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

We are having an analogy to a sentence, in our case we are referring to an operation in which the subject is the entity doing the operation, objects is the information protected and the action is the operation.

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

We need to understand that a partial order is reflexive, transitive, and antisymmetric.

3. Show that dominates is not a total order.

There are security labels A and B, such that neither $A \geq B$ nor $B \geq A$.

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

L1 = L2 and S1 is a subset of S2 and S2 is a subset of S1

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

This is simply saying that subjects with higher clearance can read anything below their clearance level.

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

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

Because the rule does not work the opposite direction ie. if S with clearance (Ls, Cs) is granted read access to object O does not mean that (Ls, Cs) >= (Lo, Co) since we don't know that Co is a subset of Cs.

Lecture 9

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

The simple security property codifies restriction on read access to documents. We are worried about someone with a higher clearance to write information in a lower clearance level. This will clearly violate confidentiality.

2. Why do we need constraints on write access?

Subjects will always make the mistake to write information where classified information can be accessed by unauthorized parties.

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

Some program I run may have embedded malicious logic (a "trojan horse") that causes it to "leak" information without my knowledge or consent.

4. State informally what the *-Property says.

This says that an individual may only have write access to information with equal or higher clearance level.

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

The object must have exactly the same clearance level as the subject.

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

We need control over who read and writes operations. Authentication can be a mechanism to decide whether a read or write should be allowed.

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

An overwrite should not be allowed if the current information has been written by a subject with a higher clearance level. We give information persistence to the subject with higher priority.

Lecture 10:

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

For the case of lowering the level of a subject we don't have the risk that simple security property is violated. In the other hand, the * property is violated when we give access to higher level subject to write information that can expose higher confidentiality.

In the case of changing a subject to a higher level we risk violating the simple security property. Giving access to a low level subject to a higher level subject exposes information that violates the goals of simple security. In the other hand, a subject with a low level clearance

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

cannot compromise any confidentiality to higher level subjects, however integrity is compromised.

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

Because, 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.

Compromises classified information that could be used by lower level subjects to harm a system.

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

Information is not carried over that can compromise any higher level clearance.

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?

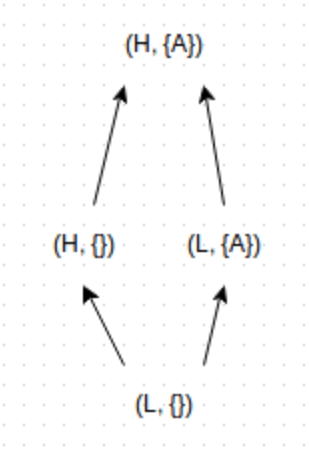
Subjects have classified level clearance and the objects are all unclassified information.

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

The matrix would be huge for most realistic systems. The matrix is implicit since 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.)



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

any two elements have a least upper bound (supremum orjoin), and any two elements have a greatest lower bound (infimum or meet).

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

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

We don't want any flow of information to flow down to prevent from any subjects with lower clearance level to compromise the information. This policy prevents us from worrying that information ever reaches lower level subjects.

Lecture 13

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

If Information can only flow up then this obeys the * property in BLP. where information can only written up

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

If object O exist and subject S wants to read O given Ls>=Lo, the READ satisfies the fact that if anything that the subject attempt to read above the its level of clearance, the object will return a 0. Otherwise it will return the current value.

For the WRITE the subject only changes the value to V if subject level is lower than the subject.

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

It is clear that if no object exist with the name O then a new one can be created at level Ls, otherwise do nothing since we might not know anything about the object. Ths satisfied BLP because we are modifying something higher.

Destroy also satisfies BLP since the object modified has a higher clearance level than the subject.

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

The system varies its behavior.

5. Why is the DESTROY statement there?

Because both channels have to do the same to avoid varying actions.

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?

It must do the same thing to avoid covert channels

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

It must do the same thing to avoid covert channels

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

It all depends on the actions of SH.

Lecture 14

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

The flow is between subjects within the system.

2. Is the following a covert channel? Why or why not?

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

Yes, SH writes 0 on object FO. Case 2 SH writes 1 on object FO. SL can read FO so this can create a covert channel.

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?

Both. Timing because of the ordering.

6. In Covert Channel #4?

Implicit.

7. Why might a termination channel have low bandwidth?

To obfuscate the timing and produce noise difference between processes.

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

There must be a difference on consumption of energy among all processes.

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

Computers.

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?

It is really hard to deal with existence, bandwidth and noise.

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.

- Both sender and receiver must have access to some attribute of a shared object.

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

- 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.

Lecture 16

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

Norman E. Lopez
UT EID: nel349
Login: nel349
noell.lpz@utexas.edu

existence" attribute?

You never know that the file exists.

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

Sharing an object , reading and modifying means that a shared resource must exist.

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. Different attributes have different semantics.

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

Provides a systematic way to investigate potential covert channels.