Lucas Harrison

LMH2538

harrisonlucas@utexas.edu

Uhm, I realize this is late by 39 minutes...I was watching the world cup game at a bar. I had you last semester for cs429 and the assignments were always due at midnight and I guess I had assumed that was the case here. I'd appreciate any leniency you could provide in this case as far as late submissions go.

Thanks,

-Lucas

Lecture 1

1. What uses of the term “security” are relevant to your everyday life?

Home security, national security, network security, cyber security.

2. What do these have in common?

They’re all trying to protect something from being taken, misused, or abused.

3. Have you been a victim of lax security?

One time growing up Time Warner shut down our home internet because we had a virus that was using our internet to spam its own messages out into various places on the net. It was clogging up Time Warner’s bandwidth. If we had better firewalls or anti-virus software, that might have been avoidable.

4. What is the likelihood that your laptop is infected? How did you decide?

Well, I don’t have a laptop :P but I imagine my desktop is infected. Not too seriously to the point where I’ve noticed any random processes spawning or slowing performance, but based on the fact that most websites have a vulnerability and therefore could be used to infect my machine, I wouldn’t be surprised if it was. Also, since infected machines tend to stay infected, its likely that I have at least one malware or virus hidden in my machine.

5. What security measures do you employ on your laptop?

None. When I’m surfing reddit and following random links, I do it in an Ubuntu VM so that I don’t accidently get something on my machine.

6. Do you think they are probably effective?

So far, so good. Its definitely not very robust but since I don’t really have anything stopping me from just simply reloading windows if I got a vicious virus, it shouldn’t be a problem.

7. Consider the quote from the FBI ofﬁcial on slide 10. Do you think it over states the case? Justify your answer.

Not really. Some extreme cases could be the stock market crashing, access to secret files, publishing people’s social security numbers allowing identity theft.

8. What is the importance in learning about computer security?

To prevent bad things from happening. Also, having a basic understanding of what can be done to my machine allows me to better defend my personal info.

Lecture 2

1. Consider the ﬁve reasons given why security is hard. Can you think of other factors?

2. Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not?

Not really. You can systematically go through and find places where bad things are a possibility but in any useful system, there are just too many variables to take into account to be able to find all the bad things that might happen.

3. Explain the asymmetry between the defender and attacker in security.

The defender has to think of ALL the bad things that are possible in a system and attempt to protect them and maintain a secure system. The attacker, on the other hand, only has to think of a SINGLE vulnerability that hasn’t been either thought of or protected well enough by the defender. Once that happens, the rest of the defenders’ security measures are out the window.

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?

I do agree. Perfect security is unattainable in any meaningful way. This problem is worsened by how fast technology changes. If everyone was still using windows 98 on their dell Pentium 2’s then maybe there would be perfectly secure networks since every vulnerability has been found and handled. However, in the real world with new architectures, hardware, software, and languages coming out every couple of months, there is never time for the defender to address every possible bad thing that can happen.

5. Explain the statement on slide 8 that a tradeoff is typically required.

Basically, perfect security is attainable, but only on a scale so small that it is useless. You could have a secure network of two computers connected to each other and not to the internet be perfectly secure but it wouldn’t be able to accomplish anything useful on a large scale perspective. So, tradeoffs are necessary to have a decently secure network of 25,000 employees. Things could go wrong, but for the most part everything is okay.

Lecture 3

1. Deﬁne “risk”?

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

2. Do you agree that software security is about managing risk?

Yes I do.

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?

I accept the risk of driving even though it can be deadly. I avoid drinking and driving because it’s not worth the potential downsides that come with it. I mitigate driving having a deadly outcome by wearing my seatbelt and so I don’t have to hear my car beep at me until I put it on. I transfer the risk of our house being robbed by having renter’s insurance. If we are robbed, I don’t have the risk of owning nothing as the insurance will reimburse me.

4. Evaluate annualized loss expectancy as a risk management tool.

It can be pretty helpful. In the given example, you could make it very difficult for tellers to get away with theft and keep your losses to a minimum. For the ATM fraud, you could act reactively since the incidence is very low. After each incidence you could address the vulnerability and keep lowering the incidence rate of ATM fraud. Then, you could put the vast majority of your security resources into the SWIFT fraud prevention because that could lead to bankruptcy while the others are recoverable.

5. List some factors relevant to rational risk assessment.

**Lecture 4**

1. Explain the key distinction between the lists on slides 2 and 3.

The list on slide 3 are ways to accomplish aspects from the list on slide 2.

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.

Confidentiality. If anyone could read my credit card info and address every time I shop at Amazon, then I would have a stolen identity in no time. Some things need to be confidential between sender and receiver.

3. What does it mean “to group and categorize data”?

When you have data that isn’t equally sensitive, you have to group and categorize the data based on how strictly it needs to be protected.

4. Why might authorizations change over time?

If a bank teller got promoted or fired, their authorizations would change. Another case would be with time-sensitive data. For example, the teacher is the only one authorized to see the answers to the test until after the test day. Then, all the students now have the same authorization.

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related?

They are related in the tradeoff sense of security. If a system is secure but not reliably available, then there really isn’t a point to worrying about the security. Also, part of the security problems relate to being able to prevent a malicious user from denying availability to other users.

6. In what contexts would authentication and non-repudiation be considered important?

In banking/identity theft cases. It’s important that there be passwords and other aspects in place to verify it is actually you who is trying to withdraw all your money. Its also important that there be non-repudiation to so that you can prove it actually wasn’t you who withdrew all your money and don’t end up penniless.

**Lecture 5**

1. Describe a possible metapolicy for a cell phone network? A military database?

For a cell phone network, a metapolicy could be that all messages between sender and receiver are confidential to sender and receiver. So people’s phone calls and text messages aren’t able to be intercepted or read by a third party.

For a military database, battle plans are either kept under secure storage or destroyed. Soldiers personal info (address, family member names etc) are confidential. This helps protect the soldier’s family and keeping battle plans under secure storage if deemed necessary and only visible to high ranking officers.

2. Why do you need a policy if you have a metapolicy?

To prevent cases of ambiguity from the metapolicy which allows the policy to provide a clear and effective implementation of the metapolicy.

3. Give three possible rules within a policy concerning students’ academic records.

Only professors can modify the student’s records. Only the students themselves, professors, and faculty can view the students records. The student’s records are securely stored even after graduation to allow proof of the student’s academic accomplishments.

4. Could stakeholders’ interest conflict in a policy? Give an example.

If I wanted to upgrade to a better data plan on my phone, I would have to have my mom do it since the account is under her name. The policy is to only allow plan modifications to be done by the account holder themselves. However, since I am on the account but its not in my name, my interests can’t be addressed due to a conflicting policy.

5. For the example given involving student SSNs, state the likely metapolicy.

Student’s SSNs are confidential and only themselves and certain faculty have access to documents containing a SSN.

6. Explain the statement: ”If you don’t understand the metapolicy, it becomes difficult to justify and evaluate the policy.”

It would be like reading the last chapter out of a book. The book itself is the metapolicy, a well crafted story overall and each individual chapter are the policies. By reading the last chapter without the rest of the story to back it up, the chapter would seem random and probably confusing. You wouldn’t be able to say if the book was good or not because you wouldn’t have the whole story to see if the last chapter was up to par.

**Lecture 6**

1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?

Because the sensitivity levels of information differ so greatly. If certain info got into the hands of spies, the war could take a turn for the worse. If the general’s lunch plans got into a spies hands, who cares. Yes there are also other aspects too. Integrity is huge because if I could call and say “this is your general speaking, where and when are we attacking again?” and find out that easily, then confidentiality policies would be useless. Availability is huge too. For example, if the plan was attack at dawn and a couple minutes before dawn the general gets a peace treaty signed and changes the plans but they aren’t available to the troops because the systems are being DDOS’d, then the attack goes ahead as originally planned even though peace was reached.

2. Describe the major threat in our MLS thought experiment.

Highly sensitive information being accessible to unauthorized/unintended recipients.

3. Why do you think the proviso is there?

Because the example alone is a poor metapolicy. There’s no way to verify you are indeed allowed to see top secret data. Also, availability isn’t addressed because the example is pre-computer era so if a folder went ‘missing’ or was being used a building over, it is unavailable.

4. Explain the form of the labels we’re using.

A double type label that has a hierarchical component to describe the data’s sensitivity and a unranked portion that places the data into any relevant groups where it might be needed.

5. Why do you suppose we’re not concerned with how the labels get there?

Because that’s a policy detail rather than a metapolicy detail. Its easy to just assume that someone fulfills the role of labeling all the documents.

6. Rank the facts listed on slide 6 by sensitivity.

Unclassified: softball game, cafeteria serving beef. Confidential: Col got a raise, col didn’t get a raise. Top Secret: Invading Normandy, broke the enigma code.

7. Invent labels for documents containing each of those facts.

Softball: {Unclassified, All groups}. Raises: {Confidential, Personnel}. Attack plans: {Top Secret: Nuclear, Air Force, Navy}. Broke code: {Top Secret: Crypto}.

8. Justify the rules for “mixed” documents.

By using the highest appropriate level you guarantee nobody can accidently see info above their level. By using both categories, you can guarantee everyone can see the info their supposed to.

**Lecture 7**

1. Document labels are stamped on the outside. How are “labels” affixed to humans?

Through an authorization level and a need to know category.

2. Explain the difference in semantics of labels for documents and labels for humans.

When labeling a document, that indicates the type of info contained inside. However, when labeling a human that indicates how much they are trusted and what group they operate in.

3. In the context of computers what do you think are the analogues of documents? Of humans?

Files could be an analog of documents and users be an analog of humans. Users are afforded certain access restrictions and not all documents are available to them potentially.

4. Explain why the Principle of Least Privilege makes sense.

If your job was to organize the softball game but everyone’s email was confidential and you were only given unclassified access, then it would be impossible for you to get the info needed to contact everyone. If you can’t get enough information needed to complete your job because of your authorization level being too low, then that doesn’t make much sense and is why the least privilege principle works.

5. For each of the pairs of labels on slide 6, explain why the answers in the third column do or do not make sense.

First one, correct group and a higher authorization access than the document. Second one, correct group but a lower authorization level than the document. Third one, no brainer.

**Lecture 8:**

1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?

To better implement policies that reflect the metapolicy. For example, you could use actions to differentiate between two subjects. One would be able to write to an object, but the other can only read.

2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).

Its reflexive in that the hierarchical compenent can be ranked so classified >= classified. Its also transistive because hierarchical compenent has a fixed ordering. Its antisymmetric because again hiearchical compenents have a fixed ordering.

3. Show that dominates is not a total order.

Its not a total order because the set compenent. They could have the same level of clearance but different need to know groups and neither would dominate the other.

4. What would have to be true for two labels to dominate each other?

L1 >= L2 and S2 is in the superset of S1.

5. State informally what the the Simple Security property says.

It says that you can only have read access to data that is at your hierarichal level or below. Which makes sense. You can't read top secret if you're only secret level access. But you can read secret, confidential, and unclassified.

6. Explain why it’s “only if” and not “if and only if.”

Its only if because its not a guaruntee that if satisfied you'll gain access. Its only the first hurdle and there could be other constraints that might prevent read access anyways.

**Lecture 9**

1. Why isn’t Simple Security enough to ensure confidentiality?

Because it only handles the heirarchical component. It doesn't deal with the fact that you may not be in the proper need to know group and really shouldn't have read access.

2. Why do we need constraints on write access?

Write access constraints are neccessary because without them, programs could maliciously write from high access levels down to unclassified from your top secret access without you knowing.

3. What is it about computers, as opposed to human beings, that makes that particularly important?

Humans can be trusted to know that top secret info shouldn't be copied to their facebook. Computers can write sensitive data inadvertantly or maliciously to somewhere it shouldn't be.

4. State informally what the \*-Property says.

It prevents a subject from writing down heirarchical levels which stops accidental/malicious leaking into unclassified levels.

5. What must be true for a subject to have both read and write access to an object?

They would have to be at the same heirarchical level since L1 >= L2 and L1 <= L2.

6. How could we deal with the problem that the General (top secret) can’t send orders to the private (Unclassified)?

He could have seperate logins for the different levels of access and send his messages at the appropriate level.

7. Isn’t it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.

Yes that is a problem but its an integrity problem. Adding another constraint on a per object basis that specifies which levels can overwrite it would be one way to solve the problem.

**Lecture 10:**

1. Evaluate changing a subject’s level (up or down) in light of weak tranquility.

Changing a subject's level with weak tranquility can be potentially non-problematic if the proper conditions are satisfied when something is downgraded. Upgrading a subject isn't too important because its essentially a write-up which is allowed.

2. Why not just use strong tranquility all the time?

Not being able to lower the level of an object can make things overly complicated. For example, if a general wants to email a private he has to logout and login on an unclassified account. However, if weak tranquility was used instead, he could write his email object to the private and then lower its level to unclassified so it could be read by the private.

3. Explain why lowering the level of an object may be dangerous.

The data it contained was at one time more sensitive than its destination level and therefore could maybe not be good for the whole world to see.

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.

The object can't have any residual high level data leftover when being downgraded and should have to pass some conditions rather than just being arbitrarily deemed okay to downgrade. That will help involuntary/malicious downgrading of files.

**Lecture 11:**

1. Suppose you wanted to build a (library) system in which all subjects had read access to all files, but write access to none of them. What levels could you give to subjects and objects?

All subjects would be given a high access and all objects would be given a low level because you can read down but not write down.

2. Why wouldn’t you usually build an access controlmatrix for a BLP system?

Because more often than not the matrix will be huge for a realistic system. Also, you don't need to reference the matrix ever because you can consult the MAC (star property and simple security) and determine if the access is valid.

**Lecture 12**

1. Suppose you had hierarchical levels L, H with L < H, but only had one category A. Draw the lattice. (Use your keyboard and editor to draw it; it doesn’t have to be fancy.)

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?

3. Explain why upward flow in the lattice really is the metapolicy for BLP.

Because the metapolicy for BLP only allows info to flow upwards. You can only write up and only read down. The arrows represent when thats possible.

**Lecture 13**

1. Explain how the BLP rules are supposed to enforce the metapolicy in the

example on slide 1.

2. Argue that the READ and WRITE operations given satisfy BLP.

3. Argue that the CREATE and DESTROY operations given satisfy BLP.

4. What has to be true for the covert channel on slide 5 to work?

5. Why is the DESTROY statement there?

6. Are the contents of any files different in the two paths?

7. Why does SL do the same thing in both cases? Must it?

8. Why does SH do different things? Must it?

9. Justify the statement on slide 7 that begins: “If SL ever sees...”

**Lecture 14**

1. Explain why “two human users talking over coffee is not a covert channel.”

Because information flowing between the two humans doesn't violate the metapolicy of having a talk over coffee. Chatting isn't using a resource not designed for inter-subject communication.

2. Is the following a covert channel? Why or why not?

Send 0 | Send 1

------------------------------------------

Write (SH, F0, 0) | Write (SH, F0, 1)

Read (SL, F0) | Read (SL, F0)

3. Where does the bit of information transmitted “reside” in Covert Channel #1?

Its a storage covert channel which is stored in the system state by the high level subject.

4. In Covert Channel #2?

It doesn't "reside" anywhere since its not stored in any way. The bit is gathered through observation of the time it takes to relinquish the cpu.

5. In Covert Channel #3?

I think this one is more of a timing covert channel so again the bit doesn't really reside anywhere. It is determined based on the timing of a repeated action from the low subject.

6. In Covert Channel #4?

The bit resides in h because the value of a high level variable is impacting the value of the low level variable l.

7. Why might a termination channel have low bandwidth?

Because computations may take a long time to terminate (ie low priority, constantly interrupted) or maybe occur rarely and sporatically.

8. What would have to be true to implement a power channel?

The low level subject would have to be able to access power data during the high level subject's actions.

9. For what sort of devices might power channels arise?

**Lecture 15**

1. Explain why covert channels, while appearing to have such a low bandwidth, can potentially be very serious threats.

Because over time the bits can add up to hundreds of thousands of bits of information sent when there shouldn't be a single bit sent.

2. Why would it be infeasible to eliminate every potential covert channel?

There are too many states in a machine to be able to monitor all of them and make sure they're too noisy or low bandwidth to be unused as a covert channel.

3. If detected, how could one respond appropriately to a covert channel?

You could mitigate the risk and reduce the bandwidth, modify the system implementation to get rid of the channel and avoid the risk, or monitor the channel and catch whoever is using it.

4. Describe a scenario in which a covert storage channel exists.

Sender and reciever have to have access to a shared object. The sender must be able to modify the object and the reciever must be able to read that object.

5. Describe how this covert storage channel can be utilized by the sender and receiver.

It could be used to determine file existance at a higher level.

**Lecture 16**

1. Why wouldn’t the “create” operation have an R in the SRMM for the “file

existence” attribute?

2. Why does an R and M in the same row of an SRMM table indicate a potential

channel?

3. If an R and M are in the same column of an SRMM table, does this also

indicate a potential covert channel? Why or why not?

4. Why would anyone want to go through the trouble to create an SRMM

table?