Haoshu Yuwen
Hy2892

Assignment 1

Lecture 1:

1. Personal, Corporate, Homeland, Communications, and Network are the big ones.

2. They all protect information nowadays.

3. Yes. A couple of years back somebody got a hold of my email password and sent out spam to all my contacts. Fortunately, I don't keep many email contacts on record so it wasn't too bad.

4. I don't think it's very likely that my laptop is infected with anything significant. I use a MacBook pro with virus scanner, which in theory should make it rather difficult to get infected with major malware, thanks to OSX's handy feature requiring a password to install.

5. I use a password to protect against physical intrusions and a virus scanner to hopefully prevent digital intrusions.

6. I believe my precautions are capable for most threats.

7. I honestly believe that this statement is a little bit overly paranoid. If our adversaries had that much access to our resources, I firmly believe we wouldn't be here anymore. For example, suppose terrorists had access to the system responsible for our nuclear arsenal, I highly doubt they wouldn't use it.

8. As the world becomes more and more interconnected, security breaches become more and more costly. Therefore, learning about security is becoming more and more important, especially since more and more of our personal information and resources are stored digitally.

Lecture 2

1. One reason I think security is extremely difficult is the whole "it won't happen to me" mentality. Considering the number of systems out there, the common user probably doesn't think they will be specifically targeted, similar to the bystander effect.

2. No. If we COULD do this, then security breaches would be a thing of the past. Considering how complicated modern software is, there is no way every threat will be predicted.

3. Unlike the offender, defenders have to defend against all possible avenues of intrusions. The offender has the luxury of only having to find one exploit to do his or her damage.

4. Basically what Morris and Chang are saying is that it is now impossible to prevent security breaches. I don't agree with this sentiment. I believe that if you are careful, you can prevent security breaches. However, I agree that the Internet must be disconnected.

5. The best way to explain this statement is to give an example. DRM is used in security to prevent software theft. However, DRM often causes software to BLOODY NOT WORK or puts up significant barriers to entry. Hence, ease of use and functionality are traded away for increased theft protection.

Lecture 3

1. Risk is the potential for something bad to happen.

2. Yes. Considering that it is generally agreed that perfect security is impossible, computer security is about minimizing the risk to appropriate levels.

3. If I'm not limited to the digital realm:

Accepted: The risk of a plane crashing when I need to travel internationally.
Avoided: The risk of going to jail from running someone over while drunk, hence I don't drink and drive.
Mitigated: I wear a helmet while biking.
Transferred: I'm covered under my parents' health insurance.

4. Annualized loss expectancy is a great way to determine where most of your resources should go since not all security threats are created equal. Some cause far more damage than others, for example: credit card number theft vs. video game password theft.

5. Economic loss and personal injury consideration are the two major ones.

Lecture 4

1. Slide two lists a few goals while slide three list ways to achieve aforementioned goals.

2. For me personally, integrity is the most important. I don't have many "secrets" on my system so confidentiality isn't as big of a deal. I'm pretty computer dependent but I have other avenues of entertainment so availability, while important, isn't as essential. However, if other people were able to change my files, it would be an absolute deal breaker.

3. Grouping and categorizing data is the segmenting of data into convenient blocks so certain blocks may be more visible than others.

4. As a person's status changes, his authorizations may as well. For example, a concrete example would be the purchase of alcohol. As soon as someone turns 21, authorization is given to purchase and consume alcohol.

5. Availability means you can use a resource when you need it. Reliability means the resource won't break spontaneously. If you happen to need a resource but it's broken, you're in for a bad time.

6. Authentication and non-repudiation are important if I'm trying to buy something.

Lecture 5

1. For a cellphone network, a good policy would be having all conversations be private but to the participants of the conversation. For the military, have all information be visible to only the necessary individuals. They're quite similar really.

2. Policies are needed to achieve the metapolicy.

3. A student may only see his own record. Parents may not access their children's records. A record may only be altered by the registrar or by a student's professor or teacher.

4. Yes. The above example may be used. A student wants his or her record to be confidential to everyone. A parent wants his or her child's record to confidential to everyone but themselves and the child, hence conflict.

5. Students' SSNs must be kept confidential.

6. If you don't understand the overall goal, you can't understand the steps to reach that goal. For example, if you don't understand the overall goal of a sporting event is to win, you won't understand why you're trying to shoot the ball into the hoop.

Lecture 6

1. Military data is a matter of life and death hence keeping battle plans out of enemy hands is critical. Of course, integrity and availability are also important because if someone were to change the plans, it would result in confusion and chaos (and perhaps friendly fire). Additionally, the best-laid plans are useless if the information can't be conveyed to the actors.

2. Since some resources contain both sensitive and non-sensitive data, care must be taken that only those cleared for sensitive data can see documents containing both.

3. Availability is another matter entirely since if your system doesn't actually function, nobody is going to be able to see it anyways. As for integrity, that can be solved the same way as confidentiality.

4. These labels are basically levels where a lower leveled entity cannot access data classified at a higher level in a linear relationship.

5. Think of it as a layer of abstraction.

6. From low sensitivity to high: softball team, cafeteria schedule, personnel information, code broken and invasion plans.

7. Unclassified{Schedules}, Secret{Personnel Files}, Top Secret{War Materials}

8. For mixed documents, the higher level of security overrules the lower since leaking sensitive information is more dangerous than letting slip casual data.

Lecture 7

1. Each individual is given clearances, which must be shown before viewing any labeled document.

2. Labels on documents indicate level of information contained while labels on individuals indicate maximum level of information receivable.

3. The documents are the password-protected files and clearances are the passwords known by people at a certain level. For unclassified documents there's no password at all!

4. The ability to access more information than necessary is risky since that increases the change the seeker sees sensitive information. This assumes that no system is perfect and there is the possibility of sensitive information being where it shouldn't be.

5. All three make sense. Each case has a person of high clearance accessing something of lower or equal clearance relating at least partially to his or her field, assuming the access is for doing his or her job.

Lecture 8

1. These terms form the basis of a generic request for information. A subject (user) acts (action) on a database (object).

2. Reflexivity: by definition, L dominates L if they are the same.
Antisymmetry: If A <= B AND B <= A, this implies that A <= A which is true.
Transitive: See antisymmetry.

3. To be a total order, totality must hold. Therefore if there is an L and M, either L must be less than or equal to M or vice versa. However, this is not the case since L and M may not be related whatsoever.

4. They must be equal.

5. Read access may only be granted if the user has a higher clearance and the database contains data that is relevant to the user's field.

6. Just because a person is has the clearance to view certain data doesn't mean he HAS to be given access.

Lecture 9

1. It's not enough because we have to deal with write as well as read.

2. We don't want anyone to be able to modify data.

3. Software often contain embedded code that is far harder to track.

4. The *- property basically says that it is okay to write upwards.

5. For both read and write, (L1, C1) == (L2, C2).

6. Label orders with a level both parties have access to.

7. Uhh…

Lecture 10

1. Changing a subject's level will violate weak tranquility since the subject has the potential of upping its own level up to the point of being able to access everything.

2. Not being able to change is a problem because it removes flexibility. For example, in the military case, not being able to change levels means that if you start as a private but are promoted all the way to a general, you'd still have the same clearance as a private.

3. Lowering an object is dangerous since it may grant unintended access to a subject with a level too low.

4. If an object is lowered, no new subjects must gain access.

Lecture 11

1. All subjects would be high clearance with access to every topic. All objects would be low clearance.

2. The matrix may become too big therefore it is easier to just calculate permissions on the fly.

Lecture 12

1.

```
H{} -> H{A}
 ^     ^     ^
L{}  -> L{A}
```

2.

Lecture 13

1. Based on BLP, H can read but not write to L. Therefore, information is flowing upwards from L to H. L cannot read H but can write to H, therefore information is again flowing upwards from L to H.

2. Read satisfies because information is flowing from a lower or equal level to the higher reader.
Write satisfies because write only works if the target dominates the source, hence you are writing up.

3. Create satisfies because you are basically writing to the same level, which satisfies BLP's requirement of writing "up."
Destroy works for the same reason as write in number 2.

4. For this to work, the create action must fail on the left hand case.

5. It destroys the object F in both cases so the SL can function again over and over.

6. No.

7. SL does the same thing in both cases because the change in result is dependent on the action of SH under the same conditions. For example, if on the right side the write wrote a 0 instead of 1, then the covert channel will fail since the result will be identical regardless of the actions of SH. Generally, the lower level subject should do the same thing.

8. SH does different things because it must signal the SL by causing a different outcome. If SH does the same thing, then no variation is seen by SL. Therefore, information cannot flow downwards and any variations would be caused by SL itself.

9. This is true by definition of what covert channels are.

Lecture 14

1. Two people talking over coffee is most likely intentional and therefore not a covert channel. This case is more like an open channel.

2. No. SL cannot see any changes based on what SH does.

3. The status of the resource.

4. The system clock.

5. Disk head location.

6. Program control flow.

7. If a process takes a very long time, it would take a very long time to transmit the information dependent on the process terminating.

8. A power channel is only possible if different operations use different amounts of power.

9. According to the in class example, mobile devices commonly have power channels.

Lecture 15

1. On modern processors, covert channels actually can operate at thousands of bits per second. This adds up quick to provide lots of information.

2. Just like predicting vulnerabilities in general, the complexity of modern software makes it impossible to anticipate every single covert channel without actually having someone exploit the covert channels.

3. We can re-implement the system to try to eliminate it or we can try adding noise to slow down the data flow.

4. IP Packet Headers

5. …

Lecture 16

1. Because the create operation doesn’t return any data to the user. It simply writes.

2. It’s a potential channel because modification means changes can be made to the attribute. Therefore a reader could potentially see the changes to that attribute. If there are only modifications in a row, then there should be no channel cause those changes never reach the eyes of a seeker.

3. No because the attributes are independent. If one operation can only modify attribute B and can only read attribute A, then regardless of the modification on B, A will remain the same.

4. To locate potential locations of information leakage.