UTEID: dpk326;
FIRSTNAME: David;
LASTNAME: Ko;
CSACCOUNT: davidko;
EMAIL: davidpeterko@gmail.com;

CS361 Questions: Week 2
These questions relate to Modules 4, 5, 6 and 7. Type your answers and submit them on Canvas by 5pm on Thursday, June 18.

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 a NI policy coul dbe s1->s2->s3 which is not compliant with the BLP since there is no arrow from s1->s3.

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

The information would have to flow one way, so depending on which has more precedence, crypto or nuclear, the policy could be A -> B, or B -> A.

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

No, because the policy dictates whihc way information flows to eliminate covert channels.

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 be low, and B could be high.

Lecture 18
1. Why do NI policies better resemble metapolicies than policies?

The BLP metapolicy resembles the NI policy in the way that information flow from L to H but not vice versa. The NI policy closely mimics the confidentiality metapolicy as well. Theres no rules about which subjects can read/write such objects. In fact, nothing about objects or actions at all.

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

L can only see L, so it would see l1, l2, l3,.. lk.

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

Realistic systems have many potential interferences.

Lecture 19
1. Explain the importance of integrity in various contexts.

Integrity is who can write or modify information. We see who is authorized to supply or modify data, how to separate and protect assets, how to detect and/or correct erroneous or unauthorized changes to data, and to see if authorizations can change over time.

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

a Software that sells commercial software has more reliability and integrity than a software that is free since more work and R&D has gone into the commercial software, therefore making it have more integrity. Also users will not write their own programs, but use existing production software.

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

Separation of duty is when several different subject must be involved to complete a critical function. And the different with seprateion of function is that a single subject cannot complete complementary roles within a critical process.

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

Auditing allows recoverability and accountability and it requires maintaining an audit trail.

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

Users cannot write their own programs and must use existing production software. Programmers develop adn test applications on a nonproduction system, possibly using contrived data. Moving applications from development to production requires a special process. This process must be controlled and audited. Mangers and auditors must have access to system state and system logs.

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

In the commercial world, using a paid software that is commercial and proven is more important than a program that is free and open source, since the code will not have been compromised even if the information isnt.

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.

Highly reliable would be some article from a newpaper from a reputed paper. A high reliable with greater sensitivity would be a banks hold on your bank information.

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

On the first row, the expert dominates the student with the same object, physics. ON row two, the label 2 dominates label 1 since expert > novice, but physics is a subset of physics, art so neither dominate. On row 3, the novice domiantes the student but the unclassified is a subset of art so neither dominate.

3. Construct the NI policy for the integrity metapolicy.

A low integrity subject writes bad information into a high integrity object, or a high integrity subject reads bad information form a low integrity object.

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

They are similiar, but htey both ahve their own unique properties that makes them separate entities.

Lecture 21

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

It is the dual because it implements the opposite ideas of the BLP model. The relations are reversed.

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

They have the same dominance, but the sets are completly different, so neither dominates.

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

It depends because the confidentiality and integrity labels are complete separate from each other and do not affect one another.

Lecture 22

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

The subject level becomes that of the obejcts if it reads below.

2. Are the subjects considered trustworthy?

They are considered trustworthy only if they read from a lower source and are made to that objects level. otherwise if it reads from a lower unreliable source it will not be reliable if it says the same level. So it is made to the objects level if it reads it.

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

It is more trustworthing in the Ring policy and trusts the subject ot be able to filter the bad information if it reads lower than its own level.

4. Are the subjects considered trustworthy?

In all of the Biba's 3 policies, the subject are precluded from writing up in integrity. The subject is only trusted if it can filter the information it receives.

Lecture 23

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

Yes an SD must have ID.

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

To be able to transfer program and codes from development to the common level

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

No

4. What form of tranquility underlies the downgrade ability?

Being able to change the label

Lecture 24

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

To make sure the security is there and confirmed

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

bank account, checking account, debit/credit

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

business cards, free items on a counter

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

certification checks the preconditions before performing, and enforcement is checked during

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

(user x, deposits y item, {safety deposit box})

Lecture 25

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

The consultant could give information about AA to UA that he left with.

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, unless the file you accessed at GM is in conflict with the file you acceeessed with Microsoft.

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

You can access anything that is not in direct competition or conflict with the opposing company.

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

The Chinese Wall policy changes the permissions for files dynamically in relation to the subjects history.

Lecture 26

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

Roles can be easily changed and priviledges can be easily changed.

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

authorized role are roles they are allowed to be and active roles are roles that they are doing right now

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

A role authorization is when an active role is authorized for the subject and a transaction authorization can only be done if the

action is within the actions of the active role.
4. What disadvantages do standard access control policies have when com- pared to RBAC?
A disadvantage would be giving a subject more priviledges that would be difficult to manage or do.

Lecture 27
1. Why would one not want to build an explicit ACM for an access control system?
It is a waste of time
2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.
Storing permissions on with object: ACL. Storing permissions with subjects: capabilities. Computing permissions on the fly: no name.

Lecture 28
1. What must be true for the receiver to interpret the answer to a “yes” or “no” question?
The receiver must know both the answers for yes and no. Like the associated bit.
2. Why would one want to quantify the information content of a message?
Maximize bandwidth
3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
If both parties know the proper encoding scheme, then there is no confusion or wrong interpretation of the data.
4. Why wouldn’t the sender want to transmit more data than the receiver needs to resolve uncertainty?
It could cause an overflow of data for the receiver.
5. If the receiver knows the answer to a question will be “yes,” how many bits of data quantify the information content? Explain.
The data can be quanified using 1 bit, a 0 or 1.

Lecture 29
1. How much information is contained in each of the first three messages from slide 2?
The first is n bits, the second 4 bits, and the third 7 bits.
2. Why does the amound of information contained in “The attack is at dawn” depend on the receiver’s level of uncertainty?
Depending on the level of the receivers uncertaininty, we can only know that the attack will be at dawn.
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
Usuing a common shared encoding, it can be 4 bits (up to 16 total).

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

256 is 100000000, so 9 bits worth.

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

because the balanced binary trees do not exist at all times.

Lecture 30

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

A bit can mean a binary bit or a quantity of information.

2. Construct the naive encoding for 8 possible messages.

000 001 010 100 101 110 111

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

We get the first bit which is 1, then we wait. If we dont get anything then we recognize that it works with a 0.

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

We can reduce the number of bits sent for a messege.

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

000001 for 1, 100000 for 2, 111000 for 3, 101010 for 4.

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

Using an optimal coding, every problem can be minimized or reduced.

Lecture 31

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

2424242.

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

-no prefix
1 - 0000000 a 3 bit encoding scheme for 1-6 with 4 zeroes added in the front with trailing values
2 - 0000001
3 - 00000011
4 - 000000111
5 - 0000001111
6 - 00000011111

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

If you keep it non-unique, then someone can figure out the decoding.

4. Why is a lossless encoding scheme desirable?

So the person figuring out the decoding cant differentiate a value from a bit encoding.

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

Not lossless.

Lecture 32

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

h = -(1/2 * log 1/2 + 1/2 x 1/2) = 1 for 1/2 prob. so for 8 sided die, - 8 * (1/8 * log 1/8) = 0.90308998699

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 = -(1/5 * log(1/5)) + 4/5 * log(4/5) = -(-0.13979400086 + -0.0775280104) = 0.21732201126

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

It tells your the limitations of the system.

Lecture 33

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

You would get the probabilities by multiplying the answers

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

length of the code * count

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

0 = 1 and 2, 1 = 3 and 4, 2 = 5 and 6.

4. What is the entropy of this language?

h = - (2 *(1/6 * log(1/6)) + 2 *(1/6 * log(1/6)) + 2 *(1/6 * log(1/6)))

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

using a bit sequence we can make the encoding liek this:

1 - 0
2 - 10
3 - 110
4 - 1110
5 - 11110
6 - 111110

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

Each encoding is unique and provides a way to identify each value.