Name: Vincent Nguy

EID: vn2863

CS Login: vn2863

Email: nguyvincent@yahoo.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, BLP as a MLS policy would imply its transitive by definition, but not all non-interference policies are transitive.

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

There would be no connection between A or B since no one dominates another.

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

Yes covert channels can still exist, The policy is as strong as how you characterize “view”. The more things that you consider to be within the view of the user, the stronger the policy. For example, if you include within a subject’s view the values of system flags, then they could not be used in a covert channel.

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 = high, low

B = low

# Lecture 18

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

The policy is really broad just that information may flow from L to H. There’re no rules about which subject can read/write or such actions. It’s really abstract.

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

l1, l2, l3, l4, …..,lk. Only the actions of l

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

In a realistic system there are many “interferences”

# Lecture 19

1. Explain the importance of integrity in various contexts.

Separation of Duty- several different subjects must be involved to complete a critical function.

Separation of Function-a single subject cannot complete complementary roles within a critical process.

Auditing-recoverability and accountability require maintaining an audit trail.

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

Integrity is a frequently more important in commercial settings so the software would cater to that more

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

Separation of duty splits the completion of a function between different subjects.

Separation of Function says a single subject cannot complete complementary roles within a critical process.

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

If there was a breach we can roll back or fix the problem.

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

Users will not write their own programs, but use existing production software.

Programmers develop and test applications on a nonproduction system.

Moving applications from development to production requires a special process.

This process must be controlled and audited.

Managers and auditors must have access to system state and system logs.

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

A newspaper wanting to check the integrity of their 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.

Expert:{Physics}

Student:{Physics, Art}

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

In the first one Expert > Student, and Physics is a superset of Physics = Yes

Novice < Expert, but {Physics, Art} is the superset of {Physics} = no

Student > Novice, and {Art} is the superset of {} = Yes

1. Construct the NI policy for the integrity metapolicy.

Don’t allow bad info to “taint” good information, don’t allow information to flow up.

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

You have to treat them as separate issues.

# Lecture 21

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

The simple security and \*-prop are opposites in Biba when compared to BLP.

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

Because the set labels in Subj3 and the set of labels in Obj3 are no supersets of one another. So no one dominates another.

1. 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?

A subjects integrity is corrupted when it read information lower then the subjects level should be lowered.

1. Are the subjects considered trustworthy?

No

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

The subject has the common sense to filter out bad information.

1. Are the subjects considered trustworthy?

Yes.

# Lecture 23

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

No.

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

Without it BLP and Biba has no policy to do something like downgrade.

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

Yes. Since he can downgrade.

1. What form of tranquility underlies the downgrade ability?

Weak tranquility.

# Lecture 24

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

Authentication, Audit, well-formed transaction, separation of duty

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

Bank balances, checks.

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

Candy from the candy bowl at a bank

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

Certification mostly checks if the 4 fundamental concerns are valid. Enforcement deals with modification only

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

(me, check balance, {my account})

# Lecture 25

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

They are both in the airline industry and would end up in the same conflict class.

1. 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. Those two are not in the same conflict class.

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

Anything in a different conflict class then GM + GM.

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

The permissions change dynamically. Your access rights depends on your history.

# Lecture 26

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

It’s easier to manage. A subject can now transition between roles without having to change identities.

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

Authorized roles, which it is allowed to fill at various times;

Active roles, is which it currently occupies.

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

Role authorization – A subjects active role must be an authorized role for that subject

Transaction authorization – A subject can execute a transaction only if the transaction is authorized for one of the subject’s active roles.

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

RBAC is more flexiable i.e. RBAC allows a subject to transition between roles without having to change identities.

# Lecture 27

1. Why would one not want to build an explicit ACM for an access control system?
2. Name, in order, the ACM alternatives for storing permissions with objects,storing permissions with subjects and computing permissions on the fly.

# Lecture 28

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

There must be one bit of data.

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

If someone wants to use a covert channel.

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

No communication would occur. It would be just random information if they did not use the same encoding scheme

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

Because the sender wants to send the message as efficiently as possible, and less bits means less time required to send the message.

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

Still one bit.

# 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?

It depends on how the receiver and senders agree on a style of encoding.

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

4 bits because that’s how many bits it takes to represent one of the 16 messages 2^4 = 16

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

8 bits.

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

In most communication scenarios the sender/reader don’t know all the possible messages that could be sent.

# Lecture 30

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

A bit can be a binary digit(discrete) its either 0 or 1.

A bit also is a quantity of information it’s a (continuous).

1. Construct the naive encoding for 8 possible messages.

0 - 000

1 - 001

2 - 010

3 - 011

4 - 100

5 - 101

6 - 110

7 - 111

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

Given the 1000 messages on average 995 of them will be message 10 of the 16 messages. In this encoding all but messages 10 uses 5 bits and 10 is just 0 so 1 bit. Then you can take (995\*1) for all the message 10s and add with (5\*5) for the other 5 messages.

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

you can calculate the number of bits required for the message.

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

1000, 0100, 0010, 0001. This requires 4 bits, while the naïve only needs 2.

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

If you can transmit your message using fewer bits.

# Lecture 31

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

“2468”

1. 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

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

If it’s not unique the message would be ambiguous and possibly could be decoded incorrectly.

1. Why is a lossless encoding scheme desirable?

If else you could lose part of the original message.

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

It fails the prefix-free property.

# Lecture 32

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

H = -8(1/8\*log(1/8)) = -(log(1/8))

1. 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\*log(4/5)) + (1/5\*log(1/5)))

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

It sets a lower limit on encoding efficiency. We can measure the efficiency of the encoding and we can’t do any better than the entropy that matches the encoding.

# Lecture 33

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

They want to give the most efficient encoding to the probability that appears the most. Since HH appears 9/16 its code is 0, and TT is only 1/16 its code its longer 111.

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

HH – 0, HT – 10, TH – 110, TT – 111.

HH appears 9, HT appears 3, TH appears 3, TT appears 1.

(9\*1)+(3\*2)+(3\*3 )+(1\*3) = 27

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

000, 001, 011, 100, 101, 111

1. What is the entropy of this language?

H = -(2\*((3/11)log(3/11))+ 2\*((1.5/11)log(1.5/11))+ 2\*((1/11)log(1/11)))

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

1 0

2 10

3 110

4 1110

5 11110

6 11111

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

It has a better entropy. On average uses less bits.