**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?

Yes, any BLP model can be turned into a non-interference policy

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

Since they are both secret, they can both write information to eachother, but not read info between the two.

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

No. The non-interference policy prohibits any means of information to be passed down.

1. 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 = secret, B = top secret

**Lecture 18**

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

The L to H non-interference policy mimics the confidenciality metapolicy

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

L1, l2, l3 ….lk

1. What is about proving NI for realistic systems?

Realisitic systems have lots of interferences

**Lecture 19**

1. Explain the importance of integrity in various contexts.

Integrity protects the modification of data from the internal users. You don’t want a bank employee to change your savings account even though they might have access to it. This is known as “trustworthiness”

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

So the company it bought it from would have to be accountable for any mistakes and would have a higher integrity level of their data. A free software might not care about the integrity as much since they aren’t making any money.

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

Seperation of Duty requires that several different subjects must be involved to complete a function, where as seperation of function requires that one subject cannot hold complementary roles in a process.

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

Auditing is necessary so that responsibility can be assigned for mistakes and so that if a mistake is made, there is a trail to find out what went wrong.

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

Users (tellers) should not do their own programming, and programmers should not opperate on real peoples data.

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

In bank account information or online retail.

**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.

Wikipedidia is highly reliable with little sensitivity, and reddit is not so highly reliable with greater sensitivity.

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

The dominates relationship is the same from the confidentiality policy. If the security level is higher or equal, and the sub catagory is a subset of the first subjects then it dominates the second subject

1. Construct the NI policy for the integrity metapolicy.

We don’t want low integrity information to currupt high integrity information

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

We shouldn’t view the policy as the same for both, even though they follow the same dominates relation

**Lecture 21**

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

Because the Biba integrity model follows the BLP model, except for the dominates relations are backwards.

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

Because neither of the sets are subsets of the other.

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

No, the subject has to satisfy both requirements.

**Lecture 22**

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

That the subjects level can be changed to a lower security level

1. Are the subjects considered trustworthy?

No, the subjects are not considered trustworthy.

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

The ring policy assumes that the subject can filter reading high integrity information from low integrity information

1. Are the subjects considered trustworthy?

Yes, subjects are considered more trust worthy.

**Lecture 23**

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

Both are development catagories, but SD is production confidentiality and ID is integrity

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

So that an object can be moved from development to production.

Can system controllers modify development code/test data?

Yes, system controllers confidentiality and integrity labels dominates those of developing and test data

What form of tranquility underlies the downgrade ability?

The down grade ability requires an object to change levels from development to production

**Lecture 24**

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

The purpose of the four concerns is to have integrity in commercial scenarios

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

Bank balances and bank checks  
3. What are some possible examples of UDIs in a commercial setting?

A piece of candy from a restruant or bank  
4. What is the difference between certification and enforcement rules?

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

Human resources, payroll, {corporate bank account, employee bank acount}

**Lecture 25**

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

Their is a conflict of intrest that could potentially spill trade secrets.

1. 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, you should still be able to because GM and Microsoft are in the same conflict group

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

Files are available for access if the subject is in the company or if the subject hasn’t worked for a company in the same conflict group in the past

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

The access control levels change dynamically over time based on the subjects history, and is designed to address a very specific problem

**Lecture 26**

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

In a large organization there can be thousands of subjects, so we can catagorized the subjects with similar jobs into the same access levels

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

Active roles is a subset of authorized roles (some of which just might not be used at all times)

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

Role authorization is a subjects active role must be an authorized role for that subject, and a transaction authorization says that a subject can execute a transaction only if the transaction is authorized for one of the subjects active roles.

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

It is harder to catagorize each subject in SAC policies, and has a harder time giving subjects various roles/change roles

**Lecture 27**

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

Because in alot of realistic systems, most subjects don’t have access to any or very many objects. It is difficult to find and change access levels

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

Access control list, capability based system, de facto permission

**Lecture 28**

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

1 bit transmitted between the two parties (0=no, 1=yes)

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

With covert channels, you want to know how much information you can transmit in a certain amount of time. So you can know what the sender is sharing with you (should 0 be encoded to be yes or no?)

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

They have to have the same encoding scheme in order to understand the data transmitted (otherwise no communication can occur).

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

It would take a longer time to transmit and could be sharing unnecesary information.

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

0 bits, because the sender doesn’t even need to send an answer if the reciever already knows it.

**Lecture 29**

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

n-bits, 4 bits, 7 bits.

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

Because you only need the number of bits needed to label each diffferent message apart from eachother.

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

4 bits. Because 2^4 =16 total different combinations

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

8 bits of information

1. Explain why very few circumstances are ideal, interms of sending information content.

You often don’t know what information you are sending in advance (how many possible messages would be sent)

**Lecture 30**

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

Either a binary digit (discrete) or a quantity of information (continuous)

1. Construct the naive encoding for 8 possible messages.

3 bits used, using all different encodings using 1s and 0s.

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

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

On average 995 of the 1000 messages will be sending a “10” and their will be 5 other messages (each of 5 bit length)

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

You can use less bits to encode messages that occur more frequently.

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

111111, 0000000, 1010101, 111000 is worse than the naive encoding

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

There are limits of the optimal encoding, and it would require you knowing the probabilities of all of the messages beforehand.

**Lecture 31**

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

2, 4, 6, 8, 10, 12…..

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

0, 1, 01, 10, 001, 010 (is non-prefix free)

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

So that each code only corresponds to one message/output

4. Why is a lossless encoding scheme desirable?

Because it is possible to recover the entire origonal sequence of symbols from the transmission.

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

Because more code would require looking ahead in parsing. It would be difficult to determine the difference between an S and three E’s (ie Streaming)

**Lecture 32**

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

Entrophy = -(8 \* 1/8 log(1/8)) = 3

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

T (4/5) H (1/5). –(4/5log(4/5) + 1/5log(1/5)) = .7215

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

Entrophy sets a lower limit on encoding effiency

**Lecture 33**

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

HH (3/4 \* ¾), HT and TH (1/4 \* ¾), TT (1/4 \*1/4)

9/16 3/16 1/16

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

(9times\*0bits) + (3times\*2bits) + (3times\*3bits) + (1time\*3bits) = 27 bits

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

Each of the outcomes has a 3 bit encoding

1. What is the entropy of this language?

~2.1141

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

Encode rolling the following numbers to the following bits.

(1, 0), (2, 10), (3, 110), (4, 1110), (5, 11110), (6, 11111)

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

The numbers rolled that have higher probability use less bits. This is better because the outcomes that are more likely require less bits.