CS361 Questions: Week 2

Daniel Ricaud
UTeid: dr25237
CSid: dr25237

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.

Thequestionsmarkedwitha dagger(†) requireexternalresearch and maybemore 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?

   No because you would need a direct line from a to c but non interference would need the line to go from a to b and then b to c.

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

   Neither dominates the other.

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

   Supposedly not because a lower level subject should not be able to see anything that gives away the behavior of a high level subject.

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?

   A->A, B->B, A->B

Lecture 18

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

   They just describe the overall policy but don't really show how to enforce the policy

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

   It should only be able to see it's own actions in a NI policy type of system.

channels.

Lecture 19

1. Explain the importance of integrity in various contexts.

   Depending on where you get your information you may or may not think it's credible

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

   Because the freeware could come bundled with unexpected stuff like malware.

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

   Seperation of duty places several people doing one task to disperse the responsibility, separation of function makes sure that one person is not doing two conflicting tasks.

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

   In a work environment there has to be accountability and a hierarchical structure.

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

   That everything should be done within procedure and using more proven commercial software as compared to using freeware or unprotected software.

CS361 Questions: Week 2

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

   When you read an article you're more likely to believe it if it came from a credible source.

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.

   Little: Time Magazine has an article about different dog breeds.

   Great: A trusted general tells the president about the enemies plans.

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

student of art will dominate a novice at anything.

3. Construct the NI policy for the integrity metapolicy.

   Good -> bad

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

   It means that they are two totally different facets of security and need to be treated as two separate things.

Lecture 21

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

   Because you can switch the reads with writes and vice versa in the BLP model to get the Biba model.

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

   Because they belong to separate sets.

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

   Yes

Lecture 22

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

   It assumes that the subject (you) is as trustworthy as the information they're reading.

2. Are the subjects considered trustworthy?

   No

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

   It assumes that eventually everyone will read information of low integrity.

3. Are the subjects considered trustworthy?

   Yes.

Lecture 23

Yes

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

So that you can transfer the software from development to software.

CS361 Questions: Week 2

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

   Yes.

3. What form of tranquility underlies the downgrade ability?

   The user being trustworthy.

Lecture 24

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

   It's the layout for a secure system that any commercial enterprise could use.

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

   Emails and phone numbers

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

   Websites visited and the number of views

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

   Enforcement rules have more to do with users executing actions while certification rules just lay out the initial checks.

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

   Delete user record.

Lecture 25

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

   He could share potentially classified information.

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, they are not in competing brackets.

3. Following the previous question, what companies' files are available for

Bank of America, Wells Fargo, Citicorp.

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

   The Chinese Wall policy is more focused on conflicts of interest by a consultant or contractor.

Lecture 26

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

   Because a subject could have multiple roles.

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

An authorized role is a role that a subject is allowed to fill at various times, an active a role is a role that a subject currently occupies.

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

   Role authorization is making sure the subject is active in the correct role and transaction authorization is making sure that the subject cannot make a role do a transaction that it was not designed to do.

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

A subject can only have one role, it's only about subject checking, it's not flexible at all.

Lecture 27

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

   Because you store the permissions with objects or subjects.

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

   You can maintain a set of rules to compute access permissions based on attributes of subjects and objects, you can store permissions with objects, this is known as an access control list, lastly, you can store permissions with subjects, this is called a capability based system.

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

   The receiver must be able to see one at least one bit of data from the sender.

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

   So you can figure out how much bandwidth it requires

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

   So the receiver can decrypt the sender’s message.

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

   Because that would be a waste of bandwidth and inefficient

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 already knows the answer then it doesn’t need any bits to quantify the information.

Lecture 29

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

   First message contains 2^n possible pieces of data
   The second contains 10^1 == 10
   The third contains 10^2 == 100

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

   Because it could be extremely vague and out of context about what they’re even talking about, so in that case it would contain almost no information. Or it could be the answer to a very specific question in which case the statement would contain a lot of information.

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

   4, because this gives you 16 different possible combinations of bits

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

   8 binary bits can encode 256 different messages

Because you usually don't know ahead of time the encoding and how many possible messages could be sent.

Lecture 30

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

   It could mean either a binary digit or a chunk of data.

2. Construct the naive encoding for 8 possible messages.

   M0 = 000, M1 = 001, M2 = 010, M3 = 011, M4 = 100, M5 = 100, M6 = 101, M7 = 111

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

   Because the encoding for message 10 only takes 1 bit, so you need 995 for M10, and you need 5 bits to encode the other 5 possible messages.

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

   Because then you don't have to waste a bunch of extra bits on messages that don't need as many bits as others, like message 10 in the last example.

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

   M0 = 000000, M1 = 000001, M2 = 000010, M3 = 000011

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

   You need to know the probability of certain messages being received.

Lecture 31

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

   749374838

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

   1= 001, 2 = 010, 3 = 011, 4 = 100, 5 = 101, 6 = 110

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

could have errors.

4. Why is a lossless encoding scheme desirable?

   Because you can recover the entire original string given the encoded string.

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

   It isn't prefix-free.

Lecture 32

1. Calculate the entropy of an 8-sided, fair die (alloutcomesareequallylikely).

   H = -((1/6) x log(1/6) + the same thing 6 more times) = entropy

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

   H = -((4/5) x log(4/5) + (1/5) x log(1/5)) = entropy

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

   Because then you know if you've found the optimal encoding.

Lecture 33

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

They just multiplied the probability of the two combinations of coin flips, this gives them an estimate of the chance of each 2 flip happening.

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

   Because they took into account how many bits it takes to represent a certain outcome in code and also how likely that outcome was to occur.

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

   M1 = 000, m2 = 001, m3 = 010, m4 = 011, m5 = 101, m6 = 110

4. What is the entropy of this language?

   H = -(2((1/9) x log(1/9)) + 2((3/9) x log(3/9)) + 2((6/9) x log(6/9)))

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

   You could roll the die in pairs and measure the probability of each die combination being rolled. Then, start encoding the outcomes using binary

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

   Because measuring pairs of die rolls takes less bits especially when you don't have to waste extra bits on combinations of die rolls that are very unlikely to happen.