CS361 Questions: Week 2

These questions relate to Modules 4, 5, 6 and 7. Type your answers and submit them via email to Dr. Young by 5pm on Thursday, June 19.

The questions marked with a dagger (†) require external research and may be more extensive and time consuming. You don't have to do them for the assignment but, but you may want to do them to increase your knowledge of the subject matter.

Lecture 17

1. If a computer system complies with the BLP model, does it necessarily comply with non-interference? Why or why not?

   It does. Non-Interference is a very general policy, we can convert an MLS policy to a Non-Interference policy.

2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?

   A → B

3. Can covert channels exist in an NI policy? Why or why not?

   They cannot because NI policies only allow the flow of information to go one way. The NI policy is created to prevent information to flow the opposite direction.

4. If the NI policy is $A->B$, in a BLP system what combinations of the levels "high" and "low" could A and B have

   Both A and B can be either High or Low, or A can be Low and B is High.

Lecture 18

1. Why do NI policies better resemble metapolicies than policies?

   These policies just state where information can flow. It is very general.

2. What would be L's view of the following actions: h1, l1, h2, h3, . . . , hj, l2, l3, . . . , lk

L1, L2, L3,…,Lk.

3. What is difficult about proving NI for realistic systems?

These systems have a lot of interference, and it is difficult to prove that L is not reading H.

Lecture 19

1. Explain the importance of integrity in various contexts.

   Integrity is important because it does not require interaction with anything else in order to change information. The information could also just be incorrect.

2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?

   Commercial Software has more integrity/credibility than the free version. There are also more protections placed on the purchased software, you know exactly what you are getting.

3. Explain the difference between separation of duty and separation of function.

   Separation of duty requires that multiple subjects have to complete a critical function while Separation of Function prevents one subject from having multiple roles in a critical process.

4. What is the importance of auditing in integrity contexts?

In order to keep a record and determine when the problem occurred, who was responsible and make it easier to fix.

5. What are the underlying ideas that raise the integrity concerns of Lipner?

   The underlying idea is that all the steps of the process are confidential to members that did not work on that particular step so that information cannot leak out, or subjects cannot obtain information that they are not authorized to modify or read.

6. Name a common scenario where integrity would be more important than confidentiality.

A common scenario is downloading your music from itunes versus a torrent off of the internet.

Lecture 20

1. Give examples of information that is highly reliable with little sensitivity and information that is not so highly reliable but with greater sensitivity.

   Info that is highly reliable but with little sensitivity includes NASA's findings on Mars and Newton's equation for gravity. Info that is not highly reliable but has greater sensitivity includes the location of Area 51.

2. Explain the dominates relationships for each row in the table on slide 4.

   For row one, the Expert on physic know more than a student learning physics. For row two, a Novice on physics and art would know less that an Expert on physics, because we would compare the knowledge of physics. And for row three, the student studying art would know more than a novice who knows nothing.

3. Construct the NI policy for the integrity metapolicy.

   If we say that A is (Expert{physics}) and B is (Student{physics}) the NI policy would be A->B

4. What does it mean that confidentiality and integrity are "orthogonal issues?"

   A program can have a very high integrity and low confidentiality and vice versa. They are independent of each other.

Lecture 21

1. Why is Biba Integrity called the "dual" of the BLP model?

   It's rules are the opposite of BLP.

2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?

   They might be on the same level but the categories for the Subj3 label is not a superset of the categories of the Obj3 label

3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?

No. If I want to use both BLP and BIBA, both sets of rules have to apply.

Lecture 22

1. What is the assumption about subjects in Biba's low water mark policy?

   That they are not worthy to carry their label if they read bad information.

2. Are the subjects considered trustworthy?

   Subjects are not trustworthy.

3. Does the Ring policy make some assumption about the subject that the LWM policy does not?

   Yes. The Ring policy assumes that its subjects can filter out bad information.

4. Are the subjects considered trustworthy?

   They are considered trustworthy.

Lecture 23

1. Are the SD and ID categories in Lipner's model related to each other?

   SD and ID most likely refer to the same development, however each label in confidentiality and integrity need different names.

2. Why is it necessary for system controllers to have to ability to downgrade?

   System controllers control the software being developed and need to have the ability to decide if a program is ready to be developed or not.

3. Can system controllers modify development code/test data?

   The can modify it because their integrity level dominates the other subjects.

4. What form of tranquility underlies the downgrade ability?

   Weak tranquility underlies the downgrade ability.

Lecture 24

1. What is the purpose of the four fundamental concerns of Clark and Wilson?

   These are to protect the integrity of a program and to keep the process consistent.

2. What are some possible examples of CDIs in a commercial setting?

   CDIs include a transaction at a store and inventory.

3. What are some possible examples of UDIs in a commercial setting?

   UDIs include free samples and pamphlets.

4. What is the difference between certification and enforcement rules?

   Certification Rules are how the system certifies that a particular data object is valid while Enforcement Rules make sure that the certified data maintains its integrity.

5. Give an example of a permission in a commercial setting.

   The cashier has permission to take a customer's money and perform a transaction.

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?

   Both Airlines are in competition with each other and might have information that can be stolen.

2. In the example conflict classes, if you accessed a file from GM, then subsequently accessed a file from Microsoft, will you then be able to access another file from GM?

   Yes, the Simple Security Rule states that a subject can get access to an object if it has already had access to the object or it is in a different class.

3. Following the previous question, what companies' files are available for access according to the simple security rule?

I can access GM, Microsoft and one of the following: Wells Fargo, Bank of America, or Citicorp.

4. What differences separate the Chinese Wall policy from the BLP model?

The Chinese Wall policy takes into consideration what you have done in the past and the subject is able to read and write as long as it has not been accessed before and complies with the Chinese Wall simple security rule.

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects?

   This makes it easier to assign specific jobs to an entire group of subjects instead of assigning specific permissions one at a time.

2. What is the difference between authorized roles and active roles?

   Authorized roles are the roles that the subject may assume while active roles are the roles that the subject is currently assuming.

3. What is the difference between role authorization and transaction authorization?

   Role authorization refers to the roles that a subject may assume while transaction authorization states that the transaction can only be done if it is in a subjects active role.

4. What disadvantages do standard access control policies have when compared to RBAC?

   They are very general policies that have to be applies to one subject at a time while RBAC has specific label and specific actions that can be given to large groups of subjects.

Lecture 27

1. Why would one not want to build an explicit ACM for an access control system?

   Most of the time in realistic systems, most subjects do not have access to any of the objects.

2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.

   We can compute permissions on the fly, make access-control lists or finally, make a capability-based system.

Lecture 28

1. What must be true for the receiver to interpret the answer to a "yes" or "no" question?

   The receiver must have prior knowledge to know which bit, 0 or 1, will represent yes or no.

2. Why would one want to quantify the information content of a message?

   We would need to know how much information is passed over a given channel. If the amount information is larger than the channel this can cause a security problem.

3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?

   Having this shared knowledge is the only way the receiver can interpret the information sent to it.

4. Why wouldn't the sender want to transmit more data than the receiver needs to resolve uncertainty?

   This could cause a problem if the sender sends an amount of information that is too big for the channel. The receiver could also leak access information that is not being used to interpret the information at that moment.

5. If the receiver knows the answer to a question will be "yes," how many bits of data quantify the information content? Explain.

   If the receiver knows, then all the sender has to send is the one bit of information that signals yes.

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?

   Message 1 contains bits or n bits, Message 2 contains about 4 bits of information, and Message 3 contains about 7 bits of information.

2. Why does the amount of information contained in "The attack is at dawn" depend on the receiver's level of uncertainty?

   The receiver is unsure of the number of options other than dawn. If it does not know how many time interval options it needs to set aside and cannot prepare for the amount of information it will receive.

3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?

   If we look at the binary tree representation of the size of the information, each value splits the number of searches in half. Therefore the amount of the bits of information sent is log(size). The amount of bits is 4.

4. How much information content is contained in a message from a space of 256 messages?

   Log(256) =8.

5. Explain why very few circumstances are ideal, in terms of sending information content.

   Many times the receiver does not know ahead of time the amount of information being sent to it.

Lecture 30

1. Explain the difference between the two connotations of the term "bit."

   Bit can either be a binary digit, 0 or 1. Bit can also be a measurement of the information content and is continuous.

2. Construct the naive encoding for 8 possible messages.

   Log(8) = 3 bits of information.

3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.

We assume that if the message is 10 it will send 1 bit. This bit will send 995 times. We then add this to the 5 times it calls an error message which we assume will send 1 bit 5 times to give us the error message.

4. How can knowing the prior probabilities of messages lead to a more efficient encoding?

   We can compute the amount of bits per message for optimal encoding.

5. Construct an encoding for 4 possible messages that is worse than the naïve encoding.

   We have to send 1000 messages which is one of 4 possibilities. 250 messages are message 10 and 750 are an error. The naïve encoding is 2 X 1000 = 2000. Or we can make it so that we have 250 that are message 10. This will give us 250 bits and with a 1 added in front of the error messages, we have 250 +(750 X 3 bits) = 2500.

6. What are some implications if it is possible to find an optimal encoding?

   It would need to be the best encoding that we could come up with in our language.

Lecture 31

1. Name a string in the language consisting of positive, even numbers.

2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.

   1= 000, 2= 001, 3= 010, 4=011, 5=100, 6=111

3. Why is it necessary for an encoding to be uniquely decodable?

   We do not want there to be different ways of interpreting the string of language.

4. Why is a lossless encoding scheme desirable?

   We want the receiver to completely recover the sequence of symbols.

5. Why doesn’t Morse code satisfy our criteria for encodings?

   Morse code does not stream, there is a break in letters.

Lecture 32

1. Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).

   H = -(log 1/n) = log n with n=8. H=log 8 =3.

2. If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?

   T = 4/4 h= -(1 log 1 + 0 log 0) = 0

   H= 0/4

3. Why is knowing the entropy of a language important?

   Entropy measures the average information content of symbols in the language which sets a lower limit on encoding efficiency.

Lecture 33

1. Explain the reasoning behind the expectations presented in slide 3.

   Since it is doubled, we multiply H with itself giving us 9/4. We multiply H with T which gives us 3/16 for both HT and TH. Finally we multiply T with itself giving us 1/16.

2. Explain why the total expected number of bits is 27 in the example presented in slide 4.

   We are doubling the number of time we count our flips. Since the number of doubled flips out of 32 is the lower denominator, we take the upper denominator as the number of times the set occurs. If we multiply this by the number of bits in our encode and add them together, we get 27.

3. What is the naive encoding for the language in slide 5?

   If we use a 2Roll, and use 24 rolls, the naïve encoding is 24 bits.

4. What is the entropy of this language?

   Approximately 1.72

5. Find an encoding more efficient than the naive encoding for this language.

If we use 24 2Rolls which is 12 rolls, this will give us 6 (12 rolls), 3(34 rolls) and 2(56 rolls). If we assign codings to these rolls with 12 having 1 bit, 34 having 2 bits and 56 having 3 bits we get a total of 18 bits.

6. Why is your encoding more efficient than the naive encoding?

   We use less bits this way.