Yun Wen Chen
dc27863

QUESTIONS WEEK 1

Lecture 1

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

Security is used in a variety of contexts. In my opinion, all of these securities, personal, corporate, personnel, energy, homeland, operational, communications, network, and system, are relevant to my everyday life, directly or indirectly.

2. What do these have in common?

All securities involve the protection of assets from threats, though the type of assets, threats, and protection vary between the different contexts of security.

3. Have you be a victim of lax security?

Yes. There have been several fraudulent charges on my debit card and my computer has definitely had its share of spyware, malware, and trojans.

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

It is highly likely that my laptop is infected. My reasoning is that most of the assets protected by the different contexts of security are now accessible by my laptop. As a result, though attacks are targeted at different assets, they can be retrieved from my computer. For instance, my code and my bank information are two different assets of mine, but a successful computer attack would yield both these assets.

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

I have anti-virus software that periodically scans my file system for malicious content. I check to make sure the websites where I do online business with are secure. I also try to avoid websites that are known to have malware, trojans, etc. However, there is never a "safe" website.

6. Do you think they are probably effective?

I believe they are somewhat effective, but not 100%, because secure sites, anti-virus software, and human judgement all have their own vulnerabilities. Naturally, they can fail to detect malware, but in addition, their software may be compromised as well.

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

I do not think it over-states the case. Cyber-attacks may not be directly capable of ending human lives, but they are definitely capable of destroying government and city infrastructure, the economy, and even the identities of many individuals. If a worm like the Stuxnet Worm shut down power plants across the United States, they would indirectly end the lives of people who are dependent on electric machines for living. In addition, physical assets protected by electronic measures would be vulnerable to looting or theft.

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

The increased access and the increased connectivity of computers are often seen a benefit to society. Access to a computer at an affordable price has increased the number of everyday users and therefore allowed the shift of many different types of everyday assets to be handled online. The disadvantage of this is that all the different contexts of security have now begun to converge to computer security. Not only can a successful computer attack yield multiple types of assets, but they can yield the same assets of a large population. For instance, a thief may come up to you and steal your credit card, but a cyber attack can steal the credit card numbers of every person that has used a credit card at Target. In summary, it seems that the advantages of having increased connectivity and access have allowed for a vulnerability at one central point: the computer. You don't have to be in a dangerous area physically to be attacked electronically, and your attacker does not have to be near you to steal your assets.

Lecture 2

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

Security is hard because there is more reward in infiltrating a system than protecting it. In other words, doing bad things pays better than doing good things. For instance, I highly doubt that the security system developers at Target got paid more than the people responsible for stealing all the customer credit card information.

Security is hard because there is a tradeoff between security intelligence and security threats. If you have one person writing your security code, then you only have one person that is vulnerable to social engineering (or torture). However, that one person could not possibly account for all the possible threats on your asset, and your security would be weak. If you hire a second person to write your security code, they would help account and code for more threats, and therefore make your security stronger. However, you now have two people vulnerable to social engineering (or torture).

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

There is not. Professor Young mentioned in lecture that perfect security is unobtainable. In my opinion, I believe that it is due to the fact that there is an endless amount of threats on an asset. In computer science terms, it is not about being smart enough to write x handlers for x amount of threats, it is about writing code smart enough to handle an infinite amount of threats. There is no way to systematically traverse through each line of code and produce a list of vulnerabilities.

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

The defender needs to protect against all the possible bad things that can happen to their asset. An attacker only needs to find one of those bad things successfully attack the asset. For instance, as a babysitter, there are multiple things that you need to do to prevent the child in your care from being hurt. However, it only takes one bad thing for the child to become hurt.

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

I agree with Morris and Chang. Having a computer alone already creates a physical asset that can be attacked. Having a computer connected to the internet allows attacks from basically anywhere. Even if someone turns off their internet, who is the say that it can not be turned back on by an attack? We did not go too in-depth about drivers in CS 439, but if I can click on the wifi button on my start menu and connect to the internet without having to complete a physical circuit, I'm sure I can accidentally download a malicious piece of software that would do this too.

5. Explain the statement on slide 9 that a tradeoff is typically required.

There is a tradeoff between security and the goals of a project, such as functionality, usability, efficiency, time-to-market, and simplicity. Suppose you have a very secure system, with the downside being that every time you are trying to access your asset, you have to type in five different passwords, call an 800 number to verify your voice, change your password and security questions for your next login, and send in a sample of your DNA to confirm that you are you. In addition, you only have two minutes after you've been granted access to conduct your business before you have to repeat the whole login process. You have great security, but it comes at the cost of functionality, usability, efficiency, and simplicity. In addition, the company that you are selling it to might not want to pay for a DNA test every time you log in. Though this is a radical example, think about how many people use the same password for all their different types of logins. Hacking one login password would give the attacker the password to multiple logins.

Lecture 3

1. Define "risk"?

Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. (Taken from slide 2 on lecture 3)

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

I agree. It is only reasonable that in a large pool of threats, we attempt to prioritize the protection against the threats with the higher probabilities.

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

I accept that my credit card number may be compromised during an online transaction.

I avoid doing online business from websites that do not have a valid certificate.

I mitigate by only buying things online that I can't buy at nearby stores. If a store is out of stock, I make the store order it instead of me personally ordering it.

I transfer the risk to my bank. Typically I can report fraudulent charges to my FDIC-insured bank and they will return my money.

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

We can modify an annualized loss expectancy table to contain the threat type, the monetary loss of a successful attack, and the likelihood of this threat. The ALE value would be the monetary loss multiplied by the likelihood. Higher ALE values would support the prioritization of security measures for that type of threat over those with lower ALE values.

While the ALE value holds some weight, the value is devoid of any background information that may be critical to good decision-making. As mentioned in the lecture, the expectancy value for the two scenarios on slide 6 would be yield $1. In one scenario, I would get a dollar. In the other, I could gain $1000 or lose $998. If $998 wasn't a big deal to me, I would flip the coin. If I had only $5 to my name however, I would rather choose to have the guaranteed $1.

5. List some factors relevant to rational risk assessment.

Rational risk management takes into account annualized loss expectancy but also includes technical, economic, psychological factors.

Lecture 4

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

Confidentiality, integrity, and availability on slide 2 are the goals of security. The list on slide 3 are the mechanisms in which we try to achieve this goal. For instance, if losing weight is the goal, then eating healthy and exercising are the mechanisms used to achieve this goal.

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

In my opinion, all three aspects of security are equally important. As a 22 year old, my two main (and perhaps only) assets are my identity and my monetary savings. Having a decent credit score, a stable job, and some savings makes my identity a good candidate for identity theft and credit fraud. Therefore, confidentiality is important to me as it protects me against people retrieving my identity and credit score to register for credit cards. Simultaneously, integrity is important because I want any modifications to my assets to only come from me and relevant people. Finally, as I typically need my money and identity ever day, availability is important to me on an everyday basis because I want to commit transactions at any time when I know I have the money.

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

To group and categorize data means to separate your data into groups based on its level of sensitivity. Data groups with higher sensitivity naturally require more protection, such as your social security and bank account number, while data groups with lower sensitivity would require little or no protection, such as the number of likes you get on a particular Facebook picture.

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

Availability and reliability are related because reliable systems give resources the traits of availability. If a reliable system provides resources in a timely, reasonable, and fair fashion, then those resources are available. If there are multiple requests for the resource, reliable systems will have concurrency control, thus making sure that your request does not give you a resource already owned by someone else. The traits of a reliable system work together to make sure the resource that you want is available.

5. In what contexts would authentication and nonrepudiation be considered important?

Online banking is a good example where authentication and non-repudiation would be considered important. Authentication is important because I want myself and a banker to be the only ones allowed in modifying my bank account. Non-repudiation is important on the banker's end because I could report fraudulent charges on transactions I've actually made in order to have my money returned to me while still keeping the asset I acquired with it.

Lecture 5

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

We should protect the confidentiality of customer phone numbers in a cell phone network.
We should protect the confidentiality and integrity of a military database.

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

A metapolicy is the overall security goals of the system. The policy is the set of detailed rules that users and developers have to follow in order to uphold the metapolicy. We need a policy because metapolicies are often too general and too open to interpretation. A policy then, is the set of security system-specific rules that work together to uphold the metapolicy. There is a policy at the Austin Animal Shelter about interactions between dogs. The rules are that two dogs that don't share a kennel together may not play together, or even touch noses. Knowing just the rules, we might not know why they exist. However, it may be that the metapolicy is to protect dogs against each other, either from fighting with each other or spreading diseases from contact.

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

Faculty/staff may not use student SSNs in documents/files/postings.

Documents containing SSNs must be destroyed unless deemed necessary.

Documents containing SSNs and deemed necessary for retention must be kept in secure storage.

Could stakeholders' interests conflict in a policy? Give an example.

Yes. Suppose there is a policy in a department that sets the registration times for a student based on their degree completion percentage in their interactive degree audit. Suppose there are two students who have completed the same sources, with one student having been with the department since freshman year, and the other being a transfer student with equivalent coursework. However, the transfer student has a lower IDA percentage because their transfer courses did not map correctly to the IDA algorithm, and proposes a rule that states every transfer student can meet with an advisor and get an accurate IDA percentage to be used to determine registration time. The regular student, knowing how cut-throat registration is, wants the rule to reflect solely on the unadjusted IDA percentage, simple to reduce the number of competitors for seats. In this case, the rules proposed by the stakeholders, the two students, conflict.

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

The likely metapolicy is to protect the confidentiality of student social security numbers.

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

If you don't understand the goals of your security system, it will be hard to first, determine the specific, lower level, system rules you need to uphold the goals of your security system, and second, justify why you are carrying out these specific measures.

Consider the student SSN example in lecture. Suppose the metapolicy was changed to solely secure the availability of student SSNs. Suppose I didn't understand this metapolicy and created a policy that had the same rules in question #3. It would be difficult to justify why documents containing SSNs need to be destroyed and necessary documents need to kept in secure storage because having to run back and forth from the secure storage room to retrieve SSNs would increase access time and decrease availability. Because I didn't understand my metapolicy, my policy wasn't suited to best uphold my metapolicy.

Lecture 6

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

Military security is mainly about confidentiality because it is crucial that we only let information be seen by people who are trusted to see that information. If the location of military bases in Afghanistan is seen by terrorists, then they would be able to attack our troops.

Naturally, there are aspects of integrity and availability. Naturally, you do not want a terrorist to write, modify, or generate information, as they could easily manipulate our forces to their advantage. Finally, availability is also important, as requests for military assets or data typically need a quick and accurate turn-around time.

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

The major threat would be that the "wrong person" seeing a particular piece of data.

3. Why do you think the proviso is there?

I think the proviso exists because it may be tricky to formulate policies on confidentiality, integrity, and availability simultaneously without accidentally producing some vulnerabilities in the system. For instance, suppose the chopped beef on toast and the Normandy invasion date were on the same document. To protect the confidentiality of the Normandy invasion date, you classify the document as top secret. However, that means that only very limited people get to see that the cafeteria is serving chopped beef on toast today. As a result, you have a good confidentiality protection, but not a good availability one in terms of the lunch announcement. In addition, if the document is top secret, then the cafeteria staff may not be able to change the menu of today to fried chicken, which impedes the integrity of the lunch data. It supports Professors Young' statement that considering integrity and availability simultaneously may lead to counterintuitive thinking.

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

The first component of our label is the hierarchal component. This label is a token from a linearly ordered set. In the context of military security, the set includes, unclassified, confidential, secret, and top secret, with unclassified being least sensitive, confidential being more sensitive than unclassified, and so on, with top secret being most sensitive.

The second component of our label is the "need-to-know" categories. This label is a token from an unordered set. In the context of military security, the set includes, crypto, nuclear, janitorial, and personnel. This label determines which group of people see the file. There is no reason why the crypto and nuclear group need to see each other's confidential files, therefore security is increased when only the right people see the right files.

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

We are not conceded with how the labels get there because it is beyond our scope of responsibility. It is not our job to determine the sensitivity of a file, only to protect the file with the necessary security.

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

Ranked from highest to lowest sensitivity

- The Normandy invasion is scheduled for June 6.
- The British have broken the German Enigma codes.
- 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. Invent labels for documents containing each of those facts.

(Top Secret: {Crypto, Nuclear}) The Normandy innovation is scheduled for June 6.
(Top Secret: {Crypto}) The British have broken the German Enigma codes.
(Confidential: {Personnel}) Col. Jones just got a raise.
(Confidential: {Personnel}) Col. Smith didn't get a raise.
(Unclassified) The base softball team has a game tomorrow at 3pm.
(Unclassified) The cafeteria is serving chopped beef on toast today.

8. Justify the rules for "mixed" documents.

If you have a document that contains both sensitive and non-sensitive information, it is intuitive that you label it as the highest appropriate level. If the chopped beef on toast and the Normandy invasion information were on the same document, you assign the document as top secret, as it is your top priority to protect the most sensitive information.

If a document contains information relating to multiple need-to-know groups, you have to label it with both categories because while a group person may be only searching for their part of the data in the document, they are also exposed to the other group's data. Thus, logically, they would need to be authorized to see it.

Lecture 7

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

Labels are affixed to humans based on group and trust. The trust component of the label indicates the level of sensitive information the human can see, unclassified, classified, secret, top secret. The group component of the label indicates the type of information the human can see. If a person is authorized for secret and works in crypto, they shouldn't be able to see a top secret crypto file, nor a secret nuclear file.

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

Labels for humans are somewhat opposite of labels for documents. You label a document based on the highest sensitive information found in the document whereas you label a human with the minimum amount of authorization needed in order to do their jobs.

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

In the context of operating system, documents could be analogous to computing instructions whereas humans could be analogous to threads. User-level threads cannot execute privileged instructions whereas kernel-level threads can. This is to protect the computer from malicious programs.

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

The Principle of Least Privilege makes sense because any subject with access to the information is capable of leaking that information. Therefore, it makes sense that a subject should only have the information necessary to do their job. For instance, in the military security context, even if you are in the crypto group, you might not need access to the top secret or even secret information, therefore you shouldn't be authorized for it until you actually need it.

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.

(Secret: {Crypto}), (Confidential: {Crypto}), Yes
This answer makes sense because this human is cleared to the secret level in the crypto group and the document is in the confidential level in the crypto group. Since confidential is less sensitive than secret, and this document and the human belong in the crypto group, the human should be allowed to access it.

(Secret: {Crypto, Nuclear}), (Top Secret: {Crypto}), No
This answer makes sense because even before analyzing his group clearance, he is already not cleared to view top secret documents, which is more sensitive than secret, the human's level of sensitivity clearance.

(Secret: {Nuclear}), (Unclassified: {}), yes
This answer makes sense because the document is unclassified, meaning everybody (to some extent) is allowed to see it.

Lecture 8

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

Vocabulary terms like objects and subjects help differentiate between entities that are requesting a resource, and the resource. In the previous lecture, humans and documents shared the same labels, though interpreted and assigned differently. However, it is very easy to confuse what label is for humans and what labels are for documents as they may share the same token name.

Actions are operations executed on behalf of subjects on objects, and it helps distinguish between operations that are caused by subjects and operations necessary to manage objects.

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

Reflexive: If A is a label with (L_a, S_a), then $A \geq A$ because $L_a \geq L_a$ and $S_a \subseteq S_a$ In other words, A dominates itself.

Transitive: If $A \geq B$ and $B \geq C$, then by the linear set properties, $A \geq C$. In addition if A is a superset of B, and B is a superset of C, then A is also a superset of C, as everything that exists in C exists in B, and everything that exists in B exists in A.

Antisymmetric: If $L_a \geq L_b$ and $L_b \geq L_a$, then L_a cannot be lower than L_b and L_b cannot be lower than L_a. Therefore, the only value where this is true is if $L_a = L_b$. In addition, if S_a has to be a superset of S_b and S_b has to be a superset of S_a, then the only value where this is true is if and only if $S_a = S_b$. Thus, label A = label B.

3. Show that dominates is not a total order.

Dominates is not a total order because of the property of totality, which states that $A \leq B$ or $B \leq A$. In other words, A must dominate B or B must dominate A. However, in the case of (Top Secret: {Crypto}) and (Top Secret: {Nuclear}), neither of these labels dominate each other.

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

They would have to be identical.

5. State informally what the Simple Security property says.

The Simple Security property simply states that you can only read objects that are at your level of clearance or lower.

6. Explain why it's "only if" and not "if and only if."

The Simple Security property is an only if condition because it may not be the only condition that needs to be satisfied in order to gain read access to the object.

Lecture 9

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

The Simple Security property ensures that only a person with the right level of clearance can read a file. However, it fails to account for a subject writing information to a place where it shouldn't be.

2. Why do we need constrains on write access?

We need constrains on write access because a subject could read an object at their level of clearance, yet write to a place with a lower level of sensitivity, thus ruining the sensitivity protection of the information.

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

It is easy to decide read/write access to humans based on their level of clearance. However, when they are on the computer, there are many running processes and applications that essentially do not have that level of clearance. For instance, suppose you are simultaneously watching a movie and doing online banking. You have clearance to access your money, the online banking application has clearance to access your money, but Netflix shouldn't have access to your money. Malicious software like key-loggers can "gain" clearance to your assets by trying to impersonate you and your level of clearance.

4. State informally what the *-Property says.

The *-Property basically means that you can't write information down sensitivity levels, only at your level of clearance or higher.

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

Since the Simple Security property states that a subject can only read an object if the subject's label dominates the objects label and the *-Property states that a subject can only write to an object if the object's label dominates the subject, having both read and write access would mean that the subject's label and the object's label have to dominate each other. Thus, both the subject and object's label should be identical.

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

The General may log out of his Top-Secret clearance account and log into to an Unclassified account and send the necessary information to the private. We are trusting that the General would not sent top secret information to the private, but that trust exists outside of the security system. We're assuming he's a good guy.

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

It is a problem, but with the issue of integrity, not confidentiality. We could deal with that by identifying rules that indicate which level of clearance is required to write a certain type of document, such as a war plan.

Lecture 10

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

Raising the level of a subject arbitrarily is bad because now a low level subject is allowed to access higher sensitivity objects.

Lowering the level of a subject arbitrarily is tricky because the subject may have some residual high-level information, which causes information to flow down.

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

It is hard to always use strong tranquility because subjects are often dynamic. Human subjects, move, get promoted, and get demoted frequently. In addition, new objects may be created at a different sensitivity level that may require a subject to increase clearance in order to do their jobs.

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

Lowering the level of an object is dangerous because while the sensitivity of the object may not change, the intensity of protection for that object does.

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

In order to downgrade an object, it must not in any way violate the security of the system. The combination of the Simple Secuirty, *-Property, and one of the tranquility properties would allow a model that could allow safe downgrading.

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?

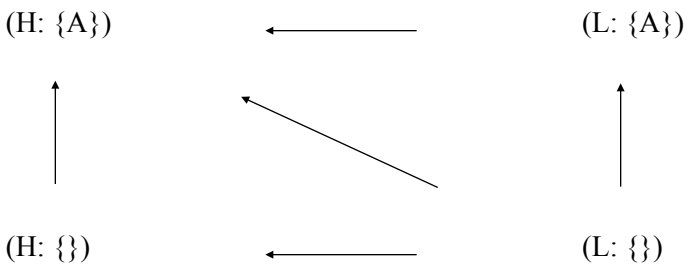
You would give levels to the subjects and objects such that all subject labels dominate object labels and no object labels dominate any subject label. This allows read access, as explained by the Simple Security property.

2. Why wouldn't you usually build an access control matrix for a BLP system?

You can compute the access permissions almost instantaneously by simply consulting the Simple Security property and the *-Property.

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 the BLP system, what is the algorithm for finding their LUB and GLB?

To find the greatest lower bound, find the label with the highest number of arrows point away from it.

To find the least upper bound, find the label with the highest number or arrows pointing to it.

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

The upward flow of the lattice is the metapolicy for BLP because it defines a system where information can only flow up, which is what we want.

Lecture 13

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

Information should blow from low to high, but not high to low. The *-Property and the Simple Security property are the parts of BLP rules that prevent this from happening.

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

The READ operation will only return the correct value if the the label of the subject dominates the label of the object, otherwise it would return 0. The WRITE operation will only write to the object if the label of the object dominates the label of the subject, otherwise it would return 0. The rules of these operations satisfy the Simple Security property and the *-Property, therefore, they satisfy BLP.

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

The CREATE operation creates a new object at the level of the subject. If the object already exists, it does nothing. This satisfies BLP, as a subject can only write at their level of clearance and higher.

The DESTROY operation destroys an object only if the level of the object donates the level of the subject. This satisfies BLP, because destroy essentially overwrites the object with nothing, thus, it needs to satisfy

the *-Property. Since destroy can only happen successfully if the object dominates the subject, it satisfies BLP.

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

The high-level subject must create the object.

5. Why is the DESTROY statement there?

The destroy statements allows the low level subject to constantly create new objects, allowing the passing of multiple arbitrary bits that flows from high to low.

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

Yes

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

It must because like the scientific processes, you can only observe changes in a particular environment by having a controlled setting.

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

A SH may do different things because it is just carrying out its actions. The SL can see these actions and the results and determine the information. Therefore, SH does not need to be controlled. In fact, it is the manipulated variable.

9. Justify the statement on slide 7 that begins: "If SL ever sees…"

If a low level subject can see results in response to actions executed from high-level subjects, it allows the flow of information from the high-level subject to the low-level subject, which violates the metapolicy. In other words, if a low level subject can see the actions of the high-level subject and the results from those actions, they can deduce what is going on, thus receiving information.

Lecture 14

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

Two humans talking over coffee is not a covert channel, because typically, two humans talking over coffee is a valid method of communicating information. However, if someone else is measuring the wavelength of the coffee to decipher what words are being pronounced by a person, that may be a covert channel.

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)
```

This is not a covert channel, just a violation of BLP. Either a high-level subject is trying to write down, or a low-level subject is trying to read up.

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

In the system state.

4. In Covert Channel #2?

The process timer.

5. In Covert Channel #3?

The sectors on the shared disk drive.

6. In Covert Channel #4?

The value of i.

7. Why might a termination channel have low bandwidth?

Termination channels might have low bandwidth because most operations execute quickly, so the metadata would be smaller.

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

The lower-level subject must be able to observe power levels based on actions of a high-level subject.

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

Electricity-delivering devices.

Lecture 15

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

Covert channels, despite having low band-width and only extracting bits, can be looped to extract hundreds, thousands, or even million bits of data.

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

A channel may exist but may be very noisy, so it is hard to determine what is being transmitted, if anything is being transmitted at all.

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

Modify the system implementation.

Introduce noise to the channel.

Monitor it for patterns and usage to determine is someone is trying to exploit it.

(Slide 4, Lecture 15)

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

Suppose both the sender and the receiver have access to a system variable that indicates what type of handler needs to be executed after a certain error.

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

The sender uses this covert storage channel to help reference the correct handler for a program, whether it be an error, exception, etc. The receiver is able to watch what the high-level subject has done and the error that it caused by looking at the attribute in the covert channel. As a result, the receiver, or the attacker, may be able to map out the structure of the handler files and design a malicious piece of code to attack a program based on it.

Lecture 16

1. Why wouldn't the "create" operation have an R in the SRMM for the "file existence" attribute?

The CREATE operation creates an object. If the object exists, it does nothing. If an object is created, there is no indication that it is. As a result, the CREATE operation doesn't provide information about whether the file exists or not, thus, it is labeled M.

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

If and R and M exist in the same row, it means that the attribute has a mechanism where someone can modify it and someone can reference it, which are the abilities required by a covert channel. In other words, there are operations that can signal changes and there are operations that can notice these changes.

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?

No. Having R and M in the same column means only means that you are observing R and M across different attributes. If you have R and M in the same column, but not across rows, there is still no mechanism where someone can modify an attribute and someone can reference it. Though we are analyzing the same operation, we are concerned with the attributes that use it.

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

Making an SRMM table can help see where a potential channel could be. Even if a developer was an expert at his software, an SRMM table outlines every potential covert channel. It is a very systematic, though maybe tedious way of eliminating covert channels. It relates to the lecture where Professor Young mentions that the bad guys only need to find one way to get in, whereas the good guys have to find all the ways that bad guys can get in.