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, because the BLP model follows the policy that information can flow from S1 to S2 if S2 dominates S1.

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

Information cannot flow between either as neither dominates the other.

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

No, because according to the definition of a NI policy, Higher level subjects cannot interfere with lower level subjects.

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(low) -> B(low)

A(low) -> B(high)

Lecture 18

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

NI policies are very general and don't describe the actual mechanism in order to achieve the metapolicy.

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

l2, l3, . . . , lk?

L would only be able to view information of the 'l' actions. Therefore, it would see l1, l2, … lk.

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

It requires identifying within the view function all potential channels of information. Some interferences are benign, etc.

Lecture 19

1. Explain the importance of integrity in various contexts.

We want people to be able to trust the source of information, ie. a General's orders, a newspapers sources, etc.

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

Commercial software may give more security liability to the company that wrote the software.

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

Separation of Duty is the principle that several *different* subjects must be involved to complete a function. Separation of Function is the principle that a subject cannot complete complementary roles in a function.

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

Recovery and accountability. If something bad happens you can pinpoint the issue.

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

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

In a company

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.

High reliability, little sensitivity: Meatloaf in the cafeteria on tuesday! -Chef, low reliability, high sensitivity: Al Queda will be having brunch on Tuesday. -Questionable informant.

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

The dominates relationships for integrity are almost exactly analogous to confidentiality. Higher level of trustworthiness dominates lower level of trustworthiness.

3. Construct the NI policy for the integrity metapolicy.

Untrustworthy information should not flow up to more trustworthy subjects.

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

Confidentiality and integrity solve different issues with practically the same model. They both use labels but must be treated separately.

Lecture 21

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

Because Biba’s two properties are analgous to BLP’s two properties. Simple Integrity Policy and Integrity *-Property. Its essentially the opposite of BLP.

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

Neither dominates the other.

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

No.

Lecture 22

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

As soon as a subject reads information lower than their integrity level, they are corrupted and must be moved down to the appropriate integrity level.

2. Are the subjects considered trustworthy?

No.

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

LWM policy does not?

Yes, the Ring policy assumes that the subject can separate low integrity information when writing the subjects own information.

4. Are the subjects considered trustworthy?

Yes.

Lecture 23

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

SD describes the level of confidentiality, whereas ID describes the level of integrity. Therefore SD and ID are orthogonal.

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

System controllers must be able to move information from the development side to the production side.

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

Yes, they can.

4. What form of tranquility underlies the downgrade ability?

Weak.

Lecture 24

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

To keep consistency.

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

Bank balances, checks, etc.

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

Candy taking from a bank.

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

Enforcement constrains actions, certification constrains results.

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

{Teller, TP, {Account Information}}

Lecture 25

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

breach of confidentiality if also hired by United Airlines?

Information privy to American Airlines may be at risk when consulting for United Airlines. There is a conflict of interest.

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.

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

access according to the simple security rule?

Companies that are not a part of conflict class with microsoft of GM.

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

The Chinese Wall policy addresses a very specific concern, whereas BLP is a much more general policy.

Lecture 26

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

subjects?

More applicable to commercial environments. There may be thousands of people that fill one type of role; therefore, handling their permissions based on that role is more efficient and easier to manage.

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

Authorized roles are functions that a subject can take on during a day or month, etc. Active roles are a subset of authorized roles.

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

Transaction authorization are a set of actions a subject is permitted to take.

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

Standard access control policies are harder to apply than RBAC to a commercial setting. RBAC is also a much more flexible policy to manage.

Lecture 27

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

It requires a large amount of space and can easily be computed on the fly instead.

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

1, maintain a set of rules to compute access permissions based on attributes of subjects and objects.

2. Access control list.

3. 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 know how to interpret the information. Therefore, they must have a previously agreed upon value for yes and no.

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

To measure the bandwidth of information.

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

Because no communication can occur if there isn’t a previously agreed upon encoding scheme

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

Sending more information than necessary can increase the security risks.

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

1, because 1 bit can differentiate between 2 different answers.

Lecture 29

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

n-bit binary number: n-bits.

single decimal digits: 4 bits.

two decimal number: 7 bits.

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

It depends on if the amount of different times an attack could occur. dawn or dusk: 1 bit, any time of day ? bits.

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

4 bits.

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 information content.

Most of the time we don't exactly know all the possibilities of a message that can be sent.

Lecture 30

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

either a binary digit (discrete piece of information), or a quantity of information (continuous).

2. Construct the naive encoding for 8 possible messages.

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

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

for bit zero, if the bit is zero we know it is message ten. Every other message has a 1 for bit zero. Therefore, if on average we send message ten 99.5% of the time, then we will send 995 '0''s to represent message 10. The other 5 times require 25 bits because 5 messages require 5 bits.

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

We can reduce the number of bits needed to represent more probable messages and use a higher number of bits to represent a less probable message. Therefore, on average we should expect to send less bits than using simply a naive encoding.

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

4 bits. message #1: 0001, message #2: 0010, message #3: 0100, message #4: 1000.

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

It means it is the best encoding we could possibly have, and therefore could never do better.

Lecture 31

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

“242244486868668”

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: 101.

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

We want only one possible message output for a message input. Therefore, there are no other possibilities when decoding.

4. Why is a lossless encoding scheme desirable?

There is no degradation of information. In other words, all original information should be recoverable.

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

Morse code is not streaming.

Lecture 32

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

h = log8 = 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 = -(⅘*log(⅘) + ⅕*log(⅕) = .72.

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

You can compute the best possible encoding for a language.

Lecture 33

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

Each flip is independent of the other flips.

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

We are using 1 bit 9 times for HH, 6 bits 3 times, 9 bits 3 times, and 3 bits 1 time.

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?

(9/16×log(9/16)/log(2)) + 2(3/16*log(3/16)/log(2)) + (1/16*log(1/16)/log(2))

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

HH 0, HT 10, TH 110, TT 111.

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

Uses less bits on average.