CS361 Intro to Computer Security Daniel Rosenwald
Young, Bill June 12, 2014

Week 1

Lecture 1

1. There are many uses of the term security relevant in my everyday life. First and foremost, my own basic and personal security - trusting my door lock to hold at night while I sleep. Depending on our nation's military to protect our borders. And trusting the protocols of the Internet and services that use the Internet to protect my personal information.
2. All these things have in common the same purpose: that is to protect something.
3. I was once allowed to go through TSA pre-check at the airport. I didn't even have to take my shoes off.
4. Quite unlikely – I have a MacBook, and although people are starting to develop more spyware and malware that runs on OSX, I've had this thing for 4 years and it still runs just like it did when I bought it.
5. I keep my laptop in my room and a locked front door when I'm gone. Otherwise it's with me. Software-wise, I really don't have much on here except for maybe choosing to use Google Chrome with Ad-Blocker.
6. Yeah, no thefts yet (fingers crossed).
7. I think it puts things in perspective. I'm sure there's a way to hack into the country's nuclear weapons launch control, and if so, yes I believe the quote. It just shows how careful we have to be when we start trusting computers to control everything around us.
8. Computer security is important not only to be poised for a professional position as a security specialist, but because the world actually needs computer security more than ever. With the rapid increase in information being passed through the web every month, attempts to steal that information increase. Security has always been an afterthought in computing, and now it needs to become a beforethought.

Lecture 2

1. Security is hard simply because technology moves at such a great pace. If today, when our new product ships, we have a 99.99% secure product, tomorrow someone could release a tool that easily breaks down our defenses to an almost spoon-feeding of data to whoever wants access. Keeping up is tough.
2. No. Unlike the ways you can error-check for bad instructions in a program, checking for hacks is nearly impossible because there is no one way to hack.
3. The defender has to eliminate all exploitable vulnerabilities. The attacker only needs to find one!
4. I do agree – the Internet allows the inevitable hacking of any given machine. However, I believe we should take the risk in order to reap the enormous benefits that computers afford us.

5. The tradeoff statement refers to the manpower involved in developing software. We have to divide our resources – equal parts on security and functionality. Those two things sometimes inhibit one another.

Lecture 3

1. Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
2. Yes, because if perfect security is unattainable, then risk management is the next best thing.
3. A risk I accept is the danger involved when I cross the street. I'm a great walker, and I'm confident that no car will hit me. A risk I avoid is dying from a skydiving accident – so I don't go skydiving. One I mitigate is skateboarding injury – I'll ride without a helmet on the street, but I'll wear one if I do bowl skating. I transfer my health risk to health insurance – they take the blow if I end up in the hospital.
4. I'm sure it has some useful applications on a large scale, but from the example presented in the lecture it is quite naïve. Yes, the chances of a SWIFT transaction being hacked are small, but all it takes is once and the company is down 50,000,000. Perhaps if the value of a single attack was given some weight as well, it would become a more useful tool.
5. There are technical, economical, and psychological factors involved in assessing risk.

Lecture 4

1. The items in the list on slide 2 are tenets of security whereas the items in the list on slide 3 are certain means of achieving those said ends.
2. Availability is most important to me. When I use the internet, half the time I'm just googling something. I want it fast, and I want it now… I don't care who sees that I googled "How long does it take a freighter to cross the Pacific Ocean?"
3. Grouping and categorizing data is the act of separating different levels of data into sections that all pertain to a certain topic, industry, or security level.
4. Authorizations could change over time to prevent malicious attempts to login to accounts that they unauthorized on.
5. Well, if your service is sporadic, you could be booted from the site during a secure transaction, and your money and the product could go into oblivion. Availability serves to bolster reliability, which in turn strengthens security.
6. In purchasing goods online – as a business, you don't want your customers saying they never ordered a $5,000.00 purse when they in fact did, and as a consumer you don't want someone else to gain access to your account and purchase that purse without your consent.

Lecture 5

1. A metapolicy for a cell phone network is make sure that phone calls get to the right places and aren't overheard by other people. A metapolicy for a military

database would say “make sure absolutely no one who in unauthorized sees any information that is not in their security clearance level.”

2. The metapolicy may be ambiguous, and so up for interpretation. The policy helps makes the rules specific and enforceable.
3. Only the guardians of the student and the student can see the academic records. If someone else requests to see the records, notify the students guardians. When e-mail addresses are added for direct records viewing, they must be authenticated as the addresses of the student and his/her family.
4. Yes, stakeholders’ interests could conflict. For example, a student may want his SSN to be used in a document, but that document may not be deemed acceptable, and therefore would have to be destroyed.
5. The likely metapolicy is: Protect the students’ SSNs.
6. The policy is a set of guidelines made to follow the metapolicy. In order to evaluate something, you need to know its intentions, therefore if you don’t understand the metapolicy, you really cannot evaluate the policy.

Lecture 6

1. Military security is mainly about confidentiality because it involves the passing of a lot of highly classified information. However there are still aspects of integrity and availability.
2. The major threat is someone who is not classified on a higher level to access that higher level information.
3. The proviso is there to isolate a certain aspect of security.
4. The labels are in 4 categories in a linear level system.
5. We’re not concerned about how they got there because they are simply there to categorize data – it’s outside our concern.
6. From most sensitive to least: The British have broken the German Enigma codes, The Normandy invasion is scheduled for June 6, Col. Jones just got a raise, Col. Smith didn’t get a raise, the base softball team has a game tomorrow at 3pm, The cafeteria is serving chopped beef on toast today.
7. Codes: Top Secret, Normandy invasion: Secret, Raise info: Private, Softball: Base, Cafeteria: All.
8. You must label it at the highest level because the higher sensitivity information takes precedence in protection. High ranks are allowed to see top secret and secret, but low ranks can only see secret. When it’s an issue of categories, both should be used in order to notify all related actors.

Lecture 7

1. Labels are “affixed” to humans by issuing them clearances or authorization levels.
2. Documents will receive one label and multiple need-to-know categories. Humans will receive one level and multiple need-to-know clearances.
3. In computers, the analogs are permissions and users.
4. The Principle of Least Privilege makes sense because it allows the right amount of access to individuals but nothing more. This way, people don’t see anything they don’t need to see.

5. For the first one, since the guy has Secret clearance and a Crypto need-to-know, and the document sensitivity is a level below him with a Crypto tag, he should be able to access it because he is on a higher clearance level than the document. For the second, it is reversed, and the document is top-secret while the man only has Secret clearance. He should not see the document. Finally, the last document is unclassified and so anyone can see it.

Lecture 8

1. We introduced those terms because they are commonly used in MLS type security.
2. Not symmetric because the levels might match up but not the classifications.
3. Dominates is not a total order because there are cases where neither label dominates the other. This can happen if the sets of classifications for each label are not subsets of one another (disjoint sets).
4. To dominate each other, both labels would have to be the same.
5. It says that you can only access a document if your level is equal to or higher than the document and all the need-to-know categories of the document are in your need-to-know clearances.
6. It's only if instead of if and only if because it means its necessary to gain access, but not sufficient. There might be other hurdles.

Lecture 9

1. It's not enough because it only codifies read access – it doesn't cover write access.
2. We need constraints on write access because we don't want people writing over important information. We also don't want people inserting malicious data into classified documents.
3. As I said before, if you write malicious code disguised in a classified document, it could reek havoc on classified systems.
4. It says that you can only write at or above your own security clearance level.
5. It must be on his security level.
6. He could log out of his Top Secret account and log back in under an unclassified account to contact the private.
7. Yes it is. We could use dominates to make sure the corporal doesn't write to things that he shouldn't be included on.

Lecture 10

1. Being able to change levels is a good idea, but it must implemented in a way that doesn't get used or abused by the wrong people. I.e., I wouldn't want it to violate the tenets of Security.
2. The reality is that some documents need to be changed in terms of security level, and it is not uncommon for subjects to rank up and therefore change their security level.
3. Lowering the level of an object could be dangerous because it would allow access of higher level information to lower level subjects.

4. To downgrade the level of an object, we must make sure it has no information inside that is sensitive at a higher level.

Lecture 11

1. To build a library system, we would have two levels of security: Book, followed by the higher level Guest. Book would be assigned to all objects (books), and Guest would be assigned to all subjects (library guests). Because Book is lower than Guest, all Guests can “read down” into the books, but they can’t write them because they’re only allowed to “write up”.
2. You don’t build a matrix with a BLP system because it is intuitive to know the relationships just by looking at the levels of objects and subjects.

Lecture 12

1.
```
(L,{}) -------------------------→ (H,{})
  |    \                             |
  |         \                        |
  |               \                  |
  |                     \            |
 \/                                 \/
(L,{A}) -----------------------→ (H,{A})
```
2. To find the GLB and HUB, simply follow the arrows to the tail and the front.
3. The lattice is the metapolicy for BLP because it diagraphs domination, which is the sole required tenet of BLP with respect to reads.

Lecture 13

1. Simply, the graph on slide 1 upholds the metapolicy of BLP by letting information flow from Low to High, and not the other way around.
2. Read follows the rules of Simple Security because it only allows the operation to happen if the subject attempting to read dominates the object in question. Conversely, Write works only if the object dominates the subject.
3. Create conforms because the object gets created at the same level as the subject creating it, which ensures read and write access at time of creation. Destroy works because it is simply a form of writing, and it requires write access and an object with name O in existence.
4. BLP has to be in place.
5. Destroy is there to show how a mistake by the system and a L-level subject can alter the documents of a H-level subject.
6. Besides for the time between the creation of the document by H in the left path and its value-setting by the L, the documents are the same.
7. SL does the same thing in both cases to control its role in the transfer of information from SH to SL.
8. SH changing one thing shows that it can actually send information down as a subject, as opposed to what’s recognized in BLP to transfer information, which is an object.
9. It is clear to see than if an action of SH can be seen by SL, the various outcomes (yes or no) of that action can be interpreted as a bit, which can be

strung together as bytes, which means that this system is not fully secure. This transfer of information is called a covert channel.

Lecture 14

1. Talk people talking over coffee is not a covert channel because there is no system whose rules are being broken to give the information away.
2. No, the example given is not a covert channel because either way, SL will get back a 0 to signify that it does not have read access to the file F0, which is presumably a H-level object.
3. The bit of information resides in system storage in Covert Channel #1. Whether or not SL gets back a message for “Resource not found” or “Access denied”, it can arbitrarily decide which one is 0 and which is 1 and proceed from there. SH can create and destroy the file, thus alternating the bit.
4. In Covert Channel #2, the covert bit resides in time. Whether or not p relinquishes the processor immediately, q can check the system clock to decide whether or not that event has happened, thus creating a 0 or 1.
5. In Covert Channel #3, the bit lies within the hardware. Where the read head of the disk is last left decides the bit, however to access that information we would have to time a successive read to figure out where the head was last. So, this covert channel has elements of time and storage.
6. In Covert Channel #4, the implicit channel, the evenness or oddness of an integer in a program decides the bit by using the mod function. Here, the bit lies in bits itself.
7. A termination channel might have low bandwidth because it would require the starting and stopping of a system or computation, which takes a good amount of time.
8. To implement a power channel, you would have to control the energy of the whole system – so, either hijack the whole thing, or ensure there are no other programs running on the system.
9. Power channels might arise with an LED or a simple one-stop capacitor-wielding device.

Lecture 15

1. Covert channels on real processors operate at thousands of bits per second, with no appreciable impact on system processing.
2. It’s infeasible because it would mean literally dismantling an entire system. No process scheduling to eliminate the timing channel – it’s just not doable.
3. To eliminate the issue, we can eliminate the channel, reduce the bandwidth by introducing noise into the channel, or finally we can implement intrusion detection – monitor the channel for anomalous behavior.
4. A high level process modifies a system attribute of a shared object. The low level subject or process observes the change in that attribute. Both processes must have access to that attribute.
5. To utilize the channel, the sender and receiver have to agree upon a set time in which to update the state of the storage object to get reliable change in “bits”.

Lecture 16

1. There's no R because although you know the file exists, the operation does not tell you that it exists. This subtle distinction merits an M rather than R.
2. R and M in the same row means a potential channel because it shows that this attribute can be both read and written to, and if those are done by the right people (a high writes and a low reads), a channel is present.
3. No, this doesn't, because it is the attribute we are concerned about manipulating, not an operation.
4. You'd want to build a table like this to actually identify covert channels and prepare to manage them.