John-Cade Griffin

EID: jcg3335

CS361 Questions: Week 1

These questions relate to Module(s) 1. Type your answers and submit them via email to the TA by 5pm on Thursday, June 12.

Lecture 1

1. What uses of the term "security" are relevant to your everyday life? **Personal security, energy security, network security, system security**

2. What do these have in common? **All incorporate the protection of assets against threats**

3. Have you been a victim of lax security? **yes**

4. What is the likelihood that your laptop is infected? How did you decide? **some what likely, I've downloaded 3rd party software**

5. What security measures do you employ on your laptop? **minimal downloads, pw protection**

6. Do you think they are probably effective? **not if someone really wanted to target my machine**

7. Consider the quote from the FBI official on slide 10. Do you think it over- states the case? Justify your answer. **I think it is meant to incite concern, and a little hyperbolic**

8. What is the importance in learning about computer security? **enhancing your own protection., contributing to security in workplace, improve overall security in cyberspace and enhance the quality and safety of interpersonal and business transactions**

9. Lecture 2

1. Consider the five reasons given why security is hard. Can you think of other factors? **Technology is increasing at a rapid pace, seesawing back and forth between giving the advantage to systems and to threats**

2. Is there a systematic way to enumerate the "bad things" that might happen to a program? Why or why not? **No, it is impossible to anticipate everything that could go wrong**

3. Explain the asymmetry between the defender and attacker in security. **The defender has to defend against all threats, the attacker only needs to find one vulnerability**

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not? **I agree, but is complete security absolutely a must? The only way to avoid getting into a car accident is by never getting into a car, yet we weigh the risks for that every day.**

5. Explain the statement on slide 8 that a tradeoff is typically required. **If you create security barriers, its typically at the expense of efficiency, or some other opportunity cost**

Lecture 3

1. Define "risk"? **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? **Yes**

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer? **Accept: driving in a car, Avoid: skydiving, mitigate:going in the sun and wearing sunscreen, transfer: health insurance**

4. Evaluate annualized loss expectancy as a risk management tool. **effective but while assessing risk is important, it can be difficult to accurately quantify with an expected result**

5. List some factors relevant to rational risk assessment. **technical, economic, phsycological**

Lecture 4

1. Explain the key distinction between the lists on slides 2 and 3. **aspects vs mechanisms**

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer. **confidentiality, I do not want my credit card being stolen every time I use it**

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

4. Why might authorizations change over time? **users and permissions can change over time**

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related? **If a system is plagued with virus' and worms, the reliability of the system will be greatly degraded and thus the availability of resources**

6. In what contexts would authentication and non-repudiation be considered important? **authentication: a bank needs to**

authenticate users, non-rep: you would want to make sure a purchase online was with Amazon and not a phishing site.

Lecture 5

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

   Cell phone network: maintain secure and reliable phone calls

   Military Database: protect confidentiality of data while allowing appropriate access

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

   You need the details of how you are going to accomplish the metapolicy. If you only have a metapolicy, you do not have a clearly defined

set of rules on how you are going to accomplish the goals of the metabolicy.

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

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

   Documents containing SSNs must be destroyed unless deemed necessary

   Documents containing SSNs are deemed necessary for retention must be kepis in secure storage

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

Yes, like with Facebook. Facebook's interest lie in advertising revenues, while the users interest rests in social media and connectivity.

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

   Protect the confidentiality of students

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

The rules of the policy will seem arbitrary

Lecture 6

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

because the data is of high security value

and the human factor is so high. Assuring the right people have access to the right information is of paramount concern.

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

An individual with improper clearance accessing confidential information such as vital war plans and selling them to a foreign nation

3. Why do you think the proviso is there?

In this example someone with lower security could overwrite information in higher security levels. In this scenario, confidentiality was maintained

but integrity is broken.

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

label 1: secrecy level of data (unclassified, confidential, secret, top secret)

label 2: clearance level of need to know info(nuclear, cryptographic, etc)

A document labeled (Secret:{Nuclear, Crypto}) can only be read by someone with a clearance level of secret or above and a need to know info level of Nuclear and Crypto.

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

Because we are primarily concerned with confidentiality

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

The cafeteria is serving chopped beef on toast today.

The base softball team has a game tomorrow at 3pm.

Col. Jones just got a raise.

Col. Smith didn't get a raise.

The British have broken the German Enigma codes.

The Normandy invasion is scheduled for June 6.

7. Invent labels for documents containing each of those facts.

Unclassified {Cafeteria}

Unclassified {Sports}

Classified {Pay}

Classified {Pay}

TopSecret {Updates}

TopSecret {War plan}

8. Justify the rules for "mixed" documents.

The more info a user has access to, the greater the chance some of that info will be leaked. Instead it is better to give users only the info they

need to do their job.

Lecture 7

1. Document labels are stamped on the outside. How are "labels" affixed to humans? **Individuals could be given access cards**

2. Explain the difference in semantics of labels for documents and labels for humans. **A human label is considered security clearance, while a document label is its sensitivity**

3. In the context of computers what do you think are the analogues of documents? Of humans? **Read/Write permissions like in linux, and users are the equivalent of humans**

4. Explain why the Principle of Least Privilege makes sense. **Humans are innately vulnerable, its better to keep information on a need to know basis**

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.

Col 1: Makes sense: human has lower clearance level than the document's sensitivity

Col 2: Makes sense: human has a lower clearance level than

the documents sensitivity level

Col 3: Makes sense: Here the human has a higher clearance level than the documents sensitivity

Lecture 8:

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

   to make logical labels for the key objects within security

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

   You can have a situation where neither a subject Ls or object Lo dominate one another

3. Show that dominates is not a total order. **Every element must be comparable in order to have total order, there is the case where two elements cannot be compared**

4. What would have to be true for two labels to dominate each other? **exact same categories and same clearance/sensitivity levels**

5. State informally what the the Simple Security property says. **Subjects can access (read) objects if Ls > Lo and the subjects need to know categories are a superset of the objects need to know categories**

6. Explain why it's "only if" and not "if and only if." **if and only if implies that it is the only requirement**

Lecture 9

1. Why isn't Simple Security enough to ensure confidentiality? **You have a problem interns of write permissions. Say a subject reads a top secret object and then writes that to a**

   public object. Confidentiality has now been violated

2. Why do we need constraints on write access? **Confidentiality can still be broken with Simple Security. See above example**

2. What is it about computers, as opposed to human beings, that makes that particularly important? **A trusted human with clearance may access sensitive material with a computer that has malware, essentially creating a scenario where confidentiality is violated even with appropriate human security**

3. State informally what the *-Property says. **A subject may only write to objects of the same security level or above Ls <= Lo**

4. What must be true for a subject to have both read and write access to an object? **Ls = Lo**

5. How could we deal with the problem that the General(topsecret) can't send orders to the private (Unclassified)? **We could have a special mechanism for the top secret subject the general writes to, essentially downgrading the sensitivity level in order to allow the private to access the document.**

6. Isn't it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that. **Yes it is a problem, you could deny writing of subject to levels greater than your own**

Lecture 10:

1. Evaluate changing a subject's level(up or down) in light of weak tranquility. **This still maintains confidentiality**

2. Why not just use strong tranquility all the time? **There may be cases where it is appropriate to adjust the subject's level, like in Linux**

3. Explain why lowering the level of an object may be dangerous. **You open read privileges to a whole new level of subjects**

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

Lecture 11:

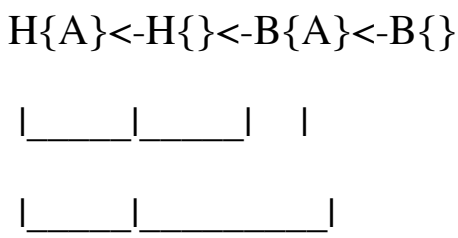
1. Suppose you wanted to build a (library) system in which all subjects had read access to all files, but write access to none of them. What levels could you give to subjects and objects? **You just need two levels, the subjects would have a higher security level than the objects, so High and Low**

2. Why wouldn't you usually build anaccesscontrolmatrixforaBLPsystem? **It is not necessary to perform all of those calculations beforehand**

Lecture 12

CS361 Questions: Week 1 5

1. Suppose you had hierarchical levels L, H with L < H, but only had one category A. Draw the lattice. (Use your keyboard and editor to draw it; it doesn't have to be fancy.)



1. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB? **To find the GLB in a lattice, you follow the edges in the opposite direction of the arrows, and to find the LUB you simply follow the direction of the arrows**

2. Explain why upward flow in the lattice really is the metapolicy for BLP. **The upward flow essentially states that Lower security levels cannot read higher security levels and that the flow of data is confidential.**

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1. **Upward flow is the metapolicy, L -> H. *-Property prevents H from writing sensitive data to L and Siple Security Prevents L from accessing sensitive data through a read in H.**

2. Argue that the READ and WRITE operations given satisfy BLP. **the metapolicy is met because a subject cannot write to a lower security level and a subject cannot read from a higher security level and this the system is confidential/**

3. Argue that the CREATE and DESTROY operations given satisfy BLP. **Since these are treated much the same as write, confidentiality is maintained.**

4. What has to be true for the covert channel on slide 5 to work? **The create channel has to be used to transfer information**

5. Why is the DESTROY statement there? **So the file can be created again to allow for the continued transfer of bits**

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

7. Why does SL do the same thing in both cases? Must it? **In order to covertly transfer information, the same outcome could be achieved in other ways**

8. Why does SH do different things? Must it? **In order to covertly transfer information**

9. Justify the statement on slide 7 that begins: "If SL ever sees..." **Here the metapolicy is being violated because information is allowed to flow down**

Lecture 14

1. Explain why "two human users talking over coffee is not a covert channel." **A coffee shop is not part of the secure system, a covert channel is always within the system**

2. Is the following a covert channel? Why or why not? **No, SH and SL are isolated from each other**

```
                Send 0        |       Send 1
```

3.
```
---------------------------------------
```
4.
```
Write (SH, F0, 0) | Write (SH, F0, 1) Read
(SL, F0) | Read (SL, F0)
```
5. Where does the bit of information transmitted "reside" in Covert Channel #1? **In the file name**

4. In Covert Channel #2? **System Clock**

5. In Covert Channel #3? **the order by which the disk system returns requests**
6. In Covert Channel #4? **The value of H, depending on if H is even or odd**
7. Why might a termination channel have low bandwidth? **Information would flow really slowly because bits are only passed on the termination of computation**
8. What would have to be true to implement a power channel? 9. For what sort of devices might power channels arise? **That the listener has access to view the power fluctuations and that the object hcan manipulate power consumption. Smart cards are a prime example of this**

Lecture 15

1. Explain why covert channels, while appearing to have such a low band- width, can potentially be very serious threats. **You can observe a great deal of information from a single bit, when translated into a boolean could inform a spy of a great deal of information. Also, processors are fast enough to where computation can be completed at relatively rapid rates**

2. Why would it be infeasible to eliminate every potential covert channel? **You would potentially end up with an unusable system, it would be too expensive**

3. If detected, how could one respond appropriately to a covert channel? **One possible method of elimination is to add noise**

4. Describe a scenario in which a covert storage channel exists. **a BLP system where a create returns a 1 or 0**

5. Describe how this covert storage channel can be utilized by the sender and receiver. **If an individual of a higher clearance wants to send a bit to a person of a lower clearance the**

individual can create a file X. When the private tries to create the file he is returned with an error bit

Lecture 16

1. Why wouldn't the "create" operation have an R in the SRMM for the "file existence" attribute? **The operation gives knowledge about an aspect of the attribute but it doesn't really give information about it.**

2. Why does an R and M in the same row of an SRMM table indicate a poten- tial channel? **Because there is a way to modify information and then read the modification**

3. If an R and M are in the same column of an SRMM table, does this also indicate a potential covert channel? Why or why not? **No, not necessarily. A single attribute must be able to be modified and read, , with R and M in the same column, this is not possible**

4. Why would anyone want to go through the trouble to create an SRMM table? **The benefit of creating an SRMM table is that you can detect covert channels.**