Name: Tyler Kemme
EID: tpk266
CS Login: tpkemme
Email: tpkemme@gmail.com

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?

No because the BLP model does not take into account the flow of information due to actions taken by any level subject.

2. What would the NI policy be for a BLP system with subjects: A at (Secret:

Crypto), B at (Secret: Nuclear)?

A -> A, B -> B

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

Covert channels can still exist within an NI policy because a system can only be as secure as the policy is strong. To have a system without any covert channels would require including everything in the system within the user's view.

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 could only be low and B could only be high.

Lecture 18

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

NI policies better resemble metapolicies because they are similar to policy tools used to insure the metapolicy of confidentiality.

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

l2, l3, . . . , lk

L's view of the actions would be l1, l2, l3, … , lk

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

You can't include everything in the system into the view of the subject because that would be much too complex.

Lecture 19

1. Explain the importance of integrity in various contexts.

Integrity is important in network security. If Alice sends Bob a message, Alice will want to ensure the integrity of her message so that she knows Bob is receiving the same message she sent. This means that someone between Alice and Bob cannot change the contents of the message

2. Why would a company or individual opt to purchase commercial software

rather than download a similar, freely available version?

Source code for commercial products is usually private so it is much harder for attackers to find vulnerabilities in the software.

3. Explain the difference between separation of duty and separation of func-

tion.

Separation of duty involves making sure that a critical task is divided among multiple subjects to decrease the chance of one subject inappropriately completing the task. Separation of function means ensuring that a subject can't complete two parts of a process that rely on each other.

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

Auditing is making sure that logs are kept of different actions so that if something does happen, there's a record of it.

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

Employees using company software should not also be the ones writing the software because they could change the software to meet their personal goals. The programmers that write the software should be able to see information used by employees who use the software.

CS361 Questions: Week 2 2

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

confidentiality.

Wikipedia is a scenario where integrity is more important than confidentiality. Anyone can view and edit all of the data on the site. But their biggest concern is ensuring the integrity of that data by including sources and checking said sources.

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.

Information that is highly reliable but not very sensitive is information in the dictionary. An example of not so reliable, but sensitive information could be witness information in a crime. The information may not be completely true, but if it got in the wrong hands it could compromise an investigation.

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

1. Label 1 dominates Label 2 because label 1 has a higher degree of trustworthiness in physics.
2. Label 1 does not dominate Label 2 because Novice is less trustworthy than Expert.
3. Label 1 dominates Label 2 because Student dominates Novices and Art is a superset of the set of nothing.

3. Construct the NI policy for the integrity metapolicy

If A is low integrity and B is high integrity:
A <- B

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

The issues are orthogonal because they are not related to each other.

Lecture 21

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

It is the “dual” because it is basically the exact same as the Simple security and * property of the BLP model except the arrows go in the opposite direction.

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

That entry is empty because although the integrity levels are the same, the set of categories in the object is not a superset of the categories in the subject.

3. If a subject satisfies confidentiality requirements but fails integrity require-

ments of an object, can the subject access the object?

No, it cannot.

Lecture 22

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

The assumption is that the subject is corrupted by poor information and thus the integrity label will go down if the subject reads low integrity information.

2. Are the subjects considered trustworthy?

Subjects are as trustworthy as their last read.

3. Does the Ring policy make some assumption about the subject that the

LWM policy does not?

The ring policy assumes that the subject is not corrupted by low integrity information.

4. Are the subjects considered trustworthy?

The subjects are considered as trustworthy as their integrity level.

Lecture 23

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

Yes, they are both the category for development.

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

CS361 Questions: Week 2 3

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

Yes, they can mondify development code/test data

4. What form of tranquility underlies the downgrade ability?

Strict tranquility.

Lecture 24

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

The purpose of the four fundamentals of the Clark and Wilson model is to outline security concerns specifically for a commercial setting.

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

An idea of a CDI would be private customer information such as bank records, addresses and credit card numbers.

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

An example of an object that is a UDI is the carpet that goes along the floor of the bank.

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

Certification rules outline how the system makes sure than a certain object passes integrity verification procedures. Enforcement rules specific how the system maintains the integrity of the object through transactions.

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

For example, a bank teller would have permission to withdraw money from a user's account.

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a

breach of confidentiality if also hired by United Airlines?

It would be a breach of confidentiality because the consultant could bring sensitive information from American Airlines over to United Airlines or vice versa.

2. In the example conflict classes, if you accessed a file from GM, then sub-

sequently accessed a file from Microsoft, will you then be able to access

another file from GM?

Yes because GM and Microsoft are not conflicting classes.

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

access according to the simple security rule?

According to the example, the user can read GM files, Microsoft files, and then one class of bank files. However, after he/she reads the company's bank files, he/she cannot access the files of any other bank.

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

The Chinese Wall policy is different than the BLP model because the permissions of the user change dynamically as they access different company files.

Lecture 26

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

subjects?

Instead of assigning individual permissions to subjects and objects, roles create a collection of permissions depending on the job title of the user.

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

Active roles is a subset of the authorized roles.

3. What is the difference between role authorization and transaction authoriza-

tion?

Role authorization simply says that a subjects' active roles must be a subset of the authorized roles whereas transaction authorization says that a subject can only perform transactions authorized by their active roles.

4. What disadvantages do standard access control policies have when com-

pared to RBAC?

Standard access control policies are much harder to implement and they also cannot allow subjects to transition to different roles without changing identities.

CS361 Questions: Week 2 4

Lecture 27

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

system?

You wouldn't want to build an explicit ACM because most users don't have access to most files so the matrix would be massive and mostly sparse.

2. Name, in order, the ACM alternatives for storing permissions with objects,

storing permissions with subjects and computing permissions on the fly.

1. access control list

2. capability-based system

3. implicit rules for access control

Lecture 28

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

question?

The receiver must know if a 1 represents a yes or no.

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

Quantifying information in a message allows the system to regulate the control of information.

3. Why must the sender and receiver have some shared knowledge and an

agreed encoding scheme?

The sender and receiver must have an encoding scheme so that the data sent back and forth makes sense to both of them. They must also have shared knowledge so they can interpret encoded results.

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

to resolve uncertainty?

If the sender sends more information, this increases the bandwidth of the channel.

5. If the receiver knows the answer to a question will be “yes,” how many bits

of data quantify the information content? Explain.

Only a single bit of data quantifies the information content. This is because the receiver only needs a 1 to say “the answer is yes” or a 0 to say “the answer is no”.

Lecture 29

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

slide 2?

1. n bits
2. 4 bits
3. 7 bits

2. Why does the amount of information contained in “The attack is at dawn”

depend on the receiver’s level of uncertainty?

Depending on how much knowledge the receiver has, you need to send a different amount of information. For instance, if the attack could be at either dawn or dusk, then you would only need one bit.

3. How many bits of information must be transmitted for a sender to send one

of exactly 16 messages? Why?

4 bits of information because each time the receiver gets a bit, the number of possible messages is cut in half.

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

256 messages?

8 bits

5. Explain why very few circumstances are ideal, in terms of sending informa-

tion content.

Circumstances are usually not ideal because the sender and receiver have to understand each other’s level of uncertainty and they also need to have previously agreed on an encoding scheme.

CS361 Questions: Week 2 5

Lecture 30

1. Explain the difference between the two connotations of the term “bit.”

A bit can either be a binary digit or it can be a continuous quantity of information.

2. Construct the naive encoding for 8 possible messages.

Msg	CODE
M0	000
M1	001
M2	010

M3	011
M4	100
M5	101
M6	110
M7	111

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

Because message 10 happens 99.5% of the time and is only a single bit, then for 1000 messages, 995 of them will only have a single bit. The other 5 messages have 5 bits each.

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

encoding?

If you know a message is very likely to occur, you can encode it with very few bits to limit the amount of bits being sent.

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

encoding.

M1	10000
M2	10001
M3	10010
M4	10011

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

If it was possible to find an optimal encoding for every language, then you would have to always know the probability that each message is sent given n messages.

Lecture 31

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

42

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

1	1
2	11
3	111
4	1111

5 11111
6 111111

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

If the encoding wasn't uniquely decodable, then the receiver could possibly decode the string and get an incorrect message.

4. Why is a lossless encoding scheme desirable?

The receiver needs to be able to completely recover the entire transmission.

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

Because if you had a constant stream of morse code, it would be impossible to distinguish between letters because there aren't breaks between letters.

Lecture 32

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

h = -(1/8 *-3 + 1/8*-3…) = -(8*(-3/8)) = 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?

H = 4/5
T = 1/5
h = -(4/5*-.321 + 1/5*-2.321) = .721

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

If you know the entropy of a language, you can figure out if a more efficient encoding is impossible.

Lecture 33

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

Because each flip is independent of each other, you multiply the individual probabilities together to get the overall probability.

CS361 Questions: Week 2 6

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

in slide 4.

For the first result, you would expect it nine times and it takes 9 bits. The next two are expected 3 times using 6 and 9 bits. Finally, for the last result you only expect it once and you use 3 bits. Thus there are 27 total bits in 16 flips.

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

000, 001, 010, 011, 100, 101, 110, 111

4. What is the entropy of this language?

Result	Probability
1	6/20
2	6/20
3	3/20
4	3/20
5	1/20
6	1/20

h = -(-1.04 + -.821 + -.432) = 2.29

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

1	00
2	01
3	10
4	110
5	1110
6	1111

Bits per 20 messages for this encoding = (2*6 + 2*6 + 2*3 + 2*3 + 8) = (12+12+6+12+10) = 52
Bits per 20 message for naïve encoding = 20*3 = 60

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

It gives less bits to results that are more likely to occur.