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?
2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?
3. Can covert channels exist in an NI policy? Why or why not?
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?

Lecture 18

1. Why do NI policies better resemble metapolicies than policies?
2. What would be L's view of the following actions: h1, l1, h2, h3, . . . , hj, l2, l3, . . . , lk
3. What is difficult about proving NI for realistic systems?

Lecture 19

1. Explain the importance of integrity in various contexts.
2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?
3. Explain the difference between separation of duty and separation of function.
4. What is the importance of auditing in integrity contexts?
5. What are the underlying ideas that raise the integrity concerns of Lipner?
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.
2. Explain the dominates relationships for each row in the table on slide 4.
3. Construct the NI policy for the integrity metapolicy.
4. What does it mean that confidentiality and integrity are "orthogonal issues?"

Lecture 21

1. Why is Biba Integrity called the "dual" of the BLP model?
2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?

Lecture 22

1. What is the assumption about subjects in Biba's low water mark policy?
2. Are the subjects considered trustworthy?
3. Does the Ring policy make some assumption about the subject that the LWM policy does not?
4. Are the subjects considered trustworthy?

Lecture 23

1. Are the SD and ID categories in Lipner's model related to each other?
2. Why is it necessary for system controllers to have to ability to downgrade?
3. Can system controllers modify development code/test data?
4. What form of tranquility underlies the downgrade ability?

Lecture 24

1. What is the purpose of the four fundamental concerns of Clark and Wilson?
2. What are some possible examples of CDIs in a commercial setting?
3. What are some possible examples of UDIs in a commercial setting?
4. What is the difference between certification and enforcement rules?
5. Give an example of a permission in a commercial setting.

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?
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?
3. Following the previous question, what companies' files are available for access according to the simple security rule?
4. What differences separate the Chinese Wall policy from the BLP model?

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects?
2. What is the difference between authorized roles and active roles?
3. What is the difference between role authorization and transaction authorization?
4. What disadvantages do standard access control policies have when compared to RBAC?

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?
2. Why would one want to quantify the information content of a message?
3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
4. Why wouldn’t the sender want to transmit more data than the receiver needs to resolve uncertainty?
5. If the receiver knows the answer to a question will be “yes,” how many bits of data quantify the information content? Explain.

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?
2. Why does the amound of information contained in “The attack is at dawn” depend on the receiver’s level of uncertainty?
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
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.”
2. Construct the naive encoding for 8 possible messages.
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 naive 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.
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?