Lena Ko
CS361
LK5399
ko.lena92@gmail.com

Lecture 1

1. Personal and institutional security are most relevant to my everyday life. Because most activities are done online, my main concern involves protecting my private information such as credit card numbers and addresses.

2. Both involve protecting assets from different threats.

3. Yes. My laptop has been infected before.

4. The likelihood that my laptop is infected is probably high. I decided on this because it is difficult to fully protect. You can only take measures to try and prevent it from happening.

5. I have a firewall installed, and I download the latest security updates.

6. I believe they are somewhat effective, but you can never be fully protected.

7. If the FBI official had used a stronger word such as “end” instead of “challenge”, I would probably think that he is overstating the case. I do believe that the ability to access computer systems can impose great harm on our country, but I'm not fully convinced it would end its existence.

8.It is important to learn about computer security because it allows you to enhance your own protection, contribute to security in the workplace, enhance the quality and safety of interpersonal and business transactions, and imporve overall security in the cyberspace.

Lecture 2

1. There will always be individuals who think of different ways to attack, and different ways to beat security systems.

2. No, it is difficult to think of all possible ways of attack.

3. The defender needs to find all possible exploitable vulnerabilities while the attacker only needs to find one.

4. Yes, I do agree with Morris and Chang. There is no way to fully protect your computer when it is turned on, so the only real way to completely protect it is to have it off. Keeping it on opens it up to vulnerabilities.

5. Too much security can effect other goals in negative ways by inhibiting them from being established. Sometimes you have to find the right balance in order to accomplish enough of both.

Lecture 3

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

2. Yes. Risk management is the process of an organization to identify and address the risk in their environment which involves assessing assets, threats, vulnerabilities, risks, etc. These all aid in software security.

3. A risk you accept is called risk acceptance. The cost of insurance could cost more than the potential loss such as the risk of purchasing defective off-the-shelf software. A risk you avoid is one that you do not allow such as remote login. A risk you mitigate is taking actions to reduce potential losses such as buying life insurance. A risk you transfer is one that you shift to someone else such as home insurance.

4. Annualized loss expectancy helps to show which risks should be accepted in comparison to those that should be avoided. The larger the expected annual loss and incidence, the more that risk should be avoided. The less annual loss of a risk tells us that it should be accepted over more threatening risks.

5. Factors relevant to risk assessment are the severity of loss from that risk, the possibility of it occurring, and the cost of avoiding the risk.

Lecture 4

1. Slide 2 is a list of the goals of security while slide 3 is a list of techniques in order to achieve those goals.

2. I believe confidentiality is the most important in my personal life. I do not want people getting into my accounts and having access to other information such as credit card numbers.

3. Grouping and categorizing data is important to protect information from unauthorized disclosure. Since not all data is equally sensitive, you should group them according to sensitivity and set permissions to those groups.

4. Authorizations could change over time depending on the sensitivity of the information as well as the change in status of an individual such as promotions and demotions.

5. High available systems are available at all times meaning computing systems, security controls, and communication channels are functioning properly. Systems should function properly in order to keep a system secure.

6. Sites that use passwords are often protecting sensitive information. These contexts require authentication. Highly confidential information, such as military and government plans, would require both authentication and non-repudiation. The receivers and senders must be who they say they are by authenticating their identities.

Lecture 5

1. A possible metapolicy for a cell phone network could be availability because the network has to be

available at all times. A possible metapolicy for a military database could be confidentiality because it would involve highly sensitive information.

2. Metapolicy is too general to adequately guide and accomplish itself. You need policy in order to specify and add guidelines to how to achieve the metapolicy.

3.

1.Only allow people with a specific level to access them.
2.Create a super password to login to see the files
3. Encryption

4. Yes. A stakeholder may think that integrity is more important than the policy of confidentiality. A student may have good grades, but many enemies. Therefore this would lead them to believe that integrity is more important than keeping their grades confidential.

5. Confidentiality would most likely be the metapolicy for SSNs.

6. Without the metapolicy, the goal is unclear. Without a clear metapolicy, it is difficult to come up with mechanisms in order to achieve that metapolicy. You need a metapolicy to create a policy.

Lecture 6

1. In military security, there are many different sensitivity levels. Some are authorized to access while others aren't which is why confidentiality plays a large roll in military. Integrity and availability also play roles in security. People don't want anyone to be able to change information/release higher levels of information and the data should be available at all times so that people are able to access the data when necessary.

2. The major threat is that someone without authorization to view a piece of information may have access to view it.

3. Without the proviso, we would be concerned with integrity and availability as well. These are aspects that are not addressed in our MLS experiment so are unable to be achieved. If we had to take integrity and availability into account, we would have to create a new solution.

4. Unclassified, Confidential, Secret, Top Secret are linearly ordered ranking from least sensitive to most sensitive. In addition to these labels, we have need-to-know categories that are unordered which include Crypto, Nuclear, Janitorial, and Personnel.

5.We are only concerned with the authorization part of the process. The retrieval of the labels are based on the context of the stituation.

6. 3,1,5,4,6,2

7.
3) (Unclassified:{janitorial})
1)(Unclassified:{personnel})
5)(Confidential: {personnel})
4)(Confidential :{personnel})

6)(Secret:{crypto})
2)(Top Secret:{nuclear})

8. Some documents are related to more than one category, therefore it must be mixed.

Lecture 7

1. Labels on humans indicate classes of information that person is authorized to see.

2. Labels on documents indicate the sensitivity of the information, and for individuals they indicate the clearances to view certain classes.

3. Computers sometimes require users to login. The different types of users (restricted, guest, and authorized) are able to see different information/ programs. These programs would be the documents and the users the humans.

4. The less that people know about something, the more secure it is. The principle of least privilege says that people have access to the minimum requirement to do their job.

5. Secret is higher clearance than confidential and crypto is a subset of crypto therefore the first pair makes sense. Secret is lower clearance than Top Secret, therefore that individual should not have access. Secret is higher clearance than unclassified and empty set is a subset of nuclear so this individual should have access.

Lecture 8

1. Using these vocabulary terms creates a broader context than using humans and documents and clarify possible relations.

2. Dominates is a partial order because some labels may not be a dominant relation. A may not be less or equal to B while B is also not less than or equal to A.

3. Dominates is not a total order because the categories also play a role in determining clearance. The category of the user must be a subset of the document's categories.

4. The label must be of higher clearance and the category must be a subset.

5. A subject must be of a clearance level that dominates the sensitivity level of the document in order to access it.

6. If and only if means that the condition is both necessary and sufficient. Only if means there may be other constraints in the system from letting it read it.

Lecture 9

1. Simple Security doesn't ensure confidentiality because it doesn't address write access. An individual could write information from a top secret to a unclassified document without challenging Simple Security.

2. Write access constraints must be put in place so that higher level information does not leak down to lower level subjects.

3. The accessing subject may be a program executing on behalf of a user. The user may have been cleared but the program may have not.

4. A user can only have write access to a document if their security clearance is lower than the document's security level.

5. A subject must dominate the object and the object must dominate the subject which means that they are equal.

6. You could distinguish a current level and max level, allowing you to communicate down. He can login to a lower account.

7. We are dealing with confidentiality, not integrity. We need to put other rules in place to deal with this integrity issue.

Lecture 10

1. Weak tranquility allows subject's levels to change if it does not violate the spirit of security. Raising the level would not be good, but it gets fuzzier with lowering the level. As long as it is a stateless subject, it should be okay.

2. A user may need to work at different levels throughout the day. Strong tranquility does not allow this.

3. If you lower the level of an object, subjects with lower clearance are able to read them.

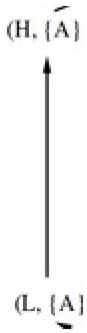
4. The object must be reviewed and determined to be viewable by lower clearance level subjects.

Lecture 11

1. In order to give all subjects read access, but write access to none of them, you would need to give your subjects higher levels than the objects. This will disallow them from writing to them, but allow them to read them.

2. You may have thousands of subjects and objects and many of the intersections could be empty. It is more efficient to determine them individually.

Lecture 12



2. Through the lattice you discover the least upper bound and the greatest upper bound.

3. The metapolicy of BLP is to constrain information flow of information among security levels. When information flows upward from x to y that means x is less than y.

Lecture 13

1. Information should be allowed to flow from low to high not from high to low, which is shown in the first example by a lattice that flows from low to high.

2. Subjects can only read if they have a greater security level and can only write up.

3. They don't violate BLP metapolicy because creates and destroys do not override any procedures.

4. The lower level subject has to see varying results depending on what the higher level subject decides to do. The higher level subject cannot create before the lower subject gets to read.

5. The destroy allows them to go back and do the same process again handing down information.

6. The contents are not different because the Lower level writes the same information on both sides.

7. SL needs to coordinate its actions depending on the SH.

8. SH does different things to allow information to flow down. It must not create in the beginning in order for this to happen.

9. If SH creates an object, it is at a level too high for the SL. Without this create, the SL is able to create and read the information. Therefore, the varying results could be used to send information.

Lecture 14

1. Covert channels involve flow of information of subjects within a system. We care about using the mechanism of the system, not human to human interaction.

2. If SH sends a bit of information on every access attempt, yes.

3. In the returned message.

4. In the ordering or duration of events on the system.

5. From the order of returned messages

6. In the control flow of a program.

7. Because a computation terminates, it may be limited to the bandwidth or capacity that it can transmit.

8. It must use some type of power and both sender and receiver must have some access to a shared space.

9. Smartcard

Lecture 15

1. Covert channels can be used to send thousands of bits of information over a greater amount of time even with low bandwidth.

2.It is difficult to identify every covert channel as well as eliminate them, although mitigating them is more feasible.

3. One could respond by eliminating it by modifying the system, reduce the bandwidth by adding noise, and monitor it.

4. Attempted access by SL to a high level resource returns one of two error messages:
Resource not found or Access denied.

5. By modulating the status of the resource, SH can send a bit of information on each access attempt by SL. SH is able to utilize by sending bits while storing information and SL is able to receive these bits by sending access requests.

Lecture 16

1. The create option wouldn't have an R because when you create it you know that the file is existent.

2. For that attribute, someone can modify it, and someone can reference it: two qualities needed for a covert channel.

3.No. It does not imply that one is able to read while one is able to write. These features are needed for a covert channel to exist.

4. By creating the SRMM table, you are able to locate where a covert channel may exist. Only after this detection, you are able to mitigate it or eliminate it. The SRMM table gives you a places to search for the covert channels.