Emily Ngo

Emn367

Ngo.emily@utexas.edu

CS 361 Questions Week 1

Lecture 1

1. Security can refer to many contexts. In my everyday life security can refer to neighborhood security, food security, or network security. For neighborhood security, I expect that my neighborhood is actively protecting my home from robberies and vandalism in the area. Food security is knowing that food is available to sustain the population that I am a part of. Network security is knowing that my home network or work network is preventing outsiders from accessing or changing devices that are under that network.
2. In all those contexts that security can be utilized in, security is means of protecting of assets against threats. Such as neighborhood security, the asset is my home and belongings and the threat is vandalism and robbery.
3. I have been a victim of lax security when I did not follow email policies about which kinds of attachments I can download in my middle school, and ended up downloading some malware to their computer lab which made several computers unavailable.
4. I'm pretty sure my laptop is infected, none of my software, driver, or even OS was installed from a CD from someone reputable. From the day I've bought it until now it has been vulnerable from all the times I've downloaded something unknown. Sometimes I've even encountered downloads that were not authentic.
5. I've only utilized a browser extension called Ghostery, it will notify me what kind of known trackers there are on the webpage I'm on and from there I can gauge how safe it is to be on that website. The other security measure I take are ones that to avoid threats such as not opening an email with attachments on my personal laptop, and opening them elsewhere.
6. These methods are not effective as I like them to be. It is impossible to be perfectly secured. For example, I know that although Ghostery works on most HTML coded sites I also know that there is another trade off while I'm using their extension. The trade-off is that they gain my information about which sites I go to, which ads I usually try to block, and which sites I "whitelist" or stop blocking on. Ghostery has the information to create even more aggressive ads and if they sell this information then I'm a victim of lax security again.
7. No it does not overstate the case, in any case no software, person, hardware, or network is perfect. A global network is target rich, because it consists of all these components and more.
8. We want to learn computer security to be able to better our efforts for protection and reduce the vulnerabilities of being connected to the internet. If everyone can implement basic security policies the overall risk of interacting with cyberspace can be reduced as well.

Lecture 2

1. Yes another factor is that you are limited with the tools and mechanisms you already have to create a policy. If security is an afterthought, how often are things being marketed and built for

stuff that hasn't even happened yet? Over time a more creative threat might appear, but you aren't even utilized with the right technology or tools to handle it.

2. No there isn't, as long as technology grows and people are still imperfect there will never be a set number on bad things that can happen. Your program interacts with other devices and not just itself so how is it possible to enumerate "bad things" when it has not even interacted with devices that don't even exist yet, but it may exist in the next year or so.
3. An attacker only needs to find one vulnerability to exploit, but we as a defender have to find all current exploitable areas, future exploitable areas, and defend them all somehow.
4. I agree, in a system because it consist of multiple components anything could mess up, the best way to be secure it to not use it at all because you don't ever have to deal with the plethora of problems that will come with using a system.
5. One of the ways to handle a threat is to not use a functionality at all, such as emails. Some attachments are threats so if there isn't a mechanism to handle all bad attachments it's better to just not attach files to emails at all. In this case convince of sending and receiving files, or storing files within emails is a lost functionality.

Lecture 3

1. Risks is a possibility that a threat can exploit a vulnerability in an information system which will have adverse consequences. You can identify a risk after assessing your assets, threats, and vulnerabilities.
2. I agree, no security system can be perfect so software security is all about managing the risks with the limitations you have.
3. A risk I accept is I can get in a car accident if I drive a car, but since I still want to go to school I still drive knowing this fact. I know that downloading an attachment from an email might be a malicious file, so I don't download email attachments anymore. A risk I transfer is that I know that I'm susceptible to illnesses so I buy health insurance to cover the financial burden of illnesses.
4. Annualized loss expectancy might be a good tool in some situations since it gives a numerical values to risks but it doesn't represent the consequences of the risk accurately. Something might have a 1% probability of it happening but if it does happen the losses are not sustainable. This risk should still be prevented in some cases, for example, a house fire.
5. Assessing risks rationally you should consider your assets, threats, and vulnerabilities then identify a risk and from there prioritize risks to counter them and then make decisions. You want to consider factors like the technical, economic, and psychological effects of a risk. A house fire might have higher psychological effects than vandalism.

Lecture 4

1. Slide two is about the goals you want to achieve in computer security. Depending on the context security can encompass any combination of those topics. Slide three is about how you can achieve those goals from slide two, rather than goals themselves they are tools you can use to achieve one or more things from slide two. For example you want integrity of all the drafts in your email server, so you use passwords and access control to manage integrity. So slide three topics are mechanisms.

2. There are all important to me, I can't pick one over the other because it depends on what I'm doing. If it's turning in assignments I would want my integrity to be prioritized, or if I'm filling a form with my SSN I want that to be confidential. It might be the case I want a combination of confidentiality, integrity, availability or all of them.
3. It means that you need to consider how your data is differently sensitive or similarly sensitive, and from there group them so they can be managed differently by the policy you are implementing.
4. Authorizations might change due to an object becoming more sensitive to be confidential, it will receive a higher authorization so it won't be seen just by any individual.
5. The security policy implemented to keep something available must also be reliable to continue keeping an asset available. If your policy becomes unreliable then the availability is not consistent either.
6. Authentication is important to businesses, you want to make sure that no one is pretending to be a vendor or no one is pretending to be you while making a transaction. You also want them to consider non-repudiation so they can't deny the transaction and just take your money or goods.

Lecture 5

1. A metapolicy for a cell phone network is availability, you never want a person that owns a cellphone to not be able to call at any location they are at. A metapolicy for a military database is confidentiality, you don't want outsiders to know your war plans or secrets.
2. A teacher is not allowed to modify academic records after that semester is over. All records are password protected. Changes to academic records must be signed by someone that is authorized to make changes.
3. Yes it can, an investment firm wants to keep their data in the company's file server confidential, a policy says that after a file has been written to the file server it can only be viewed by authorized individuals, however employees that also use the file servers to store archives do not want this policy because they don't have it available to SSC when they are being reviewed over a fund. This policy fulfills the wanted goal, but at a price of functionality which creates a conflict between different groups in the firm.
4. Confidentiality.
5. The statement is asking, why implement a tool if you don't know what is being utilized towards? How do know how well it is performing if you don't know what it is supposed to achieve? You need a goal to be able to see how much of the goal is achieved.

Lecture 6

1. Military security is focused on keeping secrets, so that is why it is mainly about confidentiality. Military doesn't want their attack plans, location, resources to be reveal to their enemies however there are also aspects of integrity and availability. You want the Military to be able to access their resources and information needed in a time of crisis quickly and swiftly to make pressured decisions. You also want integrity to maintain the secrets and not have them change to something inaccurate. Such as an inaccurate attack plan would cause high consequence.
2. The threat is the possibility of someone being able to view a piece of information when they don't have access to it.

3. It is there to show that this experiment is only concern with one goal, any policy only needs to fulfill the goals of confidentiality and not the others.
4. Labels are in hierarchal linear form, and also a set component. So every mixed category has its own hierarchy.
5. We assume that the labels reflect the sensitivity of a particular file and the focus is how to manage those labels, so we are not concerned with the individual files but a group of them.

6 and 7

a. The Normandy invasion is scheduled for June 6. Top secret, {}
b. The British have broken the German Enigma codes. Secret, {Crypto}
c. Col. Jones just got a raise, confidential {personnel}
d. Col. Smith didn't get a raise, confidential {personnel}
e. The base softball team has a game tomorrow at 3pm, unclassified {}
f. The cafeteria is serving chopped beef on toast today, unclassified {janitorial}

8.

In order to view a mixed document the Subject must also have a higher or equal authorization, and the set of the Subject must be a superset of the Object. This reasoning is to prevent documents from being seen by someone that doesn't need to see it, if someone was authorized as Secret {Nuclear} they don't need to see Secret {Crypto} so it should be the same rule for Secret {Nuclear, Crypto} Object. When classifying a mixed document, the categories should include all the categories mentioned in the document, and that the highest appropriate level should be used to maintain that dominance.

Lecture 7

1. Labels on humans are the class of information they can access, or clearance level.
2. Labels for documents are the sensitivity of the information, and labels for humans are the clearance to view the specific classes of information.
3. In computers the people are the different account users, and the documents are the files on the computer drive.
4. Principle of Least Privilege assures that only the minimal authorization is given to perform a job, this way the individual does not have higher access to view more sensitive files than the individual. If that was the case then there is a leak of highly sensitive information to low clearance individual which violates confidentiality.
5. 1. Subject of clearance Secret is greater sensitivity than Object that is Confidential and {crypto} includes {crypto} so the answer YES makes sense.
   2. Subject of clearance Secret is lower sensitivity than Object that is Top Secret so NO makes sense.
   3. Subject of clearance Secret is greater sensitivity than Object that is Unclassified and {Nuclear} includes { } so the answer YES makes sense.
   All of these answer reflects the dominance relationship.

Lecture 8

1. Since security is used in a lot of contexts, having objects, subjects, and actions simplify each context of security in different situations.
2. Dominance
   Let A, B, and C be subjects
   a. Any subject A <= A ; any subject A dominates A (reflexive)
   b. If A dominates B then B cannot dominate A, if they do then A = B (antisymmetric)
   c. If A dominates B and B dominates C, then A also dominates C (transitive)
3. A total order is a partial order in which there are no unrelated subjects, but dominance do have unrelated subjects such as: Top Secret {A,B} and Top Secret {B,C} one does not dominate the other and vice versa
4. The two labels must be the same sensitivity, and have the same set components.
5. A subject can read access only if their clearance is greater or equal to the object's sensitivity, and they contain the categories of that object.
6. If and only if means that the subject will certainly get to read the object if it fulfills the dominance, however different systems have different implementations where one system might allow read with dominance another will require another policy to be fulfilled.

Lecture 9

1. Simple Security doesn't cover restrictions to write access, only read, so an example is a General writes orders to a Janitor. This can be a way to violate confidentiality because higher sensitive material can be copied and written down to lower sensitivity subjects.
2. An example why we need constraints on write access is what if a General tries to write orders to a Janitor to read? Confidentiality is violated because higher sensitive material has a way to leak to lower sensitive material. The General can copy and then write a secret for the Janitor to see, and that is what the metapolicy wants to prevent.
3. This can be a problem when a program operates as an authorized user, it can act as the user and access a bunch of confidential files and copy them elsewhere at lower sensitivities.
4. * Property says a subject can write only to objects of higher or equal sensitivity, and the object contains the set components the subject has.
5. A subject can have both read and write access if the object is equal in sensitivity and equal in sets.
6. We can lower clearance level of the General to Unclassified if there isn't a Strong Tranquility Property in place.
7. We can restrict the write action to only write as a new file, if the file already exists then the action does nothing, if the file doesn't exist it will be made with whatever that was specified to be written in it.

Lecture 10

1. You can change a subject level down because it will lose the ability to read higher sensitive material instead of gaining it. The subject still has to "write up" so both policies are not violated. However, you can't change a subject level up because lower sensitivity subjects can read access higher sensitive material which defeats the purpose of the Simple Security Policy.

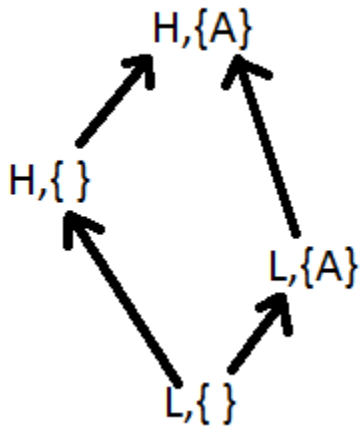
2. Strong tranquility is inflexible, what if over time a bunch of files written by subjects over time do not reflect the sensitivity level of the label? For example, someone accidently wrote “Baseball game is moved to Sunday” and made it top secret, there is no way to downgrade this. Another example, over time a subject is demoted, that person is no longer trusted with highly sensitive material. You can’t change his label.
3. You have to have some restrictions on lowering an object, if this action was utilized by a program, it may be the case that ANY file can be downgraded for access. In this case the confidentiality and simple secure policy are both violated.
4. One way to downgrade an object without risking confidentiality is hiding its existence after the downgrade, and it won’t be seen until a subject uses a write action. Then it will exist again. This way if a highly sensitive material was accidently downgraded, other subjects can’t see it.

Lecture 11

1. Give all the subjects label High {A, B, C} and all the files label Low {}; in other words all users get the highest label they can and all file the lowest label they can.
2. Access matrix would be too larger to be useful, so you don’t need to.

Lecture 12

1.



2. To find LUB start with the highest level label and compare it to all the other until you find the label where it is dominant over all the other labels in the lattice, and then continue until you run out of labels, the last label to be able to complete that algorithm should be the LUB.
   To find GLB start with the lowest level label and compare it to all others until you find the label where it is dominated by all the other labels in the lattice, and continue until you run out of labels, the last label able to complete that algorithm should be the GLB.
3. A path in the lattice represents information that is allowed to flow, which can happens in two ways subject at point A can read object at point B or subject at point B can write to object at point A. No paths represents how Simple Security and * property prevents the information flow and maintains confidentiality. In other words a subject can write to the last point of the path, or object can be read by subject at the last point of the path.

Lecture 13

1. The metapolicy is preventing low level subjects from being able to read high level subjects; in other words information cannot ever flow down. The policies will allow the information to only flow from low to high which is represented in the graph, if there is a path otherwise something is wrong. So there should never be a path that lets you write down (H point towards L).
2. READ says that only Higher leveled subjects can see lower level objects, there is no information flow going from high sensitive object to low subject, so it satisfies the BLP metapolicy. WRITE says only lower level subjects can write to higher level objects, there is still no information flow going from high sensitive objects to low subject, so it satisfies the BLP metapolicy.
3. Create and destroy modifies objects, but still does not allow the contents of file to be shared by anyone so it does not violate the BLP metapolicy.
4. Both Sh and Sl must be communicating at the same time.
5. Destroy will allow you to reproduce the file again and try again for the bit of information.
6. No, because Sl always write over the file anyways.
7. It has to do the same thing to act as a control and see where the results differ, you don't know if something is behaving differently unless you try over and over.
8. Sh does different things in order to signal different system attributes.
9. Varying actions can be manipulated to send information over this channel and convey information.

Lecture 14

1. Covert channels implies that you are communicating through means that are typically not used for communication.
2. Not a covert channel because read will be 0 either way if the file did exist.
3. It resides System state
4. It recorded in the duration or order of events on the system/ processor
5. IT resides in the head of the cylinder
6. Stored in variable H
7. You have to wait to see why a process terminates and that might take a while
8. You have to monitor the power usage at all times
9. Cars, phones, laptop, anything that consumes energy

Lecture 15

1. Covert channels on processors can operate at thousands of bits and not slow down the system process.
2. Eliminating all covert channels might mean giving up a system implementation that is functional, there are other ways to cope with channels by reducing bandwidth or monitoring the channel
3. You can reduce bandwidth by introducing noise so information would be harder to obtain, or monitor when someone is exploiting the covert channel.
4. Two computers share a processor, but have different access authorizations, however the computers have an attribute to tell if a file exist or not by returning a 1 or 2 to the person accessing it. 1 meaning it exists but is not accessible, 2 being it does not exist.
5. The sender can modify the attribute that is shared by the receiver and exploit the resource that is being shared.

Lecture 16

1. It doesn't inform you if the file existed already. You assume.
2. You have the tools to modify and reference a file, which all you need to communicate a bit of information about the system. Some combination of these actions might be able to do that.
3. One column means only one action is used to reference or modify which isn't enough to create a control and test the behavior of the system.
4. To detect potential covert channels.