NAME: Terry Liang
EID: Twl378
CSID: tliang
EMAIL: Liang810612@hotmail.com

Assignment 1

Lecture 1

1. Personal security, Network security, System Security.
2. These securities are being used to protect my personal assets from any kind of the threat.
3. Yes, with my network security. My laptop was infected with Trojan horse virus.
4. I would say that my laptop is high infected now because I do not have any anti-virus software installed in my laptop.
5. I do not have any security system to detect any malicious virus. I only depend on the security system that Google provides when I browse internet using Chrome.
6. I do not think they are really effective and that is why I do not install anything on my laptop.
7. Yes, I think someone in the world is possibly capable of doing things like that. We often see news about some networks or systems of big company being hacked by hackers. Because any security is not perfect, there is a big chance that someone will exploit the vulnerability of a system and successfully have the ability to access any computer system.
8. To enhance your 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. I think the five reasons pretty much sum up the difficulty to come up with a perfect security.
2. Yes, but it might not be perfect. We can always enumerate the bad things that could possibly happen to a program, but I do not think we can think of a perfect way to enumerate all the bad things.
3. The defender has to find and eliminate all exploitable vulnerabilities; the attacker only need to find one.

4. Yes, this is actually what my thoughts on perfect security. If we never own a computer, we then do not need to be afraid of any malicious attacks out there.

5. Security is meant to prevent bad things from happening; one side-effect is often to prevent useful things from happening. Because we often build a system for functionality first, we often have to modify later for security purpose and hence reduce our functionality.

Lecture 3

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

2. Yes, I think so. Since we cannot produce any perfect security, we try to reduce the risk.

3. Risk acceptance: I do not buy insurance for some of my stuff because I know the stuff itself is worth less.

   Risk avoidance: I do not click on suspicious link that would lead me to bad result.

   Risk mitigation: install anti-virus software to protect my computer.

   Risk transfer: Buying insurance for my car because car is worth more than the insurance.

4. There are event that are almost unlikely to happen, but it will cost a lot if it really happen.

   Most events are likely to happen, but it will cost you in an affordable range.

   We need to invest on both options to reduce the possible losses.

5. What would happen? What is the possibility that it would happen? Why would it happen? What possible impacts would it bring? Can we reduce the risk?

Lecture 4

1. Slide 2 is more like a big idea of what type of security we focus to build on and slide 3 is more like the mechanisms for protecting one or more of the major aspects.

2. I would say confidentiality. I have personal information that do not want to be seen by others.

3. How do we label the data to distinguish its level of security

4. Because some people might be promoted and gain a higher access and that changes the authorizations.
5. Availability often makes sure that the resources available in a timely fashion and reliability is often relates to availability because we need to make sure that if any faults occur the system will compensate or recover.
6. When you are paying something with your credit card online, you do not want to receive a message says that they did not receive your payment.

Lecture 5

1. It might be to consistently provide services to customers. Military database would want confidentiality as its metapolicy.
2. The metapolicy is often too general to provide adequate guidance and may be subject to multiple interpretations.
3. Faculty may not use student SSNs in documents, staff without permission may not change students' academic records, student do not have the power to see others student's' record.
4. Parents might be the stakeholder that want to see the grades of their children, but it conflicts the policy.
5. Confidentiality.
6. We cannot build policies without a bigger purpose. It would be confusing without metapolicy.

Lecture 6

1. I would say because military database contains lots of top secret documents and information. Yes, military security would also have to deal with integrity and availability. They would not want someone to be able to change some contents of important stuff.
2. The major threat would be not person not authorized to view a piece of information may have access to it.
3. Because we do not care if someone is able write something. Our goal is no one will leak any information.
4. We use different labels to indicate that only certain group of people are only able to read equal or less than their level.
5. Because they are usually people with great authority.

6. 1,3,4,5,6,2
7. 1,3: unclassified 4,5: confidential 5: secret 6: top secret
8. Use the highest appropriate level, use both categories.

Lecture 7

1. They are included in the inside bracket.
2. For documents the labels indicate the sensitivity of the information; for individuals the labels indicate the authorization to view certain classes of information.
3. Programs; users
4. Because not everyone needs to know everything. They just need what they need to know for their jobs.
5. The first row makes sense because the clearance level is higher than sensitivity and their contents are the same.

   The second row does not makes sense because the clearance level is lower than the sensitivity level and it does not contain Nuclear.

   The third row makes sense because secret is higher than unclassified and there is no content in the object.

Lecture 8

1. I am glad that there ware definitions for objects and subjects because I did not know what represents data and what represents human.
2. There are security labels A and B, s.t neither A>=B nor B>= A.
3. There are security labels A and B, s.t neither A>=B nor B>= A.
4. If they have same sensitivity and clearance.
5. The subject can only read up
6. The simple security property gives you a hurdle to get over to gain the access, but does not mean necessarily you can gain access.

Lecture 9

1. Because it only codifies restrictions on read access to documents.
2. Because it prevents the violation of confidentiality property.
3. Programs sometimes could be embedded malicious logic.
4. We can only write up in the levels.

5. Their level of clearance and the contents must be equal.
6. The general could use his unclassified email to send the message.
7. That’s an integrity problem.

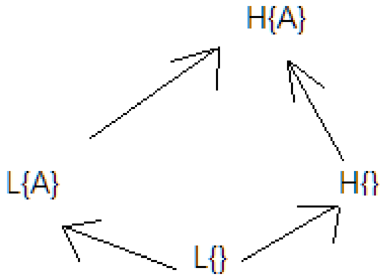
Lecture 10

1. The consequences would mean the subjects might bring information that are not supposed to be read by lower clearance.
2. Because some people might be promoted to higher position and it would not work for strong tranquility property.
3. The subjects that used to have the same level with the objects can now read the objects now because it has been lowered.
4. It must satisfy the weak tranquility property. And if the objects no longer contain important data.

Lecture 11

1. Subjects to high and objects to low.
2. The matrix would be huge for most realistic systems.

Lecture 12



1.
2. A subject at leve L2 can read a level L1, or a subject at level L1 can write a level L2 object
3. Because BLP only wants to read down and write up

Lecture 13

1. Information flow is permitted from L to H, but not vice versa
2. The definitions of read and write are read up and write down
3. Create is also applying the write down policy and destroy options is legal because level object > subject and thus you can write down or destroy here.

4. The high level subject has to create F) first for covert channel to work.
5. So it can start a new loop.
6. No, they are identical.
7. Because it has to create object for covert channel to possibly work. Yes, it must.
8. Because SH can transmit one bit. No, it does not have to be the same.
9. For cover channel to work, SL has to first check if SH has create anything. If SH does create an object, the SL would not be able to sees the value and vice versa.

Lecture 14

1. Because that is not a flow between subjects within the system.
2. No, because both return 0.
3. In the error message
4. In the ordering or duration of events on the system
5. In the events of the system
6. In the control flow of program
7. So there is not much room to work with for the covert channels
8. How much energy is consumed?
9. Low power communication channels

Lecture 15

1. Because information can be represented in just bits.
2. From the previous slides, it is easy to think of a way to attack the system and it’s hard to think of a way to prevent the attacks. It’s hard to come up with a system that can completely check if there exist a potential covert channel or not.
3. Eliminating it, restricting the bandwidth, or monitoring it.
4. When someone with lower level clearance tries to access the higher level object and receive the error messages. And the information can be sent through these error messages.
5. The sender can modify the error message and the receiver can view the message.

Lecture16

1. Because if you are the receiver, you cannot possibly modify to gain any information. The operation should tell you something about the attribute.
2. There is a mechanism that someone can modify it and someone can reference it. It is what potential covert channel can possess.
3. No. Because they would only have either modify or a reference option to even try to spread any information.
4. Because it provides a systematic way to investigate potential covert channels.
5.