John Cade Griffin

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? Yes, you can take any MLS and turn it into NI
2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)? There is none, there is no transmission
3. Can covert channels exist in an NI policy? Why or why not? no because the flow is one way
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
H	H
H	L
L	L

Lecture 18

1. Why do NI policies better resemble metapolicies than policies? Because there isn't the granularity of details on objects
2. What would be L's view of the following actions? h1, l1, h2, h3, . . . , hj, l2, l3, . . . , lk l1, l2, l3 . . . lk just the flow of info
3. What is difficult about proving NI for realistic systems? there are lots of interferences, having a model at a low level of abstraction would be difficult

Lecture 19

1. Explain the importance of integrity in various contexts. separation of duty, seperation of function, Auditing
2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version? the source is more trustworth
3. Explain the difference between separation of duty and separation of function. Seperation of duty calls for mult. individuals, possibly of the same role to complete a task, seperation of function compartmentalizes roles to complete a task, checks and balances
4. What is the importance of auditing in integrity contexts? Auditing allows for the monitoring of the quality of data and the ability to flag errors and designate those responsible
5. What are the underlying ideas that raise the integrity concerns of Lipner? the necessity for a production side and development side of a business

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

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. the school calendar on the registars website, forcasts of enemy traps mou
2. Explain the dominates relationships for each row in the table on slide 4. Expert > student Novice < Expert student > novice
3. Construct the NI policy for the integrity metapolicy. H → L
4. What does it mean that confidentiality and integrity are "orthogonal issues?" they are seperate goals and require seperate policies

Lecture 21

1. Why is Biba Integrity called the "dual" of the BLP model? because it is essentially its inverse
2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty? Because they do not have the same components
3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object? Because they do not have the same components

Lecture 22

1. What is the assumption about subjects in Biba's low water mark policy?
2. Are the subjects considered trustworthy? subjects are only as integral as the objects they need no
3. Does the Ring policy make some assumption about the subject that the LWM policy does not? a subject is able to filter out bad info
4. Are the subjects considered trustworthy? yes

Lecture 23

1. Are the SD and ID categories in Lipner's model related to each other? SD is a confidentiality category for dev and ID is an integrity catfor dev
2. Why is it necessary for system controllers to haye to ability to downgrade? because they are in charge of moving objects from dev to production

3. Can system controllers modify development code/test data? no
4. What form of tranquility underlies the downgrade ability? sft

Lecture 24

1. What is the purpose of the four fundamental concerns of Clark and Wilson? Its a meta policy of sorts for a commercial system
2. What are some possible examples of CDIs in a commercial setting? bank balances, checks
3. What are some possible examples of UDIs in a commercial setting? candy in a bowl @ the bank
4. What is the difference between certification and enforcement rules? cert rules security policy restrictions on behavior of IVPs and TPs, enf Rules built in system security mechanisms that achieve the objectives of cert rules
5. Give an example of a permission in a commercial setting. A cashier having permission to open the drawer

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines? he/she would have inside info on both 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
3. Following the previous question, what companies' files are available for access according to the simple security rule? All of the companies that are not in GM's conflict class
4. What differences separate the Chinese Wall policy from the BLP model? permissions change dynamically based on previous exposure

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects? In a large organization you can streamline and manage roles more efficiently than subjects
2. What is the difference between authorized roles and active roles? ~~Autho~~ Active roles are a subset of authorized roles
3. What is the difference between role authorization and transaction authorization? a transaction is a function a role is authorized to perform
4. What disadvantages do standard access control policies have when compared to RBAC? easier to administer for large organizations, more tailored permissions, various roles allowed w/o changing identities

Lecture 27

1. Why would one not want to build an explicit ACM for an access control system? It's not realistic, most subjects do not have access to all other objects
2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.
   1) maintain a set of rules to compute access
   2) access control list
   3) capability based system

Lecture 28

1. What must be true for the receiver to interpret the answer to a "yes" or "no" question? they have to have agreed upon a boolean format
2. Why would one want to quantify the information content of a message? In order to understand the range of the message
3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme? the message can be misinterpreted
4. Why wouldn't the sender want to transmit more data than the receiver needs to resolve uncertainty? it is possible the channel cannot handle more bandwidth
5. If the receiver knows the answer to a question will be "yes," how many bits of data quantify the information content? Explain. 1

Lecture 29

1. How much information is contained in each of the first three messages from slide 2? 2^1, 2^7
2. Why does the amount of information contained in "The attack is at dawn" depend on the receiver's level of uncertainty? the higher the uncertainty, the more info needed
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why? 4
4. How much information content is contained in a message from a space of 256 messages? 8 bits
5. Explain why very few circumstances are ideal, in terms of sending information content. you rarely know how many possible messages can be sent

Lecture 30

bit a binary digit (discrete) 0 or 1

bit a quantity of info (continuous)

1. Explain the difference between the two connotations of the term "bit."
2. Construct the naive encoding for 8 possible messages. 000 001 010 011 100 101 110 111
3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.
   You only need 1 bit for each of the 995 messages and 5 for the others
4. How can knowing the prior probabilities of messages lead to a more efficient encoding? You can optimize the 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?
   highly efficient encodings

Lecture 31

1. Name a string in the language consisting of positive, even numbers.
   "1 2 3 4 5"
2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.
   1 - 0001 2 - 010 3 - 011 4 - 000 5 - 101 6 - 1110
3. Why is it necessary for an encoding to be uniquely decodable?
   ~~the reciever can be~~ there's not multiple ways to decode
4. Why is a lossless encoding scheme desirable?
   you can use fewer bits
5. Why doesn't Morse code satisfy our criteria for encodings?
   not streamlining

Lecture 32

$-\left(\left(\frac{1}{8}\log\left(\frac{1}{8}\right) + \frac{1}{8}\log\left(\frac{1}{8}\right)\right)\right)$

1. Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).
   $-\left(\log\frac{1}{8}\right) = \log(8) = 3$
2. If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?
   $\frac{4}{5}\times\log\frac{4}{5} + \frac{1}{5}\times\log\frac{1}{5}$
3. Why is knowing the entropy of a language important?
   sets a lower limit on encoding efficiency

Lecture 33

1. Explain the reasoning behind the expectations presented in slide 3.
   you just multiply the probabilities

2. Explain why the total expected number of bits is 27 in the example presented in slide 4. on average we use 27 bits
3. What is the naive encoding for the language in slide 5? 3 bits 000 → 101
4. What is the entropy of this language? plug these probs into
5. Find an encoding more efficient than the naive encoding for this language. yes
6. Why is your encoding more efficient than the naive encoding? because it has a lower bit range