Yun Jang

ysj238

CS 361 Questions - Week 1

Lecture 1

1. The uses of security in my everyday life would be pretty much everything that I use on a daily basis. For example, my email, online storage, and more all have security to prevent unauthorized access.
2. Security and passwords are pretty much the same in terms of purpose; the two are defined methods of protection.
3. Not directly, but it might be fair to say yes due to the recent Heartbleed exploit.
4. I'm sure that this laptop is infected. It seemed like a reasonable answer as no one is truly ever sure what is on the websites on the Internet (everything may have some sort of malicious security vulnerability).
5. Personally, I don't have any security measures other than not using a poorly developed and highly targeted browser (good example being Internet Explorer).
6. I think it is mostly effective. I have yet to have my entire system overtaken by a malicious user or have my accounts accessed by unauthorized users.
7. No, I don't. This is because everything that is created and developed now are set up to use the global Internet. Additionally, considering the fact that the government and the military does not use some sort of special operating system that boasts high security, it seems more than likely that several programmers could overtake the United State's network and hinder the military.
8. It is important to learn about computer security in order to protect yourself from danger, contribute to security, and improve the overall safety of the Internet.

Lecture 2

1. Security is difficult as a developer because:

* You have to think about all possible attacks before the attacker.
* Must defend against all attacks; attacker only has to attack one vulnerability.
* Information management is large and complex.
* Principle of Easiest Penetration means intruders will use any available means to outdo security.
* Security is an afterthought; we like to program useful things -- not security.
* And no, I don't think I can think of any other factors other than the fact that no human is perfect and cannot protect against all loopholes.

1. There is no systematic way to list the "bad things" that may happen to a program because security is actively exploited by the attacker at all times.
2. The difference between the defender and attacker in security is the defender must protect against all; attacker only needs to attack one vulnerability.
3. I do agree (although the quotes are quite overboard). This is because all the software that have been made so far are made for the sake of being useful and increasing productivity. But in doing so, it increases the amount of vulnerabilities (which may be endless).
4. Trade-off is often required as developing a certain function to improve usefulness means creating one or more vulnerable aspects of a program. Because of that, trade-offs need to be evaluated.

Lecture 3

1. Risk is a possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
2. Yes, I do since there are always security tradeoffs when dealing with programming.
3. For this question:

* A risk that I would accept is driving a car. There is a chance I can get into an accident but it will get me from one location to another very quickly.
* One I would avoid is driving on the highway and taking local roads; this would allow me to avoid a costly accident but still allow me to get places faster.
* To mitigate a risk, I would drive a less expensive car instead of a more expensive one to reduce the total outcome of an accident.
* Lastly, to transfer a risk, I could just invest in insurance to shift the possibility of a risk from an accident.

1. Annualized Loss Expectancy (ALE) is a tool that simply creates a table of possible losses and their likelihood. Basically, this gives you a better idea of what risks are more likely and how costly they are -- giving you a better idea of what risks one may have to face.
2. Factors that are relevant to rational risk assessment are technical factors, economical factors, psychological factors, and more.

Lecture 4

1. In slide 2, those are the aspects of security that we are aiming to protect. Slide 3 contains “mechanisms” that are developed in order to protect the aspects of security.
2. Confidentiality – because I would prefer to have control and limit others from being able to read the information that I enter and use every single day. Modification is also of concern but not as much as confidentiality (even though they go hand in hand). Availability would not be that great of a concern to me, however.
3. To “group and categorize data” means to split out your data into different areas of permissions basically. You would move certain files to a more secure folder and other generic files to a lesser secure folder.
4. Authorization may change as certain files may become less important or secure. Additionally, authorization of a file may change so that a different user may access it (other than me).
5. The two are related because a resource being available also means that it is a reliable resource. If I have a file that is uploaded to an online storage and I have access to it again from any point of location, not only is it being available, it is also reliable in the sense that I am able to retrieve it from any point of location.
6. Authentication and non-repudiation would be considered important in many scenarios such as online shopping. Authentication is a requirement in many login processes in order to verify and establish who the user is. Non-repudiation also applies to the online shopping scenario as it prevents the shopper or the seller from denying a purchase or sale (respectively).

Lecture 5

1. A possible metapolicy for a cell phone network would be keeping the confidentiality of calls and messages that are sent over the network. As for a military database, aiming to keep the confidentiality and integrity of the database would be a possible metapolicy due to detailed military plans.
2. A policy is needed even if a metapolicy is present because the metapolicy only presents an overall security goal. Policy places more specific details on security by analyzing security assessments and utilizing mechanisms.
3. Three possible rules would be: digital signatures (to prevent potential phishing while accessing the records), access controls, and passwords.
4. Yes, it could. For example, by allowing a stakeholder to have access to their personal data online (for their convenience) also puts their personal information at risk. Additionally, it conflicts as the availability of their data is hindered by the mechanisms (such as using passwords).
5. The likely metapolicy would be to keep the social security numbers in a secure database or remove them after use.
6. Because the metapolicy is the general, overall goal of security, it becomes difficult to develop the specific set of rules (policies) without understanding the basis of security needed for the project.

Lecture 6

1. The military focuses mainly on confidentiality as they have information that cannot be leaked to the public – which would put the nation at risk. Integrity and availability also pertain to military security. The nation would want to maintain integrity by not allowing any military personnel from making undocumented modifications. Lastly, the government would probably want availability in case of any dire emergency.
2. In the MLS thought experiment, the major threat we’re protecting against is unauthorized access to data from members who are not privileged to view the piece of information.
3. The proviso is there to limit our scope in terms of thinking about security. Otherwise, if we mixed in the other two with confidentiality, we’d have to think about more cases that may affect the confidentiality security assessment.
4. The labels that are used in our experiment justify our authorization level and who can access the files.
5. We’re not concerned about how the labels get there as they provide authorization levels on their own (as in, only those with that level of access can use those files with those labels).
6. The list of facts by number:

* Fact 1 – General
* Fact 2 – National Secret
* Fact 3 – General
* Fact 4 – Personal Work
* Fact 5 – Personal Work
* Fact 6 – Military Secrets

1. The labels for those facts:

* Fact 1 – Unclassified
* Fact 2 – Top Secret
* Fact 3 – Unclassified
* Fact 4 – Confidential
* Fact 5 – Confidential
* Fact 6 – Secret

1. If there is a file with high-level classification inside a document, then it should take the authorization level of that high-level classification and above. Otherwise, the risk of security vulnerability would be extremely high.

Lecture 7

1. “Labels” that are assigned to humans act as a permissions key. If the label they have is greater than or equal to the label on the document, they have access to it.
2. The difference is that the label affixed to a document is static. Requirements of that document label act as a specific permission that must be met. However, the label for humans act different as their label grants them permission to a document label of equal or lesser level.
3. Document labels are like specific locks. Labels for humans are like a keychain with keys for each label.
4. It makes sense as a subject should only have enough permission to get the information needed to do their business. Any more would raise the chance of compromising information.
5. The answers do make sense. If the clearance that the human has is greater than or equal of the sensitivity label, the human would have access to them.

Lecture 8

1. I believe the terms were used to make the scope of security a little easier to comprehend. Now it allows us to label and reference security policy more fluently.
2. Dominates can be proved as partial by plugging in equal labels with different hierarchical components into the Dominates Relation definition.
3. Dominates is not total order. For example, say Subject A has access to a Secret Object under Action Alpha. Subject B has access to a Secret Object under Action Beta. If Subject A were to try and access the Secret Object under Action Beta, it would not work despite the fact that Subject A has clearance to the Secret Object. Vice versa for Subject B.
4. For the two labels to dominate each other, the hierarchical component of the first one is greater than or equal to the hierarchical component of the second one.
5. Basically, it means that if the subject has clearance greater than or equal to the desired object, then the subject would gain read access.
6. It is “only if” as there are additional security constraints that the subject may have to go through in order to gain clearance on the access. This would be why the proviso was mentioned earlier.

Lecture 9

1. Because a subject with high object access could copy and write the data to a lower object access – granting subjects with lower object access the permissions to read the data.
2. We need constraints on write access because those with write access may end up writing the data to places where it shouldn’t be or doesn’t belong.
3. Computers are different and particularly more important because they aren’t simply doing one thing at a time (unlike humans). Computers may be running multiple programs and throughout the day run several programs that may have malicious logic embedded within them.
4. Basically, the \*-Property states that the subject can only write up to higher objects. They cannot write down to lower objects.
5. For a subject to have both read and write access, the subject must be at the same level/permission as the object.
6. The General would have to log out of their Top Secret account and log into the lower Unclassified account before sending the orders. This way, it excludes any attempt that a malicious program would try and send an order with that information from an account with higher object permission.
7. We could deal with that problem by having some sort of authorization system that would notify the higher subjects with a request saying that the corporal wants to update the war plan. This way, the request gets verified by the higher subjects and can be confirmed to overwrite the plan.

Lecture 10

1. Changing a subject up would cause major security issues. It would grant that lower subject permission and access to more secure information that was above them (read up). Changing a subject down also has some particular security issues as they may have some residual upper security that ends up transferring down (essentially being write down which is not allowed).
2. Having strong tranquility the entire time would have massive constraints as it creates a concrete set of security that cannot be modified in the lifetime of the system. It would cause more problems for the user rather than useful.
3. It is dangerous as it would be breaking the goals of Simple Security Property and the \*-Property. Lowering the level of an object is basically like “writing down.”
4. The conditions that would have to hold would be that the data inside the object that is being lowered would have to deleted or transferred to an object of equal or greater security level. Then the object could be securely downgraded, as it would no longer contain high security objects.

Lecture 11

1. To build a system like that, I would have the subjects be on a level that is all above the objects. This way, the subjects would be able to view all of the objects but not write due to Simple Security Property (preventing them from writing down).
2. Realistically, you wouldn’t build an access control matrix for a BLP system because it’s too large.

Lecture 12

1. (H, {A}) <--------------- (H, { })

^ ^

| |

| |

(L, {A}) <--------------- (L, { })

1. The algorithm for finding the LBU and GLB involves seeing the path from L1 and L2. If the path from L1 and L2 in the graph is such that L1 is less than or equal to L2, then you can find their LUB and GLB.
2. The upward flow in BLP is the metapolicy in order to constrain the flow of information among different levels of security.

Lecture 13

1. BLP rules enforce the metapolicy in slide 1 as the lattice is shown that information can only be written from the low subject to the high subject but not vice versa.
2. The READ and WRITE operations satisfy BLP because it pretty much follows suit to the security properties it consists of. The READ can only be done if the subject is greater than or equal to the object. The WRITE can only be done if the subject is less than or equal to the object.
3. Similarly, the CREATE and DESTORY operations also somewhat satisfy the BLP. The CREATE operation can only be done if the object at that subject’s level doesn’t already exit. Lastly, the DESTROY operation can only be done to the object if the subject’s level is less than or equal to it (to prevent the higher subject from DESTROYING all lower objects).
4. The subject with the higher level must not create the object F0 in order to allow the lower level subject to CREATE F0 and WRITE/READ from it.
5. Since this mechanism is a covert channel, any information that needed to be created can be destroyed for the sake of security.
6. No, the contents of the file are not different in the two paths. Both paths obey BLP properties.
7. SL does the exact same thing because the operations that it performs are legal and safe according to the BLP properties. It can write up, read, and destroy as long as the level of the object is equal to SL. And it doesn’t necessarily to the same thing in the both cases; the second case allows SL to see a value of 1 but it just doesn’t do anything different with it.
8. SH performs different things in when it varies it behavior. This is because SH has higher level of security which may allow or not allow the SH from signaling a bit of information to the lower level. So, in this case, SH must do different behavior if it wants to signal information.
9. Basically, it is stating that the two subjects can communicate with each other to send arbitrary amount of data even though in terms of security, it isn’t allowed. This could allow for malicious actions that violate the metapolicy.

Lecture 14

1. It isn’t a covert channel since they aren’t manipulating a system resource in order to illegally flow information. They are within the flow of the system.
2. Yes, because the high level subject is writing to a file and a lower level subject is reading from that same file. It is more than likely a covert channel as the lower level subject is reading the file that the high level subject is consistently writing to.
3. The bit of information that is transmitted is stored in the status of the resource (or the system state). This is called the covert storage channel.
4. It is stored in the system clock by reading the bit based on the time that has elapsed since it was last scheduled. This is called a covert timing channel.
5. In Covert Channel 3, the bit of information resides in the disk head. It depends on where the read head is the closest on the cylinders.
6. The bit of information transmitted resides in the program fragment. The value of the high level or the low level is set depending on the value of the high or the low. This is an example of language-based information flow tools.
7. A termination channel would have low bandwidth because it can only send so many number of bits through the channel – preventing the channel from providing security over the data that is transmitted.
8. For a power channel to be true, the main system would have to be able to read from a device that outputs some signal or power level.
9. A smartcard would be one where the power channels would be involved.

Lecture 15

1. It can be a serious threat because these are real processors, which can do thousands and thousands of computation per second. Even if it is a single bit of information being transmitted, it can be done extremely quickly.
2. There are many factors such as the low bandwidth and how noisy the covert channel is. Which is why it is impossible to truly eliminate all covert channels in a real life system.
3. One could modify the system implementation, reduce the bandwidth of the channel by adding noise, or monitor the usage of the channel to see if it is being exploited. This is called intrusion detection.
4. A possible scenario would be the UNIX file system with the read and write properties of the owner being able to modify the piece of data. Any lower level subject would be able to read (or view) that file (the attribute). Whenever the owner updates the file, the lower level subject would be able to continually read the file and gain information.
5. This storage channel could be used to move sensitive data from higher security to lower security by reading the data from the higher security object. The data being read can then be brought down to a lower level by copying it into a lower level object.

Lecture 16

1. It is because the operation CREATE does not tell us about the fact whether the object the subject wants to create exists or not.
2. It means that there exists a mechanism where subjects can potentially read and write from the system – exposing a potential covert channel.
3. It could but also it could not. This is because it would depend on the semantics of the system you’re building the Shared Resource Matrix Methodology table. So, depending on the implementation it could indicate a potential covert channel but also not.
4. Despite how difficult it is to implement due to how specific the SRMM tables must be, it is a secure way of guarding against potential covert channels.