WEEK ONE LECTURE QUESTIONS

Charu Sharma
CS361
Dr. Young
Due: Thursday, 6/12/2014

LECTURE ONE

1. Personal security, corporate security (in the workplace and as a customer), energy security, homeland security (as a citizen), communications security (as a correspondent), network security (as an Internet user), and system security all affect me in daily life.
2. Each of these types of security is trying to protect some asset deemed valuable, whether it be physical body, data, or resources, safe from external threats through protection.
3. I have been a victim of viruses and therefore of lax PC security.
4. Because I use Norton Antivirus, I think the likelihood that my laptop is infected *without my knowledge* is low. However, to my knowledge, it is highly possible certain data is revealed, such as data gleaned by search engines and online retailers of past online behavior.
5. I employ Norton Antivirus on my laptop. Additionally, I only enter credit card information and other sensitive data on well-known, secured payment services.
6. I think it is probably effective to an extent. Though it can and has been breach, it is often effective after that point at notifying me of the breach and taking care of it.
7. I do not think that the FBI official quote overstates the case. Our country is at least partially and certainly vitally built on data, and it often depends on the privacy of that data. Although security engineers can attempt to foresee every possible attack, it is unlikely that they can keep up with *every* attacker's potential plan. As such, data security breaches could take down our nation.
8. Computer security education is beneficial in enhancing personal protection, workplace security, interpersonal and business transaction security, and general cyberspace security.

LECTURE TWO

1. I think security is additionally hard, because the balance between efficiency and security must always be struck. Because it is a tradeoff, I imagine it is often tempting to increase efficiency at the risk of decreasing security. Also, I think security is difficult because it is hard to define. Each person's understanding and definition of security differs, so it would be hard to come to a consensus on how safe is safe enough for a system.
2. I don't think that there is a systematic way to enumerate *every* bad thing that could happen to a program, because there is no sure way to know one has found each and every potential vulnerability. The best one could do would be to assess each asset in the process on a step by step basis and determine whether the asset is vulnerable at each given point. However, even then, unforeseen attacks could remain undiscovered, and the best one could hope for would be detection and correction after the breach.
3. The defender has to think of every possible vulnerability and potential security attack the attacker could make. Meanwhile, the attacker only has to detect one vulnerability to attack a system.
4. I entirely agree with Morris and Chang. Of course, steps have and should be taken to protect data as well as possible, but the only one hundred percent safe way to eliminate security breaches to digital data is to not make it digital at all. There will consistently be an attack that can't be foreseen, so each time a user makes his or her resource or data

digital, he or she consents to the potential breach of its privacy. Though we can hope to minimize risk, we cannot eliminate attacks altogether.

5. Security implies limitations of exploitation and as such also limits efficiency and capability. Increased capability and efficiency often necessarily poses vulnerabilities and lower security standards. Security takes time, complexity, and careful rationing, and therefore can and often does impede functionality, usability, efficiency, time-to-market, and simplicity of systems or programs.

LECTURE 3

1. Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
2. I agree that software security is about managing risk, because risk cannot entirely be eliminated. If security could be mastered to perfection, an unlikely circumstance at best, of course, software security would be about more than risk management. However, because it cannot, managing risk is the best one can hope for. My main concern though is that each person's idea of risk may differ so generalizing for a shared system would be difficult and a compromise of security standards.
3. I accept the risk of data mining, because the promise of convenience, such as Autofill, password memory, etc., outweigh the vulnerability of the data being gleaned in my opinion. I avoid the risk of illegal music downloading, because the accidental downloading of a virus is a risk I don't want to take though it may provide me free music. I mitigate the risk of unauthorized users using my PC by applying a password lock to my laptop. I transfer the risk of viruses by installing Norton Anti Virus and assigning it responsibility for virus security threats.
4. Annualized Loss Expectancy (ALE) works well as a risk management tool if you assume that the predicted likelihoods and costs are correct. However, the likelihood is not guaranteed. Since it is only an estimate, unforeseen events could make an otherwise rare event more likely. Additionally, ALE only foresees financial cost, often ignoring psychological costs, which must be considered to accurately manage risk.
5. Some factors relevant to rational risk assessment are financial loss due to a security risk or psychological trauma due to a security risk. On the other hand, compromised efficiency or capability are important to consider in deciding which risks are worth accepting.

LECTURE 4

1. The list on Slide 2 covers what we try to protect with security, while the list on Slide 3 covers how we try to protect those things.
2. Confidentiality is most important to me, since I enter important, confidential information, such as my credit card number in online transactions. Because much of my shopping is done online, I do not want anyone to be able to read the financial information I make available on the Internet.
3. You can group data by how sensitive it is, so that the most sensitive and protection-necessary data is in one group which receives high security, and each of the less sensitive data groups receive lower security, because there is lower risk to them.
4. New members added to an organization would cause a change in authorizations. Additionally, promotions would lead to an upgrade in individuals' authorizations. Changes in departments within an organization would also change the access control and thus authorizations of an organization.
5. A threat to the reliability of a machine is also a threat to security, because malicious attacks can cause a ridiculous loss of efficiency of a machine. If we rely on a machine to

do its job, and it consistently is unable to do it due to a malicious agent, security has been breached.

6. Online banking is one area in which authentication and non-repudiation would be necessary to prevent identity theft or forgery.

LECTURE 5

1. A cell phone network would probably need to protect the identity of a phone owner, keep third parties away from secure personal data kept on a phone, and keep resources of the phone available and free of attacks. A military database would probably want to keep any and all top secret plans unable to be read by unauthorized users.
2. A policy is a system specific set of rules to accomplish metapolicy. Metapolicy can be vague, but metapolicy is specific and not open to multiple interpretations. You can have more than one policy for a metapolicy. Policy is specific and enforceable while metapolicy isn't.
3. One possible rule is that only a student is allowed to read his or her grades and must authenticate with his or her name and a private password. Another would be that only faculty can modify or write to a student's grade, and thus must authenticate with his or her name and a password known only to faculty. Another policy rule could be that a student is automatically logged out of his or her account after a certain amount of time to prevent people from hanging around and looking at someone else's secure grades.
4. They might conflict, since people care about different aspects of security and efficiency. For instance, in data mining, some people may find the auto suggestions made possible by data mining beneficial, particularly vendor companies. However, the consumer may be uncomfortable with these companies knowing so much about their otherwise private cyber behavior.
5. The university would like to protect the confidentiality of students' social security numbers as much as possible.
6. Because security often undermines efficiency, policy rules can seem not only arbitrary, but crippling. However, the bigger picture of risk makes it easier to accept the value of what is being protected over the value of achieving system goals. For this reason, metapolicy allows us to understand and appreciate policy.

LECTURE 6

1. Military security relies highly on preventing the leakage of confidential or top secret information, so it is necessary to establish confidentiality so that only authorized users have access to secure information. Integrity also exists, because you wouldn't want a general to write what he knows that a footsoldier shouldn't know by accident into a document. Additionally, availability plays a role, because military plans, for instance, must be available exactly when needed.
2. We are protecting secure data from potential spies or unauthorized users looking to gain access to secure data.
3. Our solution to the MLS experiment at this point only prevents people in the wrong fields or lower authority from reading highly secure and group specific information but says nothing about rights to modify/write to documents or keep said documents available.
4. The labels have two parts. The first is the level of authority the user has which must be the same as or higher than the security level of the object he or she is trying to write to. The second part of the label is the category of the subject, which must meet the categories of objects.
5. I think we are not concerned with how those labels got there, because in reality they would probably require an authentication process prior to the problem we are solving. A

private password system or something along those lines could grant authority, and authority would likely be granted by someone even higher in authority.

6. From least sensitive to most sensitive, we have (1) The cafeteria is serving chopped beef on toast today, (2) The baseball softball team has a game tomorrow, (3) Colonel Jones just got a raise, (4) Col. Smith didn't get a raise, (5) The British have broken the German Enigma, and (6) The Normandy Invasion is scheduled for June 6.
7. My labels would be (1) General Information, (2) Military Personnel Information, (3, 4) Financial Information, (5) Confidential Data, and (6) Top Secret Data.
8. You want as little data known as necessary for someone to complete his or her job for highest possible security.

LECTURE 7

1. Labels can be affixed to humans through authentication, such as whether or not someone knows an authority level password. Additionally, a their names could be kept in a different file depending on their authority level.
2. Labels on documents indicate the sensitivity of contained information, while labels on humans indicate the classes of information that person is authorized to access.
3. I think that documents would be files, programs, or resources needing protection, while humans would be users or agents trying to access those files, programs, or resources.
4. The Principle of Least Privilege makes sense, because it balances efficiency with strong security. A subject has enough efficiency but not too much information.
5. The first one makes sense because the human has a higher security than the sensitivity, and he or she is part of crypto which is the category of sensitivity, too. The second one makes sense, because the human has lower security than the sensitivity of the information. The last one makes sense because the human has higher security than the information, and no category is required to read the information.

LECTURE 8

1. I think that the use of subjects and objects allows a broader definition of security, and pertains more closely to technical definitions. I think actions are necessary, because writing and reading have different rules.
2. The level of one could be larger than the other, but the subset could occur in reverse, in which case neither security label is greater than or equal to either. For instance, one subject could be (Top Secret, {}), and the object could be (Secret, {Crypto}).
3. The level of one could be larger than the other, but the subset could occur in reverse, in which case neither security label is greater than or equal to either. For instance, one subject could be (Top Secret, {}), and the object could be (Secret, {Crypto}).
4. The label of one object would be greater than the second, but the first would also be a subset of the second.
5. A subject must dominate an object to be able to read to it.
6. There may be and often are more rules and factors than just the "read down" rule to decide if someone is authorized to read an object.

LECTURE 9

1. It is not enough, because it only maintains confidentiality and governs reading of an object by a subject. In order to protect integrity of an object, we must create a rule to govern the writing of information to an object by a subject.
2. We don't want confidential information leaked intentionally or otherwise to lower levels.
3. While human beings can be trusted if in high ranks, programs are simply running on behalf of a trusted user. However, these programs could have malicious logic in them

which causes them to leak information without the user’s knowledge, intention, or permission. This would be far more dangerous.

4. An object’s label must dominate a subject’s level in order for the subject to write to that object.
5. The object’s label must be equal to the subject’s label.
6. We can give the General some lower level private (Unclassified) identity from which he or she can communicate with the private without leaking information.
7. We have to make special rules for integrity protection.

LECTURE 10

1. If you downgrade an object, you need to carefully assess the content of that object. Raising the level of an object should be okay. On the other hand, a subject can’t upgrade without constraint, and can only downgrade if it is stateless or carries no residual information from its higher status.
2. Sometimes, labels will have to change as the organization of authority changes.
3. Lowering the level of an object is dangerous, because if confidential information is still in the object, and low security level subjects are able to access the object, then the subject has unauthorized access to confidential information.
4. The downgrade of an object is alright if the content of that object is assessed so that confidential information is no longer in it.

LECTURE 11

1. Give the subjects read access to files, but don’t give the subjects write access. In order to do this, the subjects should have high levels and the objects should have low levels.
2. You usually have thousands of subjects and thousands of objects, but most of the matrix spots will be empty. Also with Simple Security and *-Property, you can compute accesses on the fly without a matrix.

LECTURE 12

1. $$\begin{tikzcd}
(H, \{A\}) & (H, \{\}) \arrow[l] \\
(L, \{A\}) \arrow[u] & \\
(L, \{\}) \arrow[u] \arrow[uur] &
\end{tikzcd}$$
2. For lowest upper bound, find an element such that all elements are less than it in the lattice. For greatest lower bound, find an element less than all other elements in the lattice.
3. It follows the write up policy, since information can only be written to higher levels. The Simple Security policy requires that the user’s level dominates the object level, so information can only flow through direct access and information always flows upwards.

LECTURE 13

1. Information can go from L to H, but not from H to L, because reading information requires that the level of the subject is higher than the level of the object it is reading to, while writing can only happen to higher levels.
2. The READ satisfies Simple Security in BLP, since you can only read down; that is, a subject level must dominate the level of the object it is reading from. The WRITE

satisfies *-Property in BLP, since you can only write up; that is the subject level must be dominated by the level of the object it is writing to.

3. The CREATE satisfies *-Property in BLP, since creating object O is similar to writing, and if O is created at the subject's level, it follows that the level of the subject is less than or equal to the level of the object, as dictated by BLP. The DESTROY satisfies *-Property, because destroying object O is a modification, and the level of the object destroyed or modified dominates the level of the subject destroying or modifying as dictated by *-Property in BLP.
4. The high level subject would be able to signal at least one bit of information to the low level subject, causing downward flow. In a loop even one bit could become more information and cause the covert channel to succeed.
5. It wouldn't have the information to behave differently based on what he is seeing from the object. It would be impossible for it to vary its behavior.
6. No, the files contain the same information.
7. The DESTROY exists to delete the file since it has a higher level than the subject.
8. SH does different things because it has transmitted a different bit, 0 vs. 1. He didn't try to create the object on the right, but did on the left.
9. One bit then flows from the high level subject to the low level subject, violating security, and causing downward information flow. Though it's only one bit a system could turn that into significant amounts of information.

LECTURE 14

1. The flow has to be between subjects within the system.
2. No, because SL will not be able to read the data from F0 regardless, assuming F0 is a higher level than SL. However, if SH is able to control the error message sent to SL for the read, it could be a covert channel, since a bit will be passed from high level to low level.
3. If the high level subject controls the error message sent to the lower level subject, the low level subject could receive a bit to information. It is a storage covert channel, since the low level status learns the status of the object with the illegal bit it is passed.
4. The data from the clock dictates whether p has completed the task and how long it is taking p to complete the task, and q can use that to get information about process p. This is a covert timing channel.
5. Process Q gets a bit of information from whether the disk was closer to 140 or 160, revealed by the order in which service requests were processed. This covert channel has aspects of both timing and storage covert channels.
6. The value of l is influenced by the value of h, so information is implicitly passed from high level to low level. Predictably, this is an implicit channel, and can be overcome by sophisticated language-based information flow checks to prevent this from happening.
7. A termination channel might have low bandwidth, because a process would have to wait for the other process to terminate to get information about it.
8. The low level process has to be able to sense how much energy is consumed by a high level object, and the high level subject has to be able to modify that information.
9. I think a mobile device would be susceptible to power channels, since it is not as difficult to see how much power is being taken by an application.

LECTURE 15

1. In real life, cover channels can operate at thousands of bits per second, revealing a significant amount of confidential information to unauthorized agents.

2. There are too any potential covert channels to eliminate every single one, so it's better to manage risks than try to eliminate all potential covert channels. You want to at least be able to detect the channels.
3. You could eliminate it by changing the system's implementation. You could introduce noise into the channel so that the channel had lower bandwidth. You can also use intrusion detection to monitor the channel for usage patterns showing that someone is exploiting it.
4. A storage covert channel would exist if a high level subject varied error messages to low level subjects depending on the status of the object.
5. The sender would modify the error message, and the receiver would use the error message to glean information from the sender about a high level object.

LECTURE 16

1. The CREATE operation modifies the existence of the file by creating it instead of referencing the file. Any information gleaned is inferred, not told, by the operation.
2. For that attribute, one process is modifying and the other can reference it, which is the circumstance of a covert channel.
3. No, because the information in a column is associated with one operation, not with one attribute. The attribute access patterns govern whether there is a covert channel or not.
4. You go through the trouble of creating an SRMM table, because even if there is not a way to eliminate all covert channels, once you detect them, you can deal with them accordingly. It is important to deal with potential covert channels, as they pose serious threats to the security of confidential data.