Colin Murray

UTEID: Cdm2697

UTCS-username: Tashar

Email: murray.colin43@gmail.com

CS361 Questions: Week 1

Lecture 1

1. What uses of the term "security" are relevant to your everyday life?
   Computer security, personal security, network security
2. What do these have in common?
   All protect valuable personal assets against potential threats.
3. Have you been a victim of lax security?
   I lost several dollars in quarters once due to neglecting to fully lock my car. The power locks no longer function so at times I felt the unlikely-ness of getting robbed justified not checking every door to see if it were locked properly.
4. What is the likelihood that your laptop is infected? How did you decide?
   Having had this computer since October and already having been infected with a virus that I was able to remove successfully, it is not unlikely that a subtle infection exists that chooses not to reveal itself.
5. What security measures do you employ on your laptop?
   I run antivirus, use Malwarebytes to remove any malware and use Spybot to look for spyware and other possible threats. I also have it password protected and have Prey installed in the event the computer is stolen which will hopefully aid in tracking it down or at least locking the thief out.
6. Do you think they are probably effective?
   They're effective enough for my uses, but are certainly not perfect and I still must practice caution to avoid many threats.
7. Consider the quote from the FBI official on slide 10. Do you think it over-states the case? Justify your answer.
   Very much so, his use of the term "access" is rather vague and could mean a number of things. Furthermore while perfect security may not be possible there are ways to significantly mitigate the degree of access and damage attackers can do even if they circumvent one security mechanism. This is not to say the threats are not real and that mistakes won't lead to large scale and dangerous breaches, but to suggest that a cyber-attacker could access "virtually any computer system" is patently false.
8. What is the Importance in learning about computer security?

   As we move into an increasingly computer dependent society where many sensitive tasks are done electronically it is extremely important that we can protect ourselves from cyber-threats. Strong understanding of computer security can enhance personal and interpersonal security, workplace and business security and all aspects of cyber-security.

Lecture 2

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

   Some well thought out security policies or standards may be complex enough to be poorly implemented. For example there are cases where companies implement their own implementation of well-established crypto algorithms like RSA or DSA but neglect perhaps a subtle aspect (due to a programmer's lack of understanding or simply accidental code bug).

2. Is there a systematic way to enumerate the "bad things" that might happen to a program? Why or why not?
   Not viably
3. Explain the asymmetry between the defender and attacker in security.
   The defender must prepare and defend against all possible attack points which may not even be known or obvious. An attacker must only find one and there can be many attackers trying.
4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?
   In a perfectly extreme sense they are correct. As Stuxnet has demonstrated, even keeping your computer on a system with no internet or even local network access the potential of infection can still exist (in this case over USB drives). For normal use there is no way to be perfectly secure.
5. Explain the statement on slide 8 that a tradeoff is typically required.
   Rigorous security often means strict mechanisms must be in place to prevent intrusion or leakage of data. Many browsers will remember your authentication and form data for websites for convenience at the risk that someone other than yourself might gain access to your computer and login on your behalf.

Lecture 3

1. Define "risk"?
   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, nearly all security built into software is there to prevent unintended or malicious access to data on the hard drive, in memory or across the network.
3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?
   I accept the risk that I use the same few passwords for all my accounts. A unique password for every account would not be viable even if it is more secure. I avoid posting sensitive information about myself in unsecure mediums or public forms like Facebook keeping in mind that once something is on the internet there is very little chance of permanently deleting it. I mitigate the risk of computer infection by running anti-virus, anti-malware and anti-spyware tools which hopefully will detect a majority of infections.
4. Evaluate annualized loss expectancy as a risk management tool.
   While perhaps ALE is a good way to assess the damage potential of similarly probable threats it fails to fairly demonstrate the substantial risk very high damage and low probability threats pose compared to lower damage but higher probably threats.
5. List some factors relevant to rational risk assessment.
   Technical, economic, psychological factors and the relative probability risks

Lecture 4

1) Explain the key distinction between the lists on slides 2 and 3.
   Slide 2 lists some goals and fundamental properties of computer security. Slide 3 lists mechanisms by which these properties achieved in real computer systems.
2) Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.
   Availability is most important. Most things I use the computer for are rather mundane and would be of no consequence to me if some other person learned about what I was doing or tampered with it. All 3 factors are important but if the user experience is poor than the security advantages may be outweighed.
3) What does it mean "to group and categorize data"?
   Not all data is equally sensitive. Data which cannot be leaked or replaced should be categorized in a higher level of security than public or trivial information that.
4) Why might authorizations change over time?
   Someone who is promoted high enough to be qualified for a level of security must be granted access or someone who transfers away from a position with authorization must have his access revoked if no longer qualified.
5) Some of the availability questions seem to relate more to reliability than to security. How are the two related?
   Poor security can leave a system open to infection which may impact its reliability. Like-wise if a system is unreliable (like a door that doesn't always shut properly) it may compromise security.
6) In what contexts would authentication and non-repudiation be considered important?
   In situations where your action should be irrevocable and their implications must be tied to you. If you were to take money from an ATM the ATM must not only be pretty sure that you are indeed the person accessing your account through authentication, but also prevent the user from somehow claiming a withdrawal never occurred once the money has been dispensed through non-repudiation.

Lecture 5

1) Describe a possible metapolicy for a cell phone network? A military database?
   A phone network should not allow unknown individuals listen-in on their customer's wireless communications. A military database must not leak confidential information to those who lack the proper clearance.
2) Why do you need a policy if you have a metapolicy?
   A metapolicy can be too general to thoroughly guide its own enforcement and it may have multiple interpretations. A set of policies provide specific and enforceable guidelines to the system user/developer and make the interpretation explicit.
3) Give three possible rules within a policy concerning students' academic records.
   An official grade can only be changed if authorized by the dean of the college. A student must present a photo id in person to request their own transcript. Academic records must be encrypted and hashed for integrity when stored on the school database.
4) Could stakeholders' interest conflict in a policy? Give an example.
   Yes, a company might want to provide security of user information by including a captcha in their login form so a bot cannot brute-force user passwords however this would add increased inconvenience to users who want to login.

5) Explain the statement: “If you don’t understand the metapolicy, it becomes difficult to justify and evaluate the policy.”
   A policy may seem arbitrary or down-right strange without understanding the reasoning behind it (the metapolicy). Having to take off your shoes in an airport security checkpoint would seem very odd if you didn’t know the purpose of these checkpoints.

Lecture 6

1) Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?
   The confidentiality of military information means the difference between life and death of many individuals if large military plans leak out. Integrity is certainly important in order to prevent temperament of important military information but is less of a risk if the information is confidential and its existence may be unknown to begin with. It’s harder to actively alter something that you cannot see nor be certain of it even being there. Availability is also important in that information must be accessible in order to effectively mobilize military operations. For example say a commander isn’t able to see his confidential battle plan until the window of opportunity has passed due to some availability outage.
2) Describe the major threat in our MLS thought experiment.
   The confidentiality of information. That no person not authorized to view a piece of information can access it.
3) Why would you think the proviso is there?
   The main goal of this thought experiment is to only address the major threat (confidentiality) and does not address risks related to integrity or availability. Without these risks being addressed this thought experiment has serious flaws related to integrity or availability that should be kept in mind.
4) Explain the form of the labels we’re using.
   They are a linearly ordered set of security sensitivity: Unclassified, confidential, secret, Top Secret with unclassified of the lowest level of security and top secret being the highest. There are also “need-to-know” categories associated with the data such as: Crypto, Nuclear, Janitorial,ect. Information can only be accessed if an individual has both the proper sensitivity level clearance and need-to-know clearance to view the information.
5) Why do you suppose we’re not concerned with how the labels get there?
   For the purpose of demonstration in this thought experiment it would overcomplicate things to explain an in depth reasoning why a piece of information should be secret and not top secret or be in the category {crypto} rather than {crypto, nuclear}. These decisions are made on a very circumstantial basis and likely need a good deal of context to justify the label they receive.
6) Rank the facts listed on slide 6 by sensitivity.
   1. Unclassified
   2. Top secret
   3. Unclassified
   4. Confidential
   5. Confidential
   6. Top secret
7) Invent labels for documents containing each of those facts.

1. Recreation
2. Military operation
3. Culinary
4. Payroll
5. Payroll
6. Current events

8) Justify the rules for "mixed" documents.
   A document that contains unclassified and top secret information must require top secret clearance to view rather than top secret or unclassified clearance otherwise intermixing information of varying confidentiality would present serious security risks. Likewise information grouped into multiple categories must require clearance for both categories, not one or the other. Otherwise someone with only nuclear clearance could learn crypto information that he is not privileged enough to view by looking at {nuclear, crypto} documents.

Lecture 7

1) Document labels are stamped on the outside. How are "labels" affixed to humans?
   Each individuals identity is affixed a hierarchical security level indicating their degree of trustworthiness and a set of "need-to-know" categories based on the domains of interest in which they operate. Some independent official or system must verify the individual's identity and look up their sensitivity "label" before granting them access to information.
2) Explain the difference in semantics of labels for documents and labels for humans.
   Documents indicate the sensitivity of the contained information; human "labels" indicate classes of information that person is authorized to access.
3) In the context of computers what do you think are the analogues of documents? Of humans?
   Data would be analogous to documents and running processes (and perhaps by transitivity the computer users potentially commanding them) are the analogous to the humans.
4) Explain why the Principle of Lease Privilege makes sense.
   Giving an individual access that more information than necessary at the time provides more potential for sensitive information to leak out. The less avenues for information to leak the tighter the security of the system and people can always be granted the proper access if their "need-to-know" changes.
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.
   a. Given a clearance of (Secret: {crypto}) the individual should be able to access any information of sensitivity Secret or below in the Crypto category. Given this he can indeed access a (Confidential: {crypto}) document.
   b. Given the clearance level of (Secret: {Crypto, Nuclear}) an individual could not access a document labeled (Top Secret: {crypto}) because he lacks Top Secret permission.
   c. Given the clearance level of (Secret: {nuclear}) an individual view a document labeled (unclassified: {}) because his security level is higher than the documents and the "need-to-know" category of the document is a subset of the individual's "need-to-know" clearance.

Lecture 8

1) Why do you think we introduced the vocabulary terms: objects, subjects, actions?
   These terms are often used when describing any security policy in a general sense as they represent basic elements. We can now describe aspects of the MLS example or future examples with these vocabulary terms.
2) Prove that dominates is a partial order (reflexive, transitive, anti-symmetric).

Given X1 = (L1, S1) and X2 = (L2, S2) and x3 = (L3, S3)

If x1 >= x2 (reflexive) than L1 >= L2 and S2 $\subseteq$ S1 which holds true since subsets obey the rule of reflexivity (i.e. if s1 >= s2, s2 must be a subset of s1).

If x1 >= x2 and x2 >= X3 then by transitivity since L1 >= L2 and S2 $\subseteq$ S1 and that L2 >= L3 and S3 $\subseteq$ S2 we can see that L1 >= L3 and S3 $\subseteq$ S1 by transitivity. This holds true since subsets also obey transitivity (i.e. if s1 >= s2 >= s3, s2 must be a subset of s1 and s3 must be a subset of s2).

If x1 >= x2 and x2 >= x1 we see that the following must be true: L1 >= L2 and L2 >= L1 which by the anti-symmetric property means L1 = L2. Further this must also be true S2 $\subseteq$ S1 and S1 $\subseteq$ S2. Since a set can be a subset of itself this implies that S2 = S1. Given all of this we see that the properties for partial order (reflexivity, transitivity and anti-symmetry) all hold true for The Dominates Relation.

3) Show that dominates is not a total order
   The claim here is that dominates IS a total order.
   Given 2 individuals with clearances x1 = (Secret: {crypto, janitorial}) and x2 = (confidential: {nuclear}) where Secret > confidential from a security perspective.
   L1 = secret L2 = confidential
   S1 = {crypto, janitorial} S2 = {nuclear}
   Suppose we think x1 dominates x2. This means that L1 >= L2 (which holds true in this case), however S2 is not a subset of S1. Thus x1 does not dominate x2.
   Now suppose we think x2 dominates x1. This means that L2 >= L1 which is false in this example. Additionally S1 is not a subset of S2.

   Thus in this counter-example dominates is not a total order since there exists an arrangement where neither X1 >= X2 nor X2 >= X1.

4) What would have to be true for two labels to dominate each other?
   They would have to be the same (Anti-symmetry).
5) State informally what the Simple Security Property says.
   It means for a subject to read an object it must have clearance to a hierarchal sensitivity level greater than or equal to the level of the object AND must possess clearance for at least the same security categories as the object specifies.
6) Explain why it's "only if" and not "if and only if."
   There could potentially be other security constraints that must also be considered before granting access to the subject than just the Simple Security Policy.

Lecture 9

1) Why isn't Simple Security enough to ensure confidentiality?
   A subject might read an object that the subject possesses the sufficient security level for and subsequently writes it somewhere that contains information below that object's security level. This effectively grants any subject with that lower security level access to information they shouldn't be able to view.
2) Why do we need constraints on write access?
   Simple security does not prevent a subject with privileged access from reading information and subsequently writing it to a location of lower security level.
3) What is it about computers, as opposed to human beings, that makes that particularly important?
   While people may be trusted to not write confidential information places that would be inappropriate however computers need rules in place to prevent malicious programs from writing where they shouldn't.

4) State informally what the *-Property says.
   A subject may only write an object that the subject to a security level equal to or higher than his own.
5) What must be true for a subject to have both read and write access to an object?
   The object and the subject must have the same security level.
6) How could we deal with the problem that the General (top secret) can't send orders to the private (Unclassified)?
   The general could log out of his top secret account and log into an unclassified account instead. Since the general should be trustworthy enough to not leak any top secret information to the troops that they shouldn't have access to it is acceptable for him to have 2 classification levels on 2 different accounts. He uses his unclassified account to communicate with his troops.
7) Isn't it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.
   This is a problem that exists with simple security and the *-property because they are primarily concerned with confidentiality and this is an Integrity issue. The inclusion of some sort of integrity protection could prevent this from happening.

Lecture 10

1) Evaluate changing a subject's level (up or down) in light of weak tranquility.
   Subjects may change security levels if it is done in a way that doesn't violate the spirit of the security of the system. A subject may be risen up if they are deemed trustworthy enough to handle more privileged information. The subject may be lowered as long as it can be asserted that no residual confidential objects at his current level remain with him.
2) Why not just use strong tranquility all the time?
   Strong tranquility would prohibit subjects from ever moving up in the ranks and disallow them from ever being demoted and a single individual could not communicate to his or her subordinates using 2 accounts of differing security level.

. This is certainly problematic from a military perspective but there might also be reason to promote or demote a process in a computer system as well and a single individual could not communicate to his or her subordinates

3) Explain why lowering the level of an object may be dangerous.
The object must be examined carefully to make sure it doesn't contain any information what-so-ever that should remain at its current classification.
4) Explain what conditions must hold for a downgrade (lowering object level) to be secure.
The demotion must not violate the "spirit" of the system's security policy and likely must undergo analysis from some downgrader system to verify that the demotion is acceptable.

Lecture 11

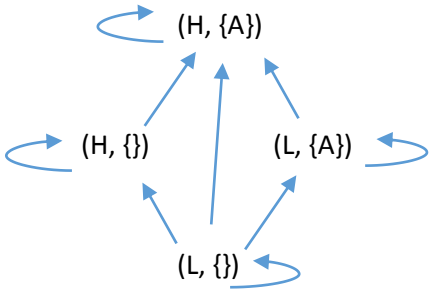
1. Suppose you wanted to build a (library) system in which all subjects had read access to all files, but write access to none of them. What levels could you give to subjects and objects?
All subjects would be given an access level higher than all objects. This way any subject can read any object but will be forbidden to write to any object (since the *-property prevents writes to lower security levels).

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

Because the amount of subject and objects in a BLP system could be in the thousands or more it would be impractical to construct an access control matrix, especially given the probable number of empty subject/object pairs with numbers that large.

Lecture 12

1. Suppose you had hierarchal levels L, H with L < H, but only had one category A. Draw a 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?
If you take any subset of a set of labels you can find the least upper bound and greatest lower bound. The set of labels under dominates allows the construction of a lattice which allows the easy discovery of the LUB and GLB for any two labels.
3. Explain why upward flow in the lattice is really the metapolicy for BLP?
BLP's metapolicy says that sensitive information should not flow "down" in the system, rather information should only flow upward. The lattice is a good way of visualizing this metapolicy. If

all labels in the lattice show an upward flow (which is the primary goal of the lattice) system conforms to the BLP metapolicy since the flow of information indicated by the lattice goes upward.

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.
   BLP specifies that if one label has a greater or equal security level than another it dominates that label. It also says that information cannot be read from a security level higher than the current label's security level (by the simple security property) and that information can only be written somewhere with a label higher or equal to the current label (by the *-principal). There are two ways then that information can flow. It can be read from a level that is dominated by the current level or it can be written to a level that is dominated by the current level. With these in mind sensitive information may only flow upward in a BLP system.
2. Argue that the READ and WRITE operations given satisfy BLP.
   Information cannot be read from a security level higher than the current label's security level, that is that a subject can only read from an object if it dominates the security level of the object (by the simple security property). This implementation of READ would then indeed satisfy BLP.
   Information can only be written somewhere with a label higher or equal to the current label, that is a subject can only write an object that to a security level that dominates the subject (by the *-principal).
3. Argue that the CREATE and DESTROY operations given satisfy BLP
   Objects can only be created at the same level as the subject. Since the subject cannot create any sensitive objects to any lower security level there's no risk of information flowing downward.
   Since a subject with write access could just as easily mangle to uselessness an object that the subject can logically write to according to BLP, it is no breach of security to also allow the subject to destroy this information. It could be argued that a subject could destroy anything and it would still be permitted by the BLP metapolicy since the flow of information never moves downward no matter what object gets destroyed.
4. What has to be true for the covert channel on slide 5 to work?
   For the covert channel to work the high level subject must decide whether or not to create an object (in this case F0). For this to work the low level subject and high level subject must somehow coordinate each iteration of the process in order to read the pass the right bit of information to the low level subject at the right time to make a coherent message.
5. Why is the DESTORY statement there?
   It is there so the process can be repeated with the same object an arbitrary amount of times.
6. Are the contents of any files different in the two paths?
   No, in both paths a 1 is written into F0 successfully.
7. Why does the SL do the same thing in both cases? Must it?
   Until the value is read any additional operations by SL done in one column but not the other could potentially lead to corrupted transmission. It might not be completely necessary to result in a still valid transmission (like reading before the write), but the all fundamental operations of SL in slide 5 must be performed at some point in both columns for it to work properly.
8. Why does the SH do different things? Must it?

Yes, it must. If it did the same thing every time there would be no difference between column 1 and column 2 and thus SL wouldn't be able to gain any information from SH.

9. Justify the statement on slide 7 that begins: "If SL ever sees…"
   Even if it's only one single occurrence that SL happened to see varying results based on something SH did, information was successfully passed through a covert channel. If this could be repeated with consistency and coordination between SL and SH a large amount of data could be passed.

Lecture 14

1. Explain why "two human users talking over coffee is not a covert channel."
   A covert channel is a flow of information in a system. 2 people talking over coffee would not constitute a system in this sense.
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)

No, because either F0 is writable by SH or F0 readable by SL due to simple security and the *-principal. Thus if F0 is the same level as SH, both of SL's reads will fail in either case and if F0 is the same level as SL both of SH's writes will fail in either case. No data can be transmitted.

3. Where does the bit of information transmitted "reside" in Covert Channel #1?
   It resides in the existence or non-existence of files in a directory (in this example one file named 0bit transmits 0 and another file name 1bit transmits 1).
4. In Covert Channel #2?
   It resides in the time difference between when the receiving process (the one being transmitted to) gave relinquished the CPU and when it got it back. The 0 or 1 state of the bit depends on if the communicating process relinquishes the CPU immediately or waits until it's time t expires. The receiving process can view this bit by checking the time before and after it relinquished the CPU.
5. In Covert Channel #3?
   The bit resides in the position of the read head of some hard disk. It is placed to the right of two sequential sectors to transmit one state of the bit and placed to the left to transmit the other state of the bit. Depending on the order in which the receiving process reads the 2 sectors it can decipher which bit was sent.
6. In Covert Channel #4?
   The bit of information is held in the state of a variable that depends exclusively on the state of another. The control flow of the program can possibly be manipulated so the variable ends up in one of the two states (communicating a 0 or a 1 depending on which).
7. Why might a termination channel have low bandwidth?
   The non-termination of the computation may result in it continuing for some time. If this means it never terminates than only one bit of information can ever be communicated, but if a time

limit is set the bandwith is both dependent on that and how long it takes to restart the computation.

8. What would have to be true to implement a power channel?
   The energy requirements of one operation must be higher than the energy requirements of another. The variable energy requirements communicate information depending on which operation the communicating system in the covert channel decides upon.
9. For what sort of devices might power channels arise?
   Computer chips may exhaust more power calculating one operation than another. In particular smart cards consume more energy setting a 1 bit than a 0 which could leak the secret key.

Lecture 15

1. Explain why covert channels, while appearing to have such a low bandwidth, can potentially be very serious threats.
   Real processors operate very quickly so the amount of information leaked may be relatively very slow compared to the computer's speed but still allow for significant amounts of information to be passed.
2. Why would it be infeasible to eliminate every potential covert channel?
   Realistic systems are often times much too complex to impose the level of restrictions necessary in order to eliminate all covert channels.
3. If detected, how could one respond appropriately to a covert channel?
   Changing the system implementation, reduce the bandwidth by introducing noise or lastly monitor the channel to check if it is being exploited maliciously.
4. Describe a scenario in which a covert storage channel exists.
   If two processes exist in a system where one can view the changes in a file-system and one can modify the file system, the modifying process can communicate information to the viewing process by somehow altering a file in a viewable way.
5. Describe how this covert storage channel can be utilized by the sender and receiver.
   If one process p2 is able to see the names of all files in a directory but cannot read them and another process p1 can alter the files in the directory some way, say by creating a new one called bit1 or bit0 and deleting it after sufficient time for transmission has passed, then p1 can communicate an arbitrary amount of data to p2.

Lecture 16

1. Why wouldn't the "create" operation have an R in the SRMM for the "file existence" attribute?
   The create operation does not inform the system that a file of the same name already existed or not, it simply does nothing if there exists a file already. If create somehow communicated this information back to the system (say by returning an error) then an R would be applicable for file existence. In the implementation on slide 4 this is not the case so no R is applicable for file existence on create.
2. Why does an R and M in the same row of an SRMM table indicate a potential channel?
   For that attribute there is a mechanism where one subject can modify it and one subject can reference it which is an important factor in the existence of covert channels (though it does not necessarily mean that one is there).

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?
   Not necessarily, the R and M for the operation specified by the column bust be in the same row for this to be true (meaning the possibility of a covert channel existing is still solely dependent on the row). The only way to communicate information via a covert channel is determinant on whether the operation or set of operations (column/s) can read and modify a *particular* attribute (row).

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

   One might use BLP to control the standard overt channels and follow up using the SRMM technique to identify the existence of any covert channels that would compromise the metapolicy by leaving an avenue where information might leak. With knowledge of these covert channels they can be properly address. BLP is simply not enough alone to be completely secure.