Name: Luis Lopez
EID: LL9338
CS Login: LL9338
Email: Lclg21@utexas.edu

CS361 Questions: Week 2

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 some Non-Interference policies might not be transitive and all MLS policies, which we include BLP, are transitive by definition.

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

B → A

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

Covert channels can exits within a NI policy because even though it controls the flow of information, there can be areas where bits of information can be detected within the subjects that are communicating.

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?

The level of B dominates the level of A, meaning that A is low level and B is high level.

Lecture 18

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

Because there are no rules about which subjects can read and/or write which objects. NI policies is more about information flowing from L to H only, which is similar to the metapolicy for confidentiality.

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?

In realistic systems, there are a lot of interferences so it would be impossible for most real systems to ever prove that it was not interfering. Also, Most involve low-level system attributes and many interferences are benign, making it hard for realistic systems to prove they are NI.

Lecture 19

1. Explain the importance of integrity in various contexts.

It is important because Integrity can be about who can modify or supply data, how you separate and protect assets, and how you detect or correct erroneous or unauthorized changes to data.

Name: Luis Lopez
EID: LL9338
CS Login: LL9338
Email: Lclg21@utexas.edu

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

Because it is about the integrity of the source that makes it more believable rather than something that its on the internet for free from an unknown source or less reliable source.

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

In separation of duty, several different subjects must be involved to complete a critical function. In separation of function, a single subject cannot complete complementary roles within a critical process.

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

To keep careful records so that if something bad does happen, we can go back and assign responsibility and perhaps rollback and take care of whatever the problem was.

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

Lipner describes integrity concerns for a commercial data processing environment which are: Users should not write their own programs, but use existing production software. Programmers develop and test applications on a nonproduction system, possibly using contrived data. Moving applications from development to production requires a special process, which needs to be controlled and audited, and managers and auditors must have access to system state and system logs.

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

Integrity would be more important than confidentiality particularly in the commercial world.

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 has to do with school grades.

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

Row 1: (Expert: {Physics}) dominates (Student: {Physics}) because expert >= student and the set of categories, physics, is a superset of the set of categories physics.

Row 2: (Novice: {Physics, Art}) Does Not Dominates (Expert: {Physics}) because label Novice is <= label Expert.

Row 3: (Student: {Art}) dominates (Novice: {}) because Student is >= Novice and the set of categories Art is a superset of the empty set of Novice.

3. Construct the NI policy for the integrity metapolicy.

The NI policy for the integrity metapolicy can be that we don’t want information to flow up within integrity.

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

It means that integrity and confidentiality are not related to each other. You can have a high integrity subject with low confidentiality and vice versa.

Name: Luis Lopez
EID: LL9338
CS Login: LL9338
Email: Lclg21@utexas.edu

Lecture 21

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

Because now in integrity the subject can read an object only if the level of the subject is dominated by the level of the object and the subject can write to object only if the level of the object its dominated by the level of the subject. That is the opposite from the BLP model, the arrows just change direction. You apply the same rules but you just apply them in the opposite order.

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

Because the set of categories for label L, A and B is not a superset of the set of categories for label L, B and C.

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

The subject cannot access the object because to protect confidentiality and integrity, the access is only allowed if it’s allowed by both the BLP rules and the Biba rules.

Lecture 22

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

The level of information flows down to the level of information that was brought in, and so, Biba is not giving much credit to the subject.

2. Are the subjects considered trustworthy?

Some of them might not be trustworthy since the flow of information can be corrupted once it flows down to the level of information that was brought in.

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

That the subject can properly filter the information it receives.

4. Are the subjects considered trustworthy?

Yes the subjects are considered more trustworthy in the Ring Policy.

Lecture 23

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

They are not related to each other. SD is a confidentiality category and ID is an integrity category.

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

Because there is not a way to downgrade in BLP and Biba.

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

Yes because system controllers have SL access and that includes SP and SD, which is production code and data and programs under development.

4. What form of tranquility underlies the downgrade ability?

The weak Tranquility property.

Lecture 24

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

The purpose of the four fundamental concerns of Clarck and Wilson is to better reflect the integrity requirements of real commercial enterprises.

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

Bank balances, checks. Objects whose integrity is protected.

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

Taking a piece of candy from the counter at the bank, no one will audit that activity.

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

In certification rules, All IVPs must ensure that CDIs are in a valid state when the IVP is run. That all TPs must be certified as integrity-preserving. The operation of TPs must be logged. And in Enforcement rules, Only certified TPs can manipulate CDIs. Users must only access CDIs by means of TPs for which they are authorized.

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

If some user wants to perform an action, it has to be the case that that action is in the form of the transaction procedure and it can only be performed on certain sets of items or objects within the system.

Lecture 25

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

Because the simple access control policy states that a subject may access information from any company as long as that subject has never accessed information from a different company in the same conflict class and since American Airlines and United Airlines are in the same conflict class, there would be a breach of confidentiality.

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, because you are accessing a file from two different conflict classes. GM can access a file from Microsoft and then Microsoft can access a file from GM.

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

All the files since both subjects are from a different conflict of interest class.

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

That the Chinese wall is an access control policy that was designed to address a very specific concern which is conflict of interests by a consultant or contractor and also illustrates that security policies can be crafted to solve very specialized problems.

Lecture 26

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

It makes managing and organization much more possible and easier.

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

Authorized roles is the set of roles the subject may assume. Active roles is the set of roles the subject currently assumes.

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

In role authorization, A subject's active role must be an authorized role for that subject. In Transaction authorization, a subject can execute a transaction only if the transaction is authorized for one of the subject's active roles.

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

That standard access control policies is a little bit more complicated to administered. It doesn't allow subjects to transition between roles without having to change identities. It doesn't recognize that a subject often has various functions within the organization.

Lecture 27

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

Because in realistic systems most subjects don't have any access to most objects.

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

First, maintain a set of rules to compute access permissions on the fly based on attributes of subjects and objects. Second, Access control list, which stores the permissions with objects. Third, a capability-based system, which stores the permissions with subjects.

Name: Luis Lopez
EID: LL9338
CS Login: LL9338
Email: Lclg21@utexas.edu

Lecture 28

1. What must be true for the receiver to interpret the answer to a “yes” or “no” question?
The receiver has to know how to interpret the answer. So there has to be an agreement between the sender and the receiver on a coding scheme.

2. Why would one want to quantify the information content of a message?
Because the information would make it more clear for the receiver to understand and also so that the information traveling between the sender and the receiver be more efficient.

3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
Because if they do not have shared knowledge and agree on an encoding scheme, they no communication will occur.

4. Why wouldn’t the sender want to transmit more data than the receiver needs to resolve uncertainty?
Because that would make the transmission of information less efficient, since the receiver might only need one bit of information to clear uncertainty.

5. If the receiver knows the answer to a question will be “yes”, how many bits of data quantify the information content? Explain.
Only one bit because since the receiver already knows that the answer is “yes”, that means that both the sender and the receiver have some shared knowledge and probably agreed on an encoding scheme, which can be 0 for no and 1 for yes, only one bit of information.

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?
In the first message it contains n-bits of information. On the second message it contains 4 bits of information. On the third message it contains 8 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?
Because if the receiver knows the encoding scheme, specially for strings, then the amount of information sent by the sender would be less bits than the actual string message.

3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
It would need 4 bits of information. Because it would be an efficient way to find the message transmitted out of the 16 messages by splitting the search space in half until the message has been found. That would only take at most 4 times.

4. How much information content is contained in a message from a space of 256 messages?
By using log2(256) we get 8 bits of information.

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

Some circumstances are ideal because it’s more efficient and because it reduces the search space by half.

Lecture 30

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

Bit1 is a binary digit which is discrete. Bit2 is a quantity of information which is continuous.

2. Construct the naive encoding for 8 possible messages.

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 since 99.5% will be message 10, then it would require 995 bits plus 5 additional bits for each other message, which are 5 messages, so it would require 25 bits for the other 5 messages.

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

Because if we know how often a message appears in an arbitrarily long sequence of messages, it would be easier to compute the number of bits per message.

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

M0:100
M1:010
M2:001
M3:011

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

That it would be the most efficient way to transmit messages.

Lecture 31

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

String = “2468”

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

1: 00
2: 001
3: 0010
4: 10
5: 101
6: 1010

Name: Luis Lopez
EID: LL9338
CS Login: LL9338
Email: Lclg21@utexas.edu

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

Because for any encoded string , there is only one possible decoding.

4. Why is a lossless encoding scheme desirable?

Because by using lossless encoding, we would not lose any information between the transmission of information and would recover the entire original sequence of symbols.

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

Because Morse code is non-prefix-free and it can assign a tree consecutive dots to S and we would not know if its 3 E's or S. So this type of encoding is note very efficient.

Lecture 32

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

1: 1/8
2: 1/8
3: 1/8
4: 1/8
5: 1/8
6: 1/8
7: 1/8
8: 1/8

h = -(1/8 X log1/8 + 1/8 X log1/8 + 1/8 X log1/8 + 1/8 X log1/8 +
1/8 X log1/8 + 1/8 X log1/8 + 1/8 X log1/8 + 1/8 X log1/8)
h = 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: x   Probabilities -> H: 1/5
T: 4x   T: 4/5

4x + x = 5x
5x = 1
x = 1/5

h = - (1/5 X log1/5 + 4/5 X log4/5)

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

Because it measures the average information content of symbols in the language and sets a lower limit on encoding efficiency.

Name: Luis Lopez
EID: LL9338
CS Login: LL9338
Email: Lclg21@utexas.edu

Lecture 33

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

By using 2 flips we can get an even better average of bits per message than using only 1 flip. A better efficient encoding.

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

Because for HH it lands 9 times and it uses 1 bit, HT it lands 3 times and it uses 2 bits, so 6 bits, TH lands 3 times but it uses 3 bits, so 9 bits total, and TT lands 1 times and it uses 3 bits, so 3 bits. Then the total bits uses counts to 27 bits.

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

1: 000
2: 001
3: 010
4:011
5:100
6:101

4. What is the entropy of this language?

h = - (6/20 X log 6/20 + 6/20 X log 6/20 + 3/20 X log 3/20 +
3/20 X log 3/20 + 1/20 X log 1/20 + 1/20 X log 1/20)

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

1: 0
2: 10
3: 110
4: 1110
5: 11110
6: 11111

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

Because since 1 and 2 are more likely to appear than the other 4 numbers, they are assign less bits than the other ones so that the information can be more efficient to decode.