Name: Olamide Fayemiwo
EID: oaf226
CS Login: ofaye
Email: olamide.fayemiwo@live.com

Lecture 1

1) Personal security, communications, network and system security
2) The thing that they all have in common is that they are all protecting something against threats.
3) Yes, I had a laptop that had a certain antivirus on it which had a security breach.
4) There is a low possibility that my laptop is infected right now due to new and upcoming ways to implant viruses on laptops. I ran a system scan with my antivirus.
5) I installed an antivirus which I run regularly and I do not go on websites that are not secure, meaning I look for the lock on each of the websites I go to.
6) It is effective for the mean time because I have a tool checking for possible security breaches butthat does not mean a virus cannot duplicate itself as one of the process so I do what I can by not going to suspicious websites.
7) I think it over-states the case because while this may be true;it can be prevented by always finding ways to take out the weakest spot in security so that individuals who want to cause harm will have to think of another way to do so. If the three concepts (Confidentiality, Integrity and Availability) are applied amongst others, then there should be a harder chance of this occurring.
8) Learning about security helps open one’s eyes to see that the problem of security is a huge issue that tends to be underrated. It can help protect one’s own belongings, contribute to the safety of the workplace, improve overall security in cyberspace and enhance the quality and safety of interpersonal and business transactions.

Lecture 2

1) Security is also hard because we cannot control the choices of users. For example password choices, If a website such as yahoo mail states that the password you have chosen is deemed to be weak but the user ignores the warning but sets it as his/her password anyway. If the email account is breached and information is taken out, who is to blame?
2) It is difficult to enumerate the bad things that may occur in a program. This is so because you may have a long list of the possibilities, but there is always something that another person, possibly a hacker will think of that you have not even thought of.
3) The defender tries to come up with possible solutions to the problem before the attacker strikes but the attacker only has to figure out one solution the defender has never thought of.
4) I agree with it because if perfect security is what you aim for, you have to be willing to put in a lot of work to ensure that what you are protecting does not become exposed. This is extremely difficult because perfect security does not exist, it can be close to being perfect by

constantly updating your security measures and thinking inside and outside the box.
5) A tradeoff is typically required because in security, there are certain things that may be good but it is being prevented from entering in due to the measures to keep the system safe from vulnerabilities.

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 believe that software security is about managing risk because in doing so, it helps identify and address such risk in order to be solved. It finds and figures out ways to prevent such things like that from happening again
3) **Risk Acceptance:** Losing sleep is less than turning in an important work project that could determine your promotion.
Risk Avoidance: Not procrastinating on the project.
Risk Mitigation: Asking questions if stuck on a problem and using resources.
Risk Transfer: Hiring a company approved vendor that does not come through with the products you requests on time.
4) Annualized loss expectancy is basically a way to show which risk is more important to focus on and prevent. Showing which one to accept, avoid, mitigate or transfer.
5) Technical, economic, psychological.

Lecture 4

1) The list on slide 2 focuses on the major characteristics needed to solve the security problem while the list on slide 3 focuses on the specific solutions (mechanisms) to prevent bad things from happening. There is a possibility of something such as a confidentiality issue when it comes to cryptography and the rest. So slide 2 is about the things that happen while slide 3 is the mechanisms to it.
2) I think everything is important to me, Confidentiality is important because I want my information to be private at all times when I log onto my online bank account. Integrity is important to me because I do not want my account to be hacked into and there is a transfer of money to another person’s account. And availability is important because I always want to be able to log into my onlinebank account without a hassle.
3) It means to have them in sections and break it down to specific subsections. For example having top secret, secure, confidential information and inside those groups having subsections such as who can see it.
4) Authorizations may change over time due to users allowing certain things/people to have access.
5) Availability relates to reliability because we as users will always want accessed to certain information and if we are unable to access it multiple times,we view it as being unreliable. It also relates to security because we do not want to be denied of service when we need it, if the system does not recognize us but recognizes another person,

orallows another person in it will not be available to us. These are ways that viruses can enter a computer.
6) Authentication is important when we are trying to access information and we need it to know if it truly is the authorized person while Non-repudiation is important as a way to prevent denial of actions by an individual. Example: Authentication -- logging into an online bank account. Non-repudiation -- buying something online and then denying ever purchasing it.

Lecture 5

1) A metapolicy for a cell phone network will be securing customers information and transactions. A metapolicy for a military database will be securing pertinent information that could potentially cause harm to unauthorized individuals who can see it.
2) A policy is needed because it is a system specific refinement of the metapolicy itself. The metapolicy is an overall goal while a policy is specific to the section that you want to be secured.
3) Unauthorized persons cannot see the student's academic records; the academic records cannot be changed by said persons or the student itself and the academic record cannot be leaked under any circumstances.
4) It could be possible that stakeholders' interest conflict in a policy by someone deeming an issue important than the rest. For instance, a person could think that privacy of information is important while someone else could deem authentication as being important.
5) The metapolicy is to make sure the students SSN is secure at all times.
6) This just simply means that if we do not understand the goal of it, then we cannot break it down and find different sections to solve the problem. For the previous example, if we do not know that the goalis to secure every student SSN, then we would find all the actions such as destroying documents containing SSNs as being tedious and unnecessary.

Lecture 6

1) Military security is mainly about confidentiality because their main goal is to keep information they have private. They do not want unauthorized users accessing information that is not for them; it causes security problems. There are aspects of integrity and availability but it is not as important as confidentiality.
2) The major threat was someone not authorized to view certain information getting access to it and reading it.
3) The proviso is there to make sure that the goal is being reached, integrity and availability is not to be thought of in this case.
4) We are using labels from a linearly ordered set which shows the level of importance from unclassified to top secret.
5) We are not concerned because we are only worried about confidentiality, making sure that privacy is not breached.
6) 2, 6, 4, 5, 1, 3
7) Top Secret: 2, 6 Secret: 4, 5 Unclassified: 1, 3
8) The rules for "mixed" documents make sense because a document that contains both sensitive and non-sensitive information should be handled with the highest appropriate level because the problem is a

confidentiality problem. No one under that level should be able to access such information because it does not involve them. And using both categories when it involves information relating to two sections is justifiable because we cannot limit one person from accessing the information even if they have the authorization for it.

Lecture 7

1) They are stamped on the inside, part of a set which are the need-to-know categories.
2) The labels for documents are linearly ordered sets showing the degree level of trustworthiness while humans are in a set that group together with other people that are given authority to access the document (classes of information).
3) **Documents**: Word Processor **Humans**: Users
4) Principle of Least Privilege makes sense because just because Crypto and Nuclear are in the same class does not mean that they can see each other's information. Although they might be on the same level, they should only be allowed to see information that pertains to them alone.
5) The answers on the third column do make sense because for the first instance, the sensitivity level is not high enough for it to see documents with a secret clearance but with the mixed document. The second instance makes sense because the top secret only has crypto in its class of information so therefore it cannot view the other one. The last instance makes sense because secret can view unclassified [no set].

Lecture 8

1) These terms are being introduced to classify what we have been learning in its proper term and also categorize objects as being the document we look at in MLS, the subjects as being humans and the action as the operation the subjects can perform.
2) The 'dominates' relation is a partial order because (L1, S1) dominates (L2, S2) iff L1 >= L2 and S2 is a subset of S1.

Let Z be the set of ordered pairs, let D be a 'dominates' relation, meaning that D is a subset of Z.

We say that D is reflexive because L1 can be equal to L2 [Security labels A and B, A = A and B = B]

We say that D is transitive if the level of the subject is the same for both but they have different objects, the higher level is clearly going to dominate.

We say D is antisymmetric because looking at two labels with security labels A and B in which (A, B) can be in D and (B, A) can also be in D.

3) The dominates relation would not be a total order because it does not have the qualities of totality, meaning that with two security labels A and B, A <= B nor B <= A
4) Two labels would have to dominate each other if they have the same subject and object.
5) The Simple Security Property simply states that you can read from top down (no read up)
6) It is only if because there are multiple instances that this can be true, it is not uniform to one way only.

Lecture 9

1) Simple Security is not enough to ensure confidentiality because it only pertains to reading/accessing information.
2) We need constraints on the write access because we do not want important information being passed down
3) This is particularly important because there are malicious attacks (viruses) on computers that can pass down information that is not supposed to be seen by other subjects.
4) *-Property simply states that you can write up at your level and upwards. (no write down)
5) They must be at the same level for a subject to have both read and write access to an object.
6) We can deal with the problem by invoking a clause or a property that prevents information leaks from the top to the bottom.
7) That would have to be an integrity problem, in which there should be a clause that states that nothing important can be changed by writing up.

Lecture 10

1) Information cannot be changed from a Secret: {Crypto, Nuclear} to a Confidential: {Crypto} because it is changing the policy.
2) Using strong tranquility all the time does not allow authorized information to flow flexibly.
3) Lowering the level of an object may be dangerous because what happens to the information in the object that is not supposed to be seen by a lower object status.
4) A downgrade occurs when there are two different objects, one high and one low with the same subjects or a low object with an empty set and either a low level or high level with multiple objects.

Lecture 11

1) I would give the subjects a discretionary access control while the objects will have a mandatory access control.
2) Building an access control matrix for a BLP system requires having a large matrix for the system

Lecture 12

1)

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

2) Begin at the bottom of the level to find the LUB, work your way to the top, halt when you detect a high level. You compute vice versa for finding the GLB.

3) The upward flow in the lattice is the metapolicy for BLP because is goal is to prevent information flow from a higher level to a lower level.

Lecture 13

1) The BLP rules enforce the metapolicy by making sure the information flows from the lower level to the higher level only.
2) The Read and Write operations satisfies the BLP system because the read checks to see if the subject level is greater than the object level meaning that you can only read down while the write operation checks to see if the subject level is less than the object level meaning that you can only write upward.
3) The ‘create’ and ‘destroy’ operations satisfies the BLP system because the create operation creates an object at the exact same level which the BLP system accepts and the destroy operation only destroys things that can be edited (destroy objects at its level and above).
4) There has to be an object already created so that it does not misread the value.
5) The destroy statement is there in order to prevent the exact object being accessed twice.
6) The contents of the files are different in both paths because in the first one, when it creates the object at the high level, it does not exist then it creates it again at the low level so when it wants to eventually read it, it does not see the value of 1 but of 0 while the other path sees the value of 1 because it did not create the object at the high level.
7) It must do the same thing because it has to be consistent on both ends. The other path doing something different shows error because how is it supposed to know what to do differently
8) SH has to do different things in order to show the difference in the path.
9) It is basically stating that if the lower leveled subject has different results from both paths doing different actions with the higher leveled subjects which in turn sends information from high to low, it basically means that there is a violation of the metapolicy which states that information should only flow upwards not from high to low.

Lecture 14

1) It is the flow of information between two subjects in a system that shows an illegal flow of information. Nothing prevents two human users from performing that action.
2) It is a covert channel because the flow of information is different in both instances
3) It resides in the higher level subject (SH)
4) It depends on the timing but it resides in both
5) It depends on the timing but it resides in both
6) It resides in the higher level subject
7) A termination channel may have low bandwidth due to the high rate of channel attack. A low bandwidth shows the less number of bits transmitted over the channel in one second. An attacker can easily analyze the covert

channel and guess the sender information because of the less number of bits.
8) The amount of energy being consumed is high and clearly consuming above average.
9) CPUs

Lecture 15

1) Covert channels can potentially be very serious threat due to low bandwidth because a low bandwidth shows the less number of bits transmitted over the channel in one second. An attacker can watch the traffic of a covert channel and easily guess the sender information.
2) It will be infeasible to eliminate every potential covert channel because there is a high responsibility infiguring out how to fix it and there are a lot of covert channels that users will ignore.
3) Eliminating it by modifying the system implementation, reducing the bandwidth by introducing noise into the channel and monitoring the patterns of usage that indicates that someone is trying to exploit it.
4) When a user uses a file that is meant for holding certain types of information to convey passwords that can be read by all users to signal the contents of the file.
5) The sender and the receiver have access to the file that has the passwords because the receiver (other users) can read it while the sender can modify it.

Lecture 16

1) The ‘create’ will not have an R for the file existence attribute because we do not have information about the existence of the file due to us actually creating it.
2) This indicates a potential channel because for a covert channel to exist, the sender and receiver have to have some attribute of a shared object. The sender has to be able to modify it while the receiver has to be able to reference it.
3) This does not indicate a potential covert channel because there are different objects and shared attributes
4) An SRMM table shows us ways in which we can see potential effects on certain objects. (Storage channels only)