Brian Chow (brianj.chow@yahoo.com)
EID/CS login: bc23784
CS 361 (90155)
For 06/12/14

CS361 Questions: Week 1

Lecture 1

1) What uses of the term “security” are relevant to your everyday life?
    1. Using passwords to log in to various sites/my computer, remembering to lock the front door when I leave, making sure a website I use to handle sensitive information is legitimate and hasn't been compromised.
2) What do these have in common?
    1. The common aspects of computer security, namely confidentiality, integrity, availability, and authentication (non-repudiation for financial transactions).
3) Have you been a victim of lax security?
    1. Not in recent memory. The last thing that happened was a junk email account I had getting hijacked several years ago due to one of the many password breaches at Yahoo.
4) What is the likelihood that your laptop is infected? How did you decide?
    1. Low. Pop-up blockers prevent me from accidentally clicking on a rogue website, and I periodically boot into safe mode and scan the computer using some tool (usually Malwarebytes). Safe browsing habits and not downloading questionable material help.
5) What security measures do you employ on your laptop?
    1. Antivirus, pop-up blockers, anti-tracking extensions (browsing), programs such as Malwarebytes
6) Do you think they are probably effective?
    1. Combined with safe/cautious usage habits and periodic scans/cleans, yes.
7) Consider the quote from the FBI official on slide 10. Do you think it overstates the case? Justify your answer.
    1. While it does sound overly-dramatic, most likely to grab peoples' attention, it is possible that an attacker could cause widespread disruption in the US, whether by compromising a nuclear plant (see Stuxnet) or interrupting large portions of critical infrastructure (namely electricity).
8) What is the importance in learning about computer security?
    1. Given society's heavy reliance upon computers to perform a wide variety of important tasks, it is paramount that they be protected and safeguarded in order to guarantee the safety of the resources they control and their continued functionality.

Lecture 2

1) Consider the five reasons given why security is hard. Can you think of other factors?
    1. The cost of adapting security feature(s) may be more than the company is willing to spend.
2) Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not?
    1. Generally, no. Most useful programs are far too large to consider this feasible (i.e., without

spending large amounts of time and/or money). Adding too many security checks could hamper the performance of the program, and there is always the issue of new vulnerabilities being found.

3) Explain the asymmetry between the defender and attacker in security.
    1. The attacker only has to find one vulnerability in the program to potentially wreak havoc. The defender must determine and protect all vulnerabilities that are present.
4) Examine the quotes from Morris and Chang. Do you agree? Why or why not?
    1. Yes. Computers and their programs are far too large and complex to be able to effectively protect against any and all attacks.
5) Explain the statement on slide 8 that a tradeoff is typically required.
    1. The program and its design must strike a balance between usability/efficiency/etc and being secure. For instance, diverting too many resources to security could make for a very secure program but potentially at the cost of speed, resource usage, and simplicity.

Lecture 3

1) Define “risk”.
    1. Risk is “the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability”.
2) Do you agree that software security is about managing risk?
    1. Yes (but not only about managing risk). Individual risks should be analysed for their potential consequences, with higher-priority risks taking precedence over those of lesser priority.
3) Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer.
    1. Acceptance: the reduced cost of a high-deductible health plan outweighs the potential of me getting sick/requiring treatment
    2. Mitigation: making regular backups of my documents and files
    3. Transfer: praying that I am never at fault in a car accident and that my insurance company will handle damages
4) Evaluate annualized loss expectancy as a risk management tool.
    1. The tool is handy to predict the likelihood of losses being incurred, but should not be exclusively relied upon when assessing risks and how to handle them.
5) List some factors relevant to rational risk assessment.
    1. Likelihood of the risk occurring, potential consequences/losses resulting from it occurring, and time/cost/performance factors of developing protection against it.

Lecture 4

1) Explain the key distinction between the lists on slides 2 and 3.
    1. The list on slide 3 provides implementations for enforcing the concepts given in slide 2.
2) Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.
    1. All three are, but for me availability would take precedence over the other two. There are only a few aspects of my use that require confidentiality and integrity (banking, paying bills, etc), and most breaches can be handled by a phone call or restoring one of the several backups I keep around.

3) What does it mean to “group and categorize data”?
    1. Not all data are equally sensitive – it is more efficient to tailor security protocols to a group of objects sharing similar levels of sensitivity than it is to create a separate protocol for each object.
4) Why might authorisations change over time?
    1. A person might be fired, transferred to another department/position, promoted, or retire.
5) Some of the availability questions seem to relate more to reliability than to security. How are the two related?
    1. The two rely upon each other – a lock that never unlocks is just as useless as a lock that no one knows how to unlock.
6) In what contexts would authentication and non-repudiation be considered important?
    1. Online retail – your identity must be verified before placing an order (email/billing address verification, credit card security number), and afterward the retailer cannot claim that they never received the payment.

Lecture 5

1) Describe a possible metapolicy for a) a cell phone network and b) a military database.
    1. a) Reception/service is guaranteed for those subscribed to the network.
    2. b) Nobody is allowed to access the database (before reading/writing to it) without first supplying proper credentials.
2) Why do you need a policy if you have a metapolicy?
    1. The metapolicy only describes the overarching security policies that should be enforced. The policy implements them.
3) Give three possible rules within a policy concerning students' academic records.
    1. Outside of administration, the student can only access his/her own records.
    2. A student should never be allowed to modify his/her own records.
    3. Physical records should be stored in a safe and secure location (somewhat metapolicy).
4) Could stakeholders' interest conflict in a policy? Give an example.
    1. Yes – in the example above, a student wanting to view other students' records.
5) For the example given involving student SSNs, state the likely metapolicy.
    1. Do not keep or store SSNs anywhere, whether physically or electronically.
6) Explain the statement: “If you don't understand the metapolicy, it becomes difficult to justify and evaluate the policy.”
    1. One cannot evaluate and develop the policy without knowing what the policy is supposed to achieve.

Lecture 6

1) Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?
    1. The military is the defensive backbone of a country - its actions can be globally influential and have the ability to change the geopolitical landscape. Thus, it stands to reason that all of its plans should be kept under tight control. Integrity is also present, in that only the top brass should be able to make changes to those plans, as well as availability, but confidentiality is the key issue.

2) Describe the major threat in our MLS thought experiment.
    1. Unauthorised parties gaining access to, viewing, and/or leaking highly sensitive information to enemies.
3) Why do you think the proviso is there?
    1. Only the confidentiality aspect of security is being analysed here; other aspects (e.g., integrity) are needed in the final solution.
4) Explain the form of the labels we're using.
    1. The labels are used to classify a document's level of sensitivity. These levels of sensitivity are then used to determine who has access to them.
5) Why do you suppose we're not concerned with how the labels get there?
    1. They are only there to aid in the development of a viable (security) policy. They can be considered part of the metapolicy (label documents hierarchically).
6) Rank the facts listed on slide 6 by sensitivity.
    1. Unclassified: softball game, cafeteria menu
    2. Confidential: Jones and Smith got a raise and didn't get a raise, respectively
    3. Secret: German Enigma codes broken
    4. Top Secret: Normandy invasion
7) Invent labels for documents containing each of those facts.
    1. Unclassified: General Operations and Activities
    2. Confidential: Personnel Files
    3. Secret: Global Intel
    4. Top Secret: Wartime Operations and Activities
8) Justify the rules for “mixed” documents.
    1. Documents containing information of varying sensitivities should always be classified by the highest sensitivity - Private Joe Bob might not care about what's on the menu for lunch, but as a spy he would care about plans to attack his home country. Documents containing information from different domains should have both domains/categories included to allow all authorised persons to view them.

Lecture 7

1) Document labels are stamped on the outside. How are “labels” affixed to humans?
    1. Usually through badges or IDs that contain a barcode/microchip detailing the person's clearance level (e.g., access to GDC through the card readers).
2) Explain the difference in semantics of labels for documents and labels for humans.
    1. Multiple people with the clearance level denoted by a document label can view the document; a “human” label only authorises a single person to view certain documents and generally denotes his/her level of trust within an organization.
3) In the context of computers, what do you think are the analogues of documents? Of humans?
    1. Documents => files; labels => file permissions; humans => user accounts
4) Explain why the Principle of Least Privilege makes sense.
    1. It doesn't make sense to give a person access to more resources than he/she needs; this could lead to a litany of problems, including the additional resources affecting decisions or being leaked and just wasting time.
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.

1. Pair 1: yes, because “secret” clearance outweighs “confidential” clearance and the human is authorised to read “crypto” documents.
2. Pair 2: yes, because “secret” clearance does not outweigh “top secret” clearance.
3. Pair 3: yes, because clearance is irrelevant/inapplicable for an unclassified document.
4. (All explanations ignore the Principle of Least Privilege.)

Lecture 8

1) Why do you think we introduced the vocabulary terms objects, subjects, and actions?
    1. To formalize the notions of documents, humans, and humans' actions on those documents, respectively.
2) Prove that dominates is a partial order (reflexive, transitive, antisymmetric).
    1. Reflexivity: for every label *x* in the set, *x* <= *x*.
    2. Transitivity: for each label *x*, *y*, and *z* in the set, the relationships *x* <= *y* and *y* <= *z* imply the relationship *x* <= *z*.
    3. Antisymmetry: if *x* <= *y* and *y* <= *x*, then *x* and *y* are equal/identical.
3) Show that dominates is not a total order.
    1. For every label *x* and *y* in the set, *x* is not always <= *y*.
4) What would have to be true for two labels to dominate each other?
    1. The labels' classifications are equivalent (numerically, etc), and the labels share the same compartments. They are equal.
5) State informally what the Simple Security Property says.
    1. A subject at a given security level cannot read an object at a higher security level.
6) Explain why it's “only if” and not “if and only if”.
    1. “If and only if” is a biconditional statement - either both statements are true, or both are false. “X only if Y” means X can only be true when Y is true (A => B); “X iff Y” means that A is true if B is true, and B is true if A is true ((A => B) ^ (B => A)).

Lecture 9

1) Why isn't Simple Security enough to ensure confidentiality?
    1. Simple Security only deals with read restrictions and doesn't include write restrictions.
2) Why do we need constraints on write access?
    1. To prevent persons with a higher clearance level writing to a document on a lower clearance level and to prevent those with lower clearances who gained unauthorised access to a higher-level document from modifying it (double safety).
3) What is it about computers, as opposed to human beings, that makes that particularly important?
    1. Computers aren't sentient - they do whatever their human operator(s) tell them to do (which creates issues in the case of compromised access credentials).
4) State informally what the *-Property says.
    1. A subject at a given security level cannot write to an object at a lower security level.
5) What must be true for a subject to have both read and write access to an object?
    1. The subject and object must both have the same security level; if the former's level is higher than the latter's, then the * Property would be violated, and if the former's level is lower than the latter's, then the Simple Security Property would be violated.

6) How could we deal with the problem that the General (top secret) can't send orders to the Private (unclassified)?
    1. Another system with different policies could be used that allows such functionality. For instance, the Biba Model is a no-read-down and no-write-up model (the opposite of BLP).
7) Isn't it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.
    1. Yes. One solution might be to have multiple people of at least the same security clearance level sign off on the change before it takes effect.

Lecture 10

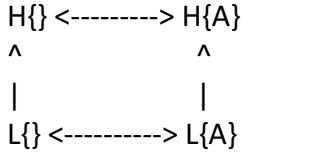
1) Evaluate changing a subject's level (up or down) in light of weak tranquility.
    1. Weak tranquility would be observed if the change in level didn't allow any subjects that couldn't write to the document before the change to read it after the change, and if the change didn't allow any subjects that couldn't read it before to read it after.
2) Why not just use strong tranquility all the time?
    1. It is very restrictive, never allows declassification, and does not observe the Principle of Least Privilege.
3) Explain why lowering the level of an object may be dangerous. Explain what conditions must hold for a downgrade (lowering of object level) to be secure.
    1. Allowing anyone to lower the level of an object would constitute a write-down situation; this is insecure and should never be allowed. Downgrades cannot occur under systems observing strong tranquility.

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?
    1. All objects could be given an arbitrary level *x*, with subjects having a level of *x* + *y*, where *y* is >= 1. This would observe the no-read-up and no-write-down principles.
2) Why wouldn't you usually build an access control matrix for a BLP system?
    1. They can be extremely large depending on the system in question. In addition, BLP systems do not feature dynamically-changeable security levels. One benefit of an ACM is that it is implicit in the rules/policies, so access permissions can be determined in real-time; since security levels never change while a BLP system is in use, this benefit is negated.

Lecture 12

1) Suppose you had hierarchical levels L and H with L < H, but only one had category A. Draw the lattice. (Use keyboard and Paint)



2) Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?
    1. LUB: follow a path up to the highest label. GLB: is label at which the path starts.
3) Explain why upward flow in the lattice really is the metapolicy for BLP.
    1. Any other directional flow of information would violate the Simple Security and * Properties of the BLP system, that is, the principles of no-read-up and no-write-down, respectively.

Lecture 13

1) Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.
    1. Information can only flow upwards in the hierarchy. A person at a higher level writing down to a lower level and a person at a lower level reading up to a higher level would constitute violations to the Simple Security and * Properties.
2) Argue that the READ and WRITE operations given satisfy BLP.
    1. Yes; the READ operation only succeeds if the Simple Security Property is satisfied. Yes; the WRITE operation only succeeds if the * Property is satisfied.
3) Argue that the CREATE and DESTROY operations given satisfy BLP.
    1. Yes; both operations demonstrate the upward flow of information necessary. However, the DESTROY operation may violate the metapolicy (should a Private be allowed to delete a Top Secret document?).
4) What has to be true for the covert channel on slide 5 to work?
    1. There exists a communication channel between the two subjects and a means to coordinate their activities.
5) Why is the DESTROY statement there?
    1. To “reset” the covert channel in order for the lower-level subject to receive a response from the higher-level subject.
6) Are the contents of any files different in the two paths?
    1. No.
7) Why does SL do the same thing in both cases? Must it?
    1. Yes. In this scenario, information flows from high to low; SL is always the receiver. It must repeatedly check for the existence of the file in order to glean the message SH is sending.
8) Why does SH do different things? Must it?
    1. Yes; it does so in order to send a binary message (1s and 0s), bit-by-bit, to SL.
9) Justify the statement on slide 7 that begins with “If SL ever sees . . . .”
    1. As computers are built around the concept of streams of bits, all it takes is a covert channel and some time to be able to assemble a message that can later be decoded.

Lecture 14

1) Explain why “two human users talking over coffee” is not a covert channel.
    1. A coffee shop is not a BLP, and they are not “utilizing system resources that were not designed to be used for inter-subject communication.”
2) Is the following a covert channel? Why or why not? (see sheet)
    1. No, if the system observes a no-read-up policy.
3) Where does the bit of information transmitted “reside” in Covert Channel #1?
    1. A status flag or a return value.

4) In Covert Channel #2?
    1. The time elapsed since the process was last scheduled.
5) In Covert Channel #3?
    1. The cylinder where the drive head was last.
6) In Covert Channel #4?
    1. The boolean result generated by the if/else statement
7) Why might a termination channel have low bandwidth?
    1. If a binary message is to be sent, the program must be terminated at some point to send either a 0 or a 1. Since programs are not normally closed before the user is finished with it, a termination channel has the potential for a very low bandwidth.
8) What would have to be true to implement a power channel?
    1. There exists a means of measuring power/energy consumption as well as a means of translating or quantifying the consumption data into meaningful/human-readable data.
9) For what sort of devices might power channels arise?
    1. Any device with a battery, electric/nuclear powerplants.

Lecture 15

1) Explain why covert channels, while appearing to have such a low bandwidth, can potentially be very serious threats.
    1. A document or piece of information can be split into several smaller chunks, making delivery easier to hide as well as being more reliable. Most files are not very large.
2) Why would it be infeasible to eliminate every potential covert channel?
    1. It is not realistic to attempt to account for every possible channel and attempt to modify or eliminate it, especially since they can be on the hardware side of the system.
3) If detected, how could one respond appropriately to a covert channel?
    1. One could make changes to the system to eliminate it or introduce noise into the channel to reduce its bandwidth.
4) Describe a scenario in which a covert storage channel exists.
    1. Sending information through or otherwise using portions of an IP packet header.
5) Describe how this covert storage channel can be utilised by the sender and receiver.
    1. It can be used to redirect the destination to an alternate IP address.

Lecture 16

1) Why wouldn't the “create” operation have an R in the SRMM for the “file existence” attribute?
    1. A nonexistent object cannot be referenced, and by its nature the operation does not need to reference the object or its attributes after it is created.
2) Why does an R and an M in the same row of an SRMM table indicate a potential channel?
    1. It indicates that two or more operations can reference or modify an object or its attributes, fulfilling the most basic requirement of a covert (storage) channel (“both sender and receiver must have access to some attribute of a shared object”).
3) If an R and an M are in the same column of an SRMM table, does this also indicate a potential covert channel? Why or why not?
    1. Possibly, if the objects/their attributes are related to each other and/or change status based on actions made to one of the objects/attributes.

4) Why would anyone want to go through the trouble to create an SRMM table?
    1. It is a useful way to consolidate the changes possible to objects and/or their attributes and to visualize the covert channels that may exist.