Name: Ali Khan
EID: aak849
CS Login: alikhan@cs.utexas.edu
Email: alikhan2010@live.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?

   It is possible to take any MLS policy (including BLP) and turn in it into a a Non-interference policy. A BLP may not necessarily comply with a non-interference policy because of the possible existence of a covert channel that contradicts the meta policy of an NI policy

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

   Because there is no dominance relation between A and B, the NI policy does not articulate a flow of information between the subjects

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

   Theoretically if it is confirmed that a low level subject's scope/view cannot observe a high level's subjects action, then a covert policy cannot exist and therefore meets the NI metapolicy. But if a covert channel exists then both the meta-policy is violated and the policy is flawed

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 -> B in an NI policy implies that the level of B dominates the level of A which necessitates B>A. B: High, A: Low

Lecture 18

1. Why do NI policies better resemble meta-policies than policies?

   NI's policy of L |—> H mimics the confidentiality the confidentiality meta-policy that information may flow from L to H but not vice-versa. NI's advocacy of the constraint of flow of information is resembled both in the policy and meta-policy

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

   L's view in an NI policy framework would be the same in the two aforementioned situations. L's scope is limited to an area that H's actions cannot affect

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

   Realistically NI is difficult to prove given the myriad of interferences in a real system. Most of these interference involve low-level system attributes.

Lecture 19

1. Explain the importance of integrity in various contexts.

   Integrity of information is important when attempting to confirm various types of news. For example, if one news agency claimed there was some conflict going on abroad, the trustworthiness of that agency becomes pertinent when I make the decision to believe that piece of information.

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

   A commercial piece of software has some form of certification that garners it more credibility than a freeware software whose origins and credibility are unclear

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

   Separation of duty involves multiple people performing a critical function for the sake of redundancy i.e. two banker's signature is necessary to authenticate a check. Separation of function involves restricting one person on working on two different complementary parts of a system which is aimed at a checks and balances system.

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

   It is important for accountability and recoverability standards

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

   Lipner raises integrity concerns in the context of software production. His argument is that there need to be some form control and oversight on what is put through the pipeline of production. This pipeline should be controlled and audited with various employees having access to the system state and system logs

CS361 Questions: Week 2 2

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

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.

   A quantam physics book from an esteemed Harvard professor is highly reliable but with little sensitivity as it is open to the public whereas documents created in congress by politicians are not so highly reliable (because politicians are buffoons) but have greater sensitivity as the public does not always have access to them

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

   In row 1 an expert physics professor has the trustworthiness to "write" information into the student of physics. However, a novice in physics and arts does not have the trustworthiness to "write" information to an expert in physics (row 2). Finally in row three a student in art has valuable information she can "write" to the novice.

3. Construct the NI policy for the integrity metapolicy.

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

   The labels in a confidentiality system would be the inverse of the labels in an integrity system. For example a high level subject that can write to a low level subject in an integrity system describes the read relationship in a confidentiality system.

Lecture 21

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

   As mentioned before, Biba integrity is orthogonal to the BLP model. This is observably noticed in an access control matrix where all the the "Read" access in a Biba matrix would "Write" access in a BLP matrix

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

   {A,B} is not a superset of {B,C} therefore no dominates relation exists. A dominance relation would articulate the read/write relation but because one does not exist, there is no relation.

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

   If you are combining both BLP and strict integrity, then an access is allowed only if allows by both Biba rules and BLP rules. But if the system is only subscribing to BLP rules, then the subject can access the object

Lecture 22

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

   The low water mark policy assumes that a high level subject's credibility/ integrity is diminished when reading the unreliable content of a low level object

2. Are the subjects considered trustworthy?

   LWM does not put much credit into the subject as it assumes that the subject's integrity can be adulterated by a low level object. Consequently, a subjects trustworthiness is predicated on the content they have previously read

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

   Yes; the ring policy assumes that a subject can filter out bad/unreliable information. Consequently, the integrity of a subject should remain unaffected when reading a low-level object

4. Are the subjects considered trustworthy?

   A subject is given more credit in the ring policy. Any subject can read anything regardless of integrity information because the assumption is that a subject cannot be demoted by bad information

Lecture 23

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

They are related in that they manipulate the same information (that being the programs under production). They are different in that SD articulates who is allowed to view the production and ID articulates who can write to production.

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

So that after a software meets all necessary standards the controller has the ability to move software from development to production.

CS361 Questions: Week 2 3

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

Yes because they have both the IP and ID integrity labels

4. 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?

Clark and Wilson argued that commercial security has its own unique concerns and merits a model crafted uniquely for that domain. The overriding concern was consistency. Consequently, the goal of the four fundamental concerns was that established a system that met the aforementioned framework.

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

The balance of a customer's checking account, account history of a retail site, and credit card information.

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

The user interface of a web application, content about the company's philosophy on the website, and time information on a website

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

Enforcement is the implementation of various certification rules

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

As a software engineer, the permission to commit code to the trunk or original code

Lecture 25

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

   There would possibly be a conflict of interests given both airlines are direct competitors and would divulge sensitive information in their consultancy. The risk that the sensitive information divulged gets into the wrong hands increases when there is a conflict of interests

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 Microsoft and GM are not in the same conflict class. You will be barred from accessing companies like Ford but not Microsoft.

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

   A subject s can be granted access to an object o if the object is in the same company datasets as the objects already accessed by s <u>or</u> belongs to an entirely different conflict of interest class.

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

   The Chinese Wall Policy is designed <u>specifically</u> to address conflicts of interest by a consultant or contractor whereas BLP may be a more intra-company confidentiality system

Lecture 26

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

   Assigning permissions with roles may be a lot more robust than with assigning it with subjects. This is true because subjects are constantly changing roles by being promoted or switching departments. Rather then changing the entire security protocol you simply change the role of the subject

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

   An active role is the what the subject currently occupies whereas authorized roles are the potential roles that could be filled at various times

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

In role assignment a subject can execute a transaction only if the subject has an active role where as role authorization necessitates that a subject's active role must ben an authorized role as well for that subject

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

   RBAC is a lot easier to manage given that everyone in the same role has the same permissions. Furthermore, RBAC recognizes that a subject often has various functions within an organization. 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?

   ACM's for real world systems may be too cumbersome to create. Additionally, there are reasonable alternatives that are a lot more scalable and that maintain rules on the fl based on attributes of subjects and objects i.e. an Access control list.

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

   Access Control list and a capability based system

Lecture 28

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

   There must be some mechanism that allows the recipient to distinguish between the two responses. This can be reconciled with more data or an additional bit of data. Furthermore, if there is some form of shared knowledge that can be referenced to distinguish the two responses

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

   To interpret the data and the analyze the potential for that channel to send other forms of data i.e. the capacity of channels on which information may flow

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

   For information to be sensical, there has to be a consistent message form which can be referenced from some shared knowledge

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

   It has the risk to increase the amount of uncertainty

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

Simply the amount of bits required to convey yes

Lecture 29

1. How much information is contained in each of the first three messages from slide 2? **24, 23, 27**
2. Why does the amount of information contained in "The attack is at dawn" depend on the receiver's level of uncertainty?

   How the receiver parses the information dictates the amount of information contained within the message. Depending on the uncertainty, it could provide a lot of information or little to no information at all
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?

   4, because that is the shared information articulated
4. How much information content is contained in a message from a space of 256 messages?

   Log2(256)
5. Explain why very few circumstances are ideal,interms of sending information content.

   To get a realistically efficient transmission the sender and receiver must know in advance the space of possible transmission and have an agreed on an encoding. Furthermore, the receiver's level of uncertainty ought to be sufficient enough to decipher the message

Lecture 30

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

   One argument is that it is a binary digit (discrete) and the other is that it is a quantity of information (continuous)
2. Construct the naive encoding for 8 possible messages.

- **M0: 0000**
- **M1: 0001**
- **M2: 0010**
- **M3: 0011**
- **M4: 0100**
- **M5: 0101**
- **M6: 0110**
- **M7: 0111**
- **M8: 1000**

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

Given 1000 messages, on average 995 of them will be message 10, and 5 will be other messages

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

   Computing the number of bits per message depends on knowing the prior probabilities thereby increasing efficiency if you have prior probabilities

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

- **M0: 00001**
- **M1: 10001**
- **M2: 10010**
- **M3: 10011**

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

   That we have some reasonable form of insight on prior probabilities

Lecture 31

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

Number of feet in the city of Austin (assuming there are no one legged people and this excludes 0)

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

000,001,010, 011, 100, 101

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

So you can property decipher the data

4. Why is a lossless encoding scheme desirable?

Avoiding redundancies and have prefix-free data

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

Because it does not user fewer inputs for the symbols that occur more frequently

Lecture 32

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

   Log8

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

   .217

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

Entropy sets a lower limit on encoding efficiency which is important information

Lecture 33

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

Slide 3 simply presents compounded probabilities pairs of flips which makes sense given the misbalance favoring heads

CS361 Questions: Week 2 6

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

   That is how many bits it would take to reflect all possibilities presented in the dual flip example