Colt Whaley

cww688

Module 1 Questions

Lecture 1:

1. I want my information to be secure and uncompromised online. I want to feel safe when walking around in public.
2. They all deal with making sure some asset is uncompromised.
3. Yes, I leave my phone unlocked. I often leave my door unlocked and I only run virus scans monthly usually.
4. Probably very likely. However, infected with a major virus/bug that could cause serious damage is rather unlikely. I run virus scans with AVG and Microsoft Security Essentials.
5. I back up my data online and on an external hard drive. I have a password on my laptop and I have anti-virus programs.
6. Mostly, I haven't experienced much loss of data or productivity over the life of this laptop.
7. I believe it to be true; however, I also believe he is exaggerating to prove a point. They already know this to be true seeing as the NSA spies on half the world on a daily basis.
8. As the world becomes increasingly more digital, more and more information is being stores electronically. Just as you hope that your money is protected when you take it to a bank, one hopes to have assurances when they store information electronically.

Lecture 2:

1. There are so many multiple platforms and operating systems now that it is practically impossible to make sure that your program works perfectly and is completely secure.
2. No, there is no possible way to think of every bad thing that could go wrong. You would spend all of your development time debating what could go wrong instead of actually completing your project.
3. The defender must think of every way you could maliciously access information while an attacker only has to find one.
4. Yes, I agree. There is no possible way to completely secure a system; you can only limit the damages and risks.
5. Like I said in question 2, you would have to spend far too much development time dedicated to completely securing your project that would take away from the actual functionality of the project.

Lecture 3:

1. The possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
2. Yes, it is the most efficient use of development time.

3. Acceptance, driving knowing that there is a chance of an accident. Avoidance, not driving in the night because you do not trust your eyesight. Mitigation, driving a cheaper car so that when you get in an accident it will cost less to replace it. Transfer, buying car insurance so that when you get in an accident you do not have to pay for it, the insurance company does.
4. Annualized loss expectancy shows you where you should spend the most of your time protecting. Although just because one threat has lower ALE, its threat amount may be so large in comparison to other threats that you should spend more resources protecting it.
5. Threat potential loss, ALE, which method of risk management should you use, resources available to develop mitigation.

Lecture 4

1. Slide 3 is a list of mechanisms by which you ensure the aspects on slide 2.
2. It depends on the context. If I am buying something online using a credit card, I want my information to be confidential. If I am backing up data online, I want integrity so that my data is the same when I access it next. If I am trying to play a game, I want the game servers to be available.
3. You don't want all of the information to be secured the same way, and then if one piece is compromised the entire collection is.
4. You may work for the government and get a promotion that requires you to get a higher security clearance.
5. Companies want their servers to be up as much as possible so that they can make money. By denying the availability to the consumer, they will lose money so they need protection against denial of service attacks.
6. Buying goods online.

Lecture 5

1. Secure connections across the network. Ensure the integrity and confidentiality of the military secrets.
2. The metapolicy is broad, general requirements of the project. The policies are how the metapolicy is satisfied.
3. Professor's laptops must be encrypted if they contain student information. Faculty cannot release information without the student's knowledge. Students and unrelated faculty cannot tamper with grades.
4. Students wanting their grade information to be secure.
5. Protecting the confidentiality of students SSNs to prevent identity theft
6. If you can't understand what the system is trying to protect, it would be very hard to understand why you are doing/not doing the things you are doing.

Lecture 6

1. They want to ensure that the enemy does not know their plans before they execute them. Yes, the need the plans to be available when they need them and make sure that no one have tampered with them.
2. Information being leaked to the enemy

3. The best method of protecting confidentiality may severely limit availability and integrity and any other combination thereof.
4. The hierarchal part and the need-to-know category part.
5. Outside the scope of concern
6. Softball game at 3 (Unclassified: {personnel})
   Cafeteria serving beef (Unclassified: {personnel})
   Jones got a raise (Confidential: {personnel})
   Smith didn't a raise (Confidential: {personnel})
   Normandy on June 6(Top Secret: {Strategy})
   British broken the Enigma code (Top Secret: {Crypto})
7. Added in on 6
8. It is categorized based on the highest classified information

Lecture 7

1. They are assigned authorizations/clearance level.
2. Labels for humans indicate the trust in that person whereas labels for documents indicate the sensitivity of the information
3. Documents = data ; Humans = users
4. If you deny access to information, it can't be leaked
5. They all are true. The clearance is sufficient for the first and last and insufficient on the second.

Lecture 8

1. It is relating the thought experiment to information security
2. There are labels that neither dominates each other. Like secret, crypto and secret, nuclear.
3. There is no order to sets that dominate each other based on the need-to-know categories, only by the hierarchal clearance.
4. There would have to be a hierarchal ranking of need-to-know categories
5. A subject can read an object only if their clearance is above or equal to that of the object and the subject is cleared for that category.
6. There may be other security measures in place that would prevent the subject from reading the object.

Lecture 9

1. It doesn't secure write access.
2. It prevents unwanted leaking of information. Someone with high level clearance writing to a low level file.
3. Computers run hundreds of programs using the user's clearance which opens up much more opportunity for malicious information leaks.
4. Subjects can only write to an object of equal or higher clearance.
5. It must be on the same level.
6. Having a second account with clearance necessary to write at that level that would not have access to the top secret information
7. Having a sysadmin at the top-secret level verify the edit before it is completed.

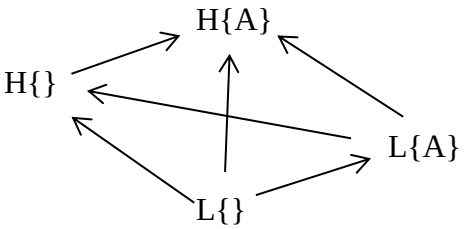
Lecture 10

1. It is all up to the interpretation of the security policies as to whether subject may be up/downgraded. So long as it doesn't hurt the confidentiality of the system then the change is okay.
2. It is necessary in certain situations for security levels to be changed. Like a document being declassified as the information is no longer sensitive.
3. The information could be too sensitive for the level it is being lowered to.
4. The information must no longer be considered too sensitive for that level and would not cause a compromise in confidentiality.

Lecture 11

1. The objects would all be L and the subjects all H
2. They would be massive and the access rights can be computed on the fly using the *-property and simple security property

Lecture 12

1. 

2.
3. The goal of BLP is to control the flow of information, which must flow along the lines of the lattice, which is up.

Lecture 13

1. It prevents H from sending information to L
2. You can only write up and you can only read down. Makes sure that information only flows up.
3. Create does not give the subject any information as to whether the creation worked or did not so it cannot be manipulated and is only writing to its level. Destroy is basically writing up which is allowed by BLP.
4. L must do the same thing each time so that the only thing that changes is what H is doing to manipulate.
5. So that when you retry the message the object is reset for manipulation by H
6. No, only whether or not the object can be read by L.
7. It is the control to ensure that other extraneous variables cause static on the channel that would disrupt the follow of information
8. H is what is manipulating the variable and sending information to L.
9. If a bit can be sent from H to L, then over time entire documents of information could be sent from H to L which violates the metapolicy.

Lecture 14

1. It is outside the system.
2. No, because L will read 0 regardless because it doesn't have access to F0.
3. The error message
4. The time clock of the two processors
5. Whichever cylinder p leaves the head closest to.
6. Whether or not h is an odd number.
7. Because the trigger is whether or not a process has terminated which takes a decent amount of time to compute.
8. A way to monitor power consumption in the system
9. Electronic keys to read the binary code associated with each key

Lecture 15

1. If not recognized and dealt with can leak large amounts of information over time.
2. Many systems are so complex that it would take too much time to redevelop each time a new one is found.
3. One could create noise on the channel that makes it difficult to interpret a message being sent via the channel
4. Anytime there is a system attribute that can be modified by the sender and referenced by the receiver.
5. The sender can modify the attribute to one of two states representing a 0 or 1. The receiver can then reference the attribute and note which state it is in and record it.

Lecture 16

1. Because create does not tell the subject whether or not it was successful or failed.
2. Anytime that a something can be used to reference and modify allows for a flow of information.
3. No, just because an operation can be referenced and modified by subjects does not mean that information can flow because of it. There may be no way for the subjects to effectively interact.
4. It shows all of the potential threats for covert channels in a system.