Name: Ali Pasha
EID: aap2493
CS Login: alipasha
Email: alipasha@utexas.edu

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 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, because non-interference demand that Sh must never communicate with Sl (i.e. there shouldn't be anything that Sh can do that has effects visible to Sl). But under BLP, this is possible.

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

> A and B may only "interfere" with themselves, but not with each other since neither dominates the other.

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

> Assuming the NI policy is strong (the view is very inclusive) then there should be no methods of sending information in violation of the policy, including 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: low, B: high), (A: high, B: high), (A: low, B: low)

Lecture 18

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

> Because NI policies are very general and abstract.

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

> Under NI, it should be l1, l2, l3, … , lk

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

> Because interferences are very common in real systems.

Lecture 19

1. Explain the importance of integrity in various contexts.

   Who is authorized to supply or modify data?
   How do you separate and protect assets?
   How do you detect and/or correct erroneous or unauthorized changes to data?
   Can authorizations change over time?

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

   It’s due to the assessment of the integrity of source. A certified application, as most commercial software likely is, may have more integrity than freeware downloaded from the internet.

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

   Separation of duty requires several different subjects to be involved with a critical task while separation of function means that the same subject cannot be involved with more than one critical task.

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

   If something bad happens, an object gets corrupted, auditing allows us to go back and see when and why it happened, and possibly correct it.

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

   Corruption through external data

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

   Maintaining a secure bank account.

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.

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

   Row 1: Expert > Student, and {Physics} is a subset of {Physics}, therefore Label 1 dominates Label 2.
   Row 2: Novice < Student, therefore Label 1 doesn’t dominate Label 2.
   Row 3: Student > Novice, and {} is a subset of {Art}, therefore Label 1dominates Label 2

3. Construct the NI policy for the integrity metapolicy.

   Don’t allow information to “flow up”.

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

It basically means that they run counter each other. That is, what one allows is exactly what the other is trying to avoid.

Lecture 21

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

Like BLP, Biba Integrity is a mandatory access control policy, and all you need to do is switch the arrows of the information flow in BLP to get Biba Integrity.

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

Because neither dominates the other.

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

If both BLP and Biba are being used, then no.

Lecture 22

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

Subjects can be trusted to read only what they are allowed to.

2. Are the subjects considered trustworthy?

Yes, but a subject’s integrity level falls if it ever reads low integrity information.

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

Yes, that the subject will filter out and not read low integrity information.

4. Are the subjects considered trustworthy?

Yes, more than in LWM since there is no consequence of reading low integrity information.

Lecture 23

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

Yes, they are both “programs under development” categories.

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

Because system controllers need to be able to move products from development to production.

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

No.

4. What form of tranquility underlies the downgrade ability?

Warm tranquility.

Lecture 24

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

The overriding concern is consistency among the various components of the system state.

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

Bank accounts, student grades in registrar at private university

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

Ads on a website

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

Certification ensures that all actions to CDIs are valid and preserve their integrity, while enforcement restricts the actions themselves in order to preserve the integrity of the CDIs.

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

(John, withdraw, {John's checking account, John's savings account}).

Lecture 25

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

Business strategies used by one airline can be very valuable to another airline.

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 GM and Microsoft are elements of two different conflict classes.

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

Only one company from each conflict class. Therefore, access is available to GM (and no other in its conflict class), Microsoft (and no other in its conflict class), and any one company from the third set.

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

Unlike previous policies, Brewer and Nash's Chinese Wall Policy is designed to address a very specific concern: conflicts of interest by a consultant or contractor.

Lecture 26

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

Allows for more generality, and allows for a subject to take on multiple roles.

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

Authorized roles are those that the individual is allowed to fill at various times while active roles are those that the individual currently occupies.

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

Role authorization means that a subject must be authorized for the subject’s active role, while transaction authorization means that subject can execute a transaction only if the transaction is authorized for one of the subject’s active roles.

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

Not as flexible as RBAC. Cannot give a subject various functions within an organization for example.

Lecture 27

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

Because it is not practical and expensive for most real systems.

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, Capability-Based System, and maintaining a set of rules to compute access permissions based on attributes of subjects and objects.

Lecture 28

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

Sender and receiver must have some shared knowledge, included an agreed encoding scheme.

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

To be able to determine how much information can be transmitted over a specific covert channel.

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

To be able to decode and receive the message.

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

Transmitting more data than is necessary is an unnecessary risk.

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

  0 bit of data, because the receiver has no uncertainty.

Lecture 29

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

  n-bit: n bites, single decimal digit: 4 bits, two digit decimal number: 7 q bits

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

  Because it depends on what question “The attack is at dawn” is answering for the receiver.

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?

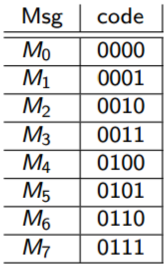
5. Explain why very few circumstances are ideal, in terms of sending information content.

Lecture 30

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

  bit1: a binary digit (discrete), bit2: a quantity of information (continuous).

2. Construct the naive encoding for 8 possible messages.



Msg	code
M_0	0000
M_1	0001
M_2	0010
M_3	0011
M_4	0100
M_5	0101
M_6	0110
M_7	0111

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

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

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

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

Lecture 31

1. Name a string in the language consisting of positive, even numbers.
“246824682468…”

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

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

4. Why is a lossless encoding scheme desirable?

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

Lecture 32

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

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

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

Lecture 33

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

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

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

4. What is the entropy of this language?

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

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