Chad Custodio

Cgc735

Aitan791

chadcus@gmail.com

Week 1 Questions

Lecture 1

1. I have to make passwords for all accounts that I make for most websites for authorization purposes. My computer also has a firewall to protect the integrity and privacy of my data.

2. These are used to protect any sort of outsiders to mess/see my personal assets

3. Not yet

4. My laptop might be infected with something but I probably don't know about it. Even though I don't have and performance issues, there might be something that made it onto my computer that is unrecognizable and doesn't affect performance.

5. I just use a firewall. I personally don't like security software.

6. I believe that the firewall works well enough. It always asks what needs to be authorized for access to my computer.

7. I think it is a pretty true statement because we are all connected to each other in some sort of way over the internet. If our information starts to get meddled with then it would be complete chaos determining who did what with who's information

8. To keep the majority of our assets safe from people that want to take advantage of other people that don't know too much about technology.

Lecture 2

1. Another reason why security is hard is because there can be new ways to breech security as time goes on.

2. I don't think so because there are so many different possibilities when it comes to subverting security. When you try to prevent too many bad things from happening, then you run the risk of preventing good things from happening as well.

3. The defender has to think of all the possible ways that the attacker might be able to get through the security. The attacker only has to find one weak point to be able to take advantage of security

4. I agree because there is no realistic way to prevent every single possibility of an attack. And just by having the computer on runs the risk of an attacker seeing and messing with your assets because of how we are all connected together so easily.

5. Trying to protect everything will cause a lot of performance issues because you have to be able to constantly check every single piece of data. This requires a lot more time and will cause these trade-offs to happen.

Lecture 3

1. It is the possibility that a threat will adversely impact an information system by exploiting a particular vulnerability.

2. In some ways it is because it helps to target the more obvious things that might affect your computer.

3. In terms of computers, I accept potential changes to my computer when updating video games, I avoid sites that I don't trust, I mitigate risk by flushing my computer every year, I have insurance on certain computer parts to transfer my risk

4. It isn't the most full proof risk management because the most expensive risk that has a small incidence can still happen especially if the attacker is really good.

5. The cost, how often an attack happens for a certain aspect.

Lecture 4

1. The list on page 3 are what you use for the list on page 2.

2. Confidentiality because if they cannot see what you have then you don't really need to worry about whether they can change or access the data

3. Grouping together what you deem to be important and what you don't care too much about.

4. In case there have been certain breeches to integrity already.

5. It is good to have things run well and quickly which is what it means to be reliable and the main problem for availability would be high traffic, causing things to run slowly.

6. When making online purchases in a video game because you want to make sure that it is on your account and that the transaction for the real money purchase went through.

Lecture 5

1. The availability of the network so that you don't miss calls or notifications. Military database would be more about confidentiality

2. You need ways to refine and strengthen your metapolicy

3. Faculty and staff cannot use student's SSN. Documents containing a SSN must be destroyed. If they aren't destroyed for a good reason, they must be in secure storage. This is for student confidentiality

4. Yes because we may not want our information to be stored at all but there are some rules that might keep the information, causing there to be a little bit of conflict of interest.

5. To help with the student's confidentiality so that nobody will be able to see their SSN and use it for other things.

6. If you don't know what your security goals are, then it would be hard to determine what different aspects about security to focus on to help with those security goals.

Lecture 6

1. Because it is important to not have classified information leaked to the public/the enemy forces. You also wouldn't want certain things to be altered, especially if it is something that is controlled remotely and you would want to have it working efficiently at all times.

2. Enemy spy

3. Confidentiality

4. We will use folders that we stamp with the label.

5. We are really only concerned that the label is on. How it gets there is outside our scope

6. Unclassified: softball game, cafeteria serving chopped beef
Confidential: People getting raises
Secret: Invasion of Normandy
Top Secret: The British have broken the codes

7. Documents: softball game, cafeteria serving chopped beef, people getting raises
Files: Invasion of Normandy, the British have broken the codes

8. Because if you label something lower than necessary, then people without proper authorization will be able to see that info because it wasn't grouped with something at a higher level.

Lecture 7

1. By their military rank/occupation

2. The document just indicates the type of information whereas the individual indicates how trustworthy the person is.

3. Files and individual pieces of data for documents and users/firewalls for humans.

4. If you don’t give people information, they won’t leak it. This helps limit who needs to know what so that there is less of a chance for this information to be leaked.

5. The first and third example make sense because they aren’t going outside of their clearance level for the information that they want. The second example is a little confusing because even though the sensitivity is higher than their clearance, he is still works with Crypto, which would benefit him from seeing the information.

Lecture 8

1. It helps to distinguish what role the humans and documents play in the situation.

2. It is partial order because something that is higher level should be able to see whatever it is below it but not the other way around.

3. It isn’t total order because something be at the same level but will pertain to something else, so neither should be able to access the other.

4. Both the level of the document and the set of the data must be higher than the other.

5. There is a way to gain access to information if you are at the proper level, but there are certain things that might prevent that from happening.

6. Because syntactically that would mean that you would always be granted this information without taking into account all the different security hurdles.

Lecture 9

1. Because information from a higher official might put top secret information into something that is readable to lower ranking people.

2. Sometimes you cannot trust what information might be leaked from the higher level writing somewhere else

3. We need to make more rules to make sure that programs won’t write your important information into a lower level, making that information available for more people to see.

4. You cannot write information into a level that is lower that your own.

5. You are at the same level and the set of information is the exact same.

6. By giving him access to an Unclassified account to get that information out there.

7. By saving the old war plan in some sort of way.

Lecture 10

1. Changing the level of the subject to be higher will grant them read access to everything below it and changing to it be lower will give them the ability to write whatever they want to change in the higher levels.

2. It is overly restrictive for things that might need to be moved around a bit.

3. It is essentially giving a chance to write down.

4. If the level of the subject is still higher, then there should be too much of a problem with lower the level of the object.

Lecture 11

1. High level subjects and low level objects

2. It is better to just evaluate right away than take up a lot of space and time.

Lecture 12

1.

$$\begin{tikzcd} (H, \{A\}) \\ (L, \{A\}) \arrow[u] \end{tikzcd}$$

2. By starting with the lower level label and finding the upward flow between that and the higher label along with their bounds

3. Because if information were allowed to flow downward, then we would run into the problems of writing down, which isn’t ideal.

Lecture 13

1. The higher level pulls the information up and lower levels will push new data upwards

2. Because it will return 0 in the case that the level of the subject is lower than the object for READ and in the case that the level of the subject is higher than the object for WRITE, there is no flow of information going downward.

3. It satisfies BLP because nothing is ever created at the same level. Everything is kept in the lower levels and deleted in the higher levels if the same object exists. These two things show that information is being kept so that information cannot be leaked downwards

4. The higher level subject shouldn't create an object.

5. So that there is no longer and object with that name. Basically recycling so that there are no future read problems.

6. Path 1 returns 0 and path 2 returns 1

7. It does the same thing because it helps to distinguish whether there are varying result with varying actions with the higher level subject. It should be the same because it will be harder to find covert channels if the lower level keeps changing.

8. It does different things because the higher level subject is the one sending varying information which will be assessed by the lower level subject to determine whether or not a channel is covert. It should be this was as it is easier to change what you send rather than the process of using that information.

9. This is true because if there is a bad pattern with varied results then that must means that there is something wrong at the higher level of things that could mess up the metapolicy.

Lecture 14

1. Because it doesn't apply within the contents of the system. It is outside the system.

2. Yes because a lower level subject is trying to read the contents of a higher level subject.

3. The SH

4. Process p

5. the disk drive

6. h

7. All you need to do is check if there is a termination sequence.

8. The low level process must sense it and high level process my modulate it.

9. Any sort of mobile device.

Lecture 15

1. They can send thousands of bits of information per second

2. Because it can be hard to detect these covert channels

3. Monitor it to see if someone is trying to exploit it.

4. When a lower level and higher level subject have access to a shared object.

5. The sender modifies while the receiver references these changes.

Lecture 16

1. Because it is hard for the receiver to get the information of whether or not a file exists or not after the create operation because that file might already exist.

2. Because there at means that there is a mechanism where someone can modify and reference it, which is needed for a covert channel.

3. No, it depends on the semantics of the system.

4. Because you can find the covert channels and eventually deal with them.