CS361 Questions: Week 2

Name: Zhenyu Zhu

Date: 6/16/2014

EID: cike

CS login: zhenyu

Email: zhu_zhenyu@utexas.edu

HW: #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?

   Yes, because Non-interference policy is more general than BLP model. It is possible to take any MLS policy (BLP model) and turn it into a Non-interference policy; by following the subjects dominate relation.

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

   There is no NI policy for subject A and B in this case.

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

   Yes, depends on L's view of system attributes, if L -> H and the system satisfy the NI policy, by definition of NI policy, unless we include everything L could ever observe, then there is nothing H can use to send information to L, but in reality, H and L always shared some system resource which makes always some possibility of covert channel.

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 is "low", and B is "High"

   A is "low" and B is "low"

   A is "high" and B is "high"

Lecture 18

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

   Policies are set of rules trying to achieve metapolicy. Here in NI, we don’t care about read/write access, objects and actions of subject; it is very abstract compare to other policy. We only care about the information flow, which mimic the confidentiality metapolicy.

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

   Depends on if L -> H satisfied NI policy or not. Assuming it is NI policy. Then we should only see l1, l2, l3…lk… by definition.

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

   To prove there is “non-interference” within the realistic system. To including everything L could ever observe from its view. Because NI theorem refers to all subject, all states, and all instruction sequences and requires an induction that touches every reachable state of the system. And because interferences are very common and involving many lower level attributes in realistic system, some interference is benign. Also very few systems are complete deterministic.

Lecture 19

1. Explain the importance of integrity in various contexts.

   To an auditor in the bank, protecting of integrity is more important.

   To the custom in the bank, who can modified the data is more important.

   To the teller in the bank, how many subjects need to produce the integrity is important

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

   Because the assessment of the integrity of the source. Commercial software usually provides more confidence to us than free version software. Also intuitively, commercial software is developed by a much larger team than freeware, hence less bug.

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

   Separation of duty is several subjects must be involved to complete one critical function. Different subjects might be able to perform the same role in that function. Separation of function is that one person can only perform one role within a critical process.

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

   In case of erroneous or unauthorized changes to the data, the data can be recovered by previous maintaining an audit trail or log, also for the accountability of the data.

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

   Integrity concerns within commercial setting, which commercial security controls are discretionary, procedural, and decentralized. Integrity in various different context, such as who is authorized to supply and modify data, how to separate and protect assets, how do you correct or recover from unauthorized change, etc.

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

   In the commercial setting example from the lecture, which can produce and modified the data in the data process environment is more important than who can see the data. Where integrity concern in this context is more important than confidentiality concern.

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. Information highly reliable with little sensitivity: “movie stars gets married” from an very reliable news source, maybe “CNN”
   b. Not so highly reliable but with greater sensitivity: “rumors about North Korea developed nuclear weapon”, from “internet news source”

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

   a. Row 1, Expert is ≥ Student, {Physics} ⊇ {Physics}, label 1 dominates label 2
   b. Row 2, Novice is ≤ Expert, {Physics, Arts} ⊇ {Physics}, no dominate relation
   c. Row 3, Student is ≥ Novice, {Art} ⊇ {}, label 1 dominate label 2

3. Construct the NI policy for the integrity metapolicy.

   H → L (“read up” , “write down”), metapolicy: don’t allow information flow up

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

   That these two security concerns can be treated by analogy, but they are not really related to each other, we need separate labels for each concerns. Both concerns should be treated either separated or in a mixed policy where only access that pass both tests are allowed. For example, an object can be highly unreliable but very sensitive.

Lecture 21

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

    Because Biba is also a MAC policy and have two very similar rules (simple integrity property, integrity *-property” as BLP model, the only difference is the opposite dominate relation within those two property.

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

    Because there is no dominate relation between Subject 3 and Object 3, they have the same hierarchical first component level, but different unrelated categories.

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

    It depends on which policy the system has. If the system only follows BLP model, then yes, the subject can access the object. If the system follows Biba model, then subject cannot access the object. If the system has to follow both BLP and Biba model, then the subject cannot access the object.

Lecture 22

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

    That the subject’s integrity level falls if it ever reads lower integrity information, also the subject might be corrupted or influenced by the “bad” information. Subject cannot distinguish the reliability of the information.

2. Are the subjects considered trustworthy?

    Not very trustworthy.

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

    Yes, that the subject can properly filter the information it receives.

4. Are the subjects considered trustworthy?

    Yes, much more trusting than LWM and Biba.

Lecture 23

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

   Yes, they are two separated labels within confidentiality and integrity concern, but they are related since they all fall in the same development category, which also contains development code and test data.

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

   Because some process has to be follow to move objects from development to production, and system controller is the only subject who has the proper access for this particular function. Also because only system controller has the highest integrity level (ISP), so he is allowed modifying all the categories assign to him.

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

   No, because confidentiality (BLP) rules do not allow write access to system controller on development code/test data.

4. What form of tranquility underlies the downgrade ability?

   Weak tranquility property.

Lecture 24

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

   To distinguish the different security concerns between a military domain and a commercial domain. To protect confidentiality and integrity of information within commercial domain.

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

   As the Dr. Young mentioned in the bank environment: bank balances of the day, checks

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

   Same bank environment: candy on the bank counter, deposit slip before the counter.

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

   Enforcement are rules design to meet mainly for authentication concerns, where certification rules are for audit, well-formed transactions, and separation of duty concerns.

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

   As in a bank example, permission can be the transformation procedure to allow cashing a personal or company check.

Lecture 25

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

   Because both American Airline and United Airline falls in the same conflict class, they have conflict of interest between these two competing companies.

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, you should be able to access another file from GM, because Microsoft is in a different conflict class with the class than contains GM.

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

   The file should be in the same company datasets as the objects already accessed by subject, in our examples, files in GM and Microsoft. And also belongs to an entirely different conflict of interest class, such as the Bank Class on slides 4 lectures 25.

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

   BLP model is more generalized and for military or multi level security domain, where Chinese wall policy is designed to address a very specific concern: conflict of interest within a commercial domain. Also the permission changes within BLP model has to follow certain tranquility property, where in Chinese wall policy, the permission change dynamically depends on the history of pass access.

Lecture 26

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

   Easy to administer, appropriate to the organization within commercial domain, allows transition between roles without having to change identities and also models separation of duty, easy to audit. It provides a flexible approach to modeling the dynamism of commercial organization.

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

   Authorized roles are the roles that a subject may allow to fill at various time within this organization, an active role is the subject's current role within an organization. Active roles are subsets of authorized roles for the same subject.

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

   Role authorization is a subject's active role must be an authorized role for this subject. Transaction authorization is a subject can execute a transaction only if the transaction is authorized for one of the subject's active roles.

   Roles authorization limited to subject's current active role, and transaction authorization does not limit the transaction to the active role, as long as it is authorized for one of subject's active roles.

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

   Difficult to manage, permission might not be appropriated to the organization. A subject might not perform several functions within the organization and transition of subject between roles is more difficult.

Lecture 27

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

   Because the realistic system might contain too much subject and objects, and most subjects don't have any access to any objects, building an explicit ACM for an access control system is expansive an unnecessary. It is difficult and expansive to store a large and sparse matrix of this sort. In a dynamic system, subjects and objects comes and goes, it requires the ability to add and remove rows and columns.

   It is a lot slower than just to compute access permission on the fly base on some rules or checking capability of subject or Access control list of an object.

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

   ACL (access control list), Capabilities of subject (ticket), implicit rules (simple security, *-property) for different models (BLP, Biba, RBAC)

Lecture 28

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

   Sender must be able to send 1 bit of message across an existing channel. Receiver must have some shared knowledge with sender, minimum an agreed encoding scheme to understand how distinguish 1 bit of information for "yes" or "no".

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

   To get an efficient transmission across the channel, to calculate the bandwidth or capacity of the channel.

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

   Because you have to have that to decode what type of information sender send to receiver via the messages. So receiver can use that to interpret what sender trying to send. Also you need the above to ensure a message can be send along the channel.

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

   Efficient purpose if limited by the bandwidth of the channel. The less data send, the less chance it will be interfere by noise or other factors.

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

   1 bit. Because even is no uncertainty for the receiver on this questions. Sender still have to send 1 bit to let receiver knows there is answer to the question, and $\log_2 0$ = 1

Lecture 29

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

   N bits of information for the first message, 4 bits of information to represent 10 possible choices between 0-9 of the second message, and 7 bits of information to represent 100 possible represent by the third message.

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

   Because different level of uncertainty can be represented by different bits of information needed to be transmitted to clear the specific uncertainty. Such as the time of the attack can be represent differently by dusk/dawn, hours of day, which day of the week, of the month, of the year, by hour, or by minutes or by seconds etc.

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

   4 bits must be transmitted. Because $\log_2 16$ = 4, and because each of the 16 messages can be encoding in a 4 bit string.

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

   8 bits, since $\log_2 256$ = 8.

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

   Because we don’t know how many possible message needs to be sent to resolve the amount of uncertainties. So we don’t have the most efficient transmission, which could be represent by the shortest path on the binary tree.

Lecture 30

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

   Discrete quantity of bit represents the binary digit, and the continuous quantity of bits represents the measure of information content.

2. Construct the naive encoding for 8 possible messages.

   000 M0, 001 M1, 010 M2, 011 M3, 100 M4, 101 M5, 110 M6, 111 M7

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

   Because Message 10 is encode with a bit of 0, and the rest 15 message were encoded by adding a bit 1 to the 4 bit string of naïve encoding. With the “on average” 99.5% message 10 within a 1000 messages, we have 995 chance of message 10, therefore 995 bits, the 0.5% of 1000 message gives us 5 other message within the rest 15 messages, which each has 5 bits, hence it is 995 + 25.

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

   As the example above, knowing the prior probability of messages, we can compute the average information content of a symbol or message using the fewer bits to represent a symbol that occurs more frequently. With the new encoding, we can have a much better bits per message ratio to transmit the message in the language.

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

   00 M0, 01 M1, 10 M2, 11 M3 (naïve)   100 M0, 0 M1, 110 M2, 111 M3 (worse)

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

   Encoding that has the following properties, such as lossless, uniquely decodable, and streaming. If we know the probability of the symbols, we can calculate the entropy of the symbols, which will give us the best possible encoding.

Lecture 31

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

   Symbols for this language: “2”, “4”…. Strings “24648124810365824…”

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

   ROLL 1 – 0
   ROLL 2 – 1
   ROLL 3 – 001
   ROLL 4 – 010
   ROLL 5 – 100
   ROLL 6 -- 101

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

   If not uniquely decodable, receiver might have ambiguous interpretation of the information sender trying to send. One string of code received can mean two or more different set of symbols.

4. Why is a lossless encoding scheme desirable?

   We don’t want to loss of information on receiver end. We might need to possibility to recover the entire original sequence of symbols from the transmission.

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

   Morse code does not have streaming property that we need. There is break in the code sending using Morse code.

Lecture 32

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

   H = - $\log_2 1/8$ = $\log 8$ = 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 = -(0.8*log 0.8 + 0.2*log 0.2) ≈ 0.722

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

   Because entropy of the language is a measure of the information of content of an average symbol in the language, it sets the lower limit on encoding efficiency for this particular language. It is the best bits/symbol for such encoding on language.

Lecture 33

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

   The probability of combination of two independent events (flips) is the multiple of each event's probability. So for HH is ¾ * ¾ = 9/16, HT is 3/16, TH is 3/16 and TT is 1/16. The code bit 0 for HH is because fewer bit for the most appear symbol.

   The goal here is to do better than 1 bit / symbol. So if we sending 1 bit after flipping twice, we might get a better entropy of 1 bit / symbol. (0.844)

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

   It is the sum of the bits needed to have 16 2flips and 4 symbol "HH, HT, TH, TT"'s appearance on average.

   a. HH appear 9 times, and use 1 bit to represent each appearance, so total 9 bits.
   b. HT has 3 appearance with 2 bits represent each, so total of 6 bits
   c. TH is 3 appearances with 3 bit represent each, so total 3*3= 9 bits
   d. TT is 1 appearance represent by 3 bits, so total of 3 bits
   e. 9 + 6 + 9 + 3 = 27

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

   Roll 1 – 000 same as naïve encoding on slide 4 of lecture 31
   Roll 2 – 001
   Roll 3 – 010
   Roll 4 – 011
   Roll 5 – 100
   Roll 6 -- 101

4. What is the entropy of this language?

   H = - (6/20 * log (6/20) + 6/20 * log (6/20) + 3/20 * log (3/20) + 3/20 * log (3/20) + 1/20 * log (1/20) + 1/20 * log (1/20)) ≈ 2.30

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

Roll 1 – 0	6 appearance	6*1 = 6 bits	on average of 20 rolls
Roll 2 – 10	6	6*2 = 12	we have total 50 bits by
Roll 3 – 110	3	3*3 = 9	adding 6+12+9+12+5+6
Roll 4 – 1110	3	3*4 = 12	50/20 = 2.5 bits / per roll
Roll 5 – 11110	1	1*5 = 5	
Roll 6 – 111110	1 1	*6 = 6	

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

   See the above calculation, my encoding has 2.5 bits per roll, where the naïve encoding has 3 bits per roll. And my encoding is more close to entropy of this particular language.