Matt Hendrickson
mjh2793
mjh2793
matthewjames@utexas.edu

WEEK 2 QUESTIONS

1. If a computer system complies with the BLP model, does it necessarily comply with non-interference? Why or why not?
Yes, BLP is an MLS model. If this system complies with BLP then it complies with MLS which implies it complies with NI.
2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?
neither would dominate the other. They are unrelated.
3. Can covert channels exist in an NI policy? Why or why not?
No, NI policy is highly abstract. It states that any object of higher level may do nothing that is "visible" to lower objects. By definition a covert channel does exactly that. Thus a covert channle cannot exist within NI policy.
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 - h B - H
A - h B - l
A - l B - l

Lecture 18

1. Why do NI policies better resemble metapolicies than policies?
It is more of an overall goal instead of the rules to satisfy that goal.
2. What would be L's view of the following actions: h1, l1, h2, h3, . . . , hj, l2, l3, . . . , lk
if this system is an NI system L's view would be
l1, l2 l3 l4 l5 l6 l7
3. What is difficult about proving NI for realistic systems?
many connections between low level system attributes. processor, clock, memory.

Lecture 19

1. Explain the importance of integrity in various contexts.
You don't want the bank hacker to be able to change your bank money numbers.
You don't want an evil TA to change your grades
You don't want an evil General to change the launch codes.
You don't want a Dalek to change you into a Dalek

2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?
The free software could be a virus. If someone is in business charging money for their software then it is most likely being scrutinzed more heavily than its free counterpart. This makes it more trustworthy.
3. Explain the difference between separation of duty and separation of function.
SOD - a single function requires many objects to carry it out. Spread the responsibility, spread the risk
SOF - a single object cannot have a bunch of complementary functions. in a grocery store context, the same person checking you out could not bag your items and then restock the shelves, they would all have to be different people.
4. What is the importance of auditing in integrity contexts?
Making sure that there are no unauthorized changes to the data.
5. What are the underlying ideas that raise the integrity concerns of Lipner?
someone changing the results of some tests that would make it seem like a product is better or worse than it really is.
6. Name a common scenario where integrity would be more important than confidentiality.
Bank account balances.

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.
the expert of physics is better than the student of physics
The student of art and physics is not better than the expert of physics
The student of art is better than the novice of nothing.
3. Construct the NI policy for the integrity metapolicy.
The novice must not interfere with the student and the student must not “interfere” with the expert. Novices cannot change what a student knows, just as a student cannot change what a expert knows. the information must flow down.
4. What does it mean that confidentiality and integrity are “orthogonal issues?”
they are not “related” in that they must be treated separately

Lecture 21

1. Why is Biba Integrity called the “dual” of the BLP model?
for BLP its write up read down. BLP is for confidentiality
for Biba its write down read up. Biba is for Integrity
2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
because they are not related. {A, B} is not a subset or superset of {B, C}

3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?
No

**special Note
Ken Biba proposed three models for integrity security
Low Water Mark Integrity Policy
Ring Policy
Strict Integrity Policy

Lecture 22
1. What is the assumption about subjects in Biba's low water mark policy?
They must be careful in what the read. Dont read stuff that has lower level clearance
2. Are the subjects considered trustworthy?
no because their levels go down as they bring in info with lower levels
3. Does the Ring policy make some assumption about the subject that the LWM policy does not?
the subject can filter out bad information
4. Are the subjects considered trustworthy?
more trustworthy than in LWM

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?
They need to be able to move objects from development to production
3. Can system controllers modify development code/test data?
no.
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?
to ensure consistency between different components of the system.
2. What are some possible examples of CDIs in a commercial setting?
Bank accounts, student records, buyer/seller profile.
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.
A teller authorizing a withdrawal from a bank account.

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?
Two companies in the same field with one person who gets access to procedures on how they work. The consultant could give either American Airlines or United Airlines an advantage by using the info from one company as strategy for the other.
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, they are in unrelated industries.

3. Following the previous question, what companies' files are available for access according to the simple security rule?
GM, Microsoft, Bank of America, Wells Fargo, Citigroup
4. What differences separate the Chinese Wall policy from the BLP model?
The BLP model does not group objects into "related insutry" subgroups

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects?
That automatically includes the principle of need-to-know. Only people who need access to perform their job should have access to those objects.
2. What is the difference between authorized roles and active roles?
Authorized is the set of everything you can do. active is the roles you are currently involved in.
3. What is the difference between role authorization and transaction authorization?
Role authorization - a persons active role(s) must be authorized for that person
transaction authorization - a subject can only carry out a certain transaction if that transaction is authorized for an active role.
4. What disadvantages do standard access control policies have when compared to RBAC?
RBAC is more flexible in commercial settings

Lecture 27

1. Why would one not want to build an explicit ACM for an access control system?
It wouldn't be dynamic.
2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.
storing permissions with objects is performed with ACL

storing permission with subjects is called capabilities
**********storing 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?
To maximize the efficiency in how the message is sent.
3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
so they can interpret each others messages. they must speak the same “language”
4. Why wouldn’t the sender want to transmit more data than the receiver needs to resolve uncertainty?
it’s not efficient.
5. If the receiver knows the answer to a question will be “yes,” how many bits of data quantify the information content? Explain.
1. you only need one bit of info to convey yes or no.

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?
2^n bits
4 bits - 2^4 is 16 which can cover a single digit (0-9)
8 bits - 2^7 is 128 which covers 99.
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 the other times the attack could take place.
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
4 bits. 4 bits can be used to represent 16 possible choices.
4. How much information content is contained in a message from a space of 256 messages?
8 bits. 2^8 is 256.
5. Explain why very few circumstances are ideal, in terms of sending information content.
The total number of choices for a valid message is either very large or unknown.

Lecture 30

1. Explain the difference between the two connotations of the term “bit.”
a discrete entity either 1 or 0.
a continuous quantity of information
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.
out of 1000 total messages 995 of them are the same. we will call this bit 0. Every other message will start with a 1 followed by 4 bits to represent the other 15 choices. so 995 messages only need one bit, the 0 bit. that brings our total to 995. For the other messages which happen the remaining 5 times, because we are sending 1000 total messages, we need 5 bits to represent them. the first bit is a one to show that its not the 0 bit. The remaining 4 bits are used to determine which of the 15 remaining messages it is. thus 5 messages at 5 bits a piece = 25 bits which brings our total up to 1020 bits per 1000 messages.
4. How can knowing the prior probabilities of messages lead to a more efficient encoding?
It can let you group messages into certain categories based on how often you need to send those messages. if you can find one way to represent something that happens a lot you won't have to keep using the same amount of data you would normally have had to do.
5. Construct an encoding for 4 possible messages that is worse than the naive encoding.
For the first message use
000
001
for the second message use
010
011
and for the third message use
100
101
and for the fourth message use
110
111

6. What are some implications if it is possible to find an optimal encoding?
If you can see the best its going to get for a certain style of message, and that best is not good enough, you can find a better format for your messages.
If you have the optimal encoding you know exactly how much bandwidth you're going to need to implement it.

Lecture 31

1. Name a string in the language consisting of positive, even numbers.
0 2 4 6 8 ????
2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.
0
01
011
0111
01111
011111
3. Why is it necessary for an encoding to be uniquely decodable?
So messages do not get incorrectly decoded.
ex. the word “now” and “tomorrow” both are represented by the number string 956. the command is given: we attack 956. How do you know when to attack? Having a uniquely decodable language fixes this.
4. Why is a lossless encoding scheme desirable?
So nothing gets lost in transmission! duh!
5. Why doesn’t Morse code satisfy our criteria for encodings?
it is not streaming

Lecture 32

1. Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).
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?
1(.2 * logbase2(.2) + .8 * logbase2(.8))
3. Why is knowing the entropy of a language important?
It gives you a theoretical lower bound on the amount of bits needed to encode this message.

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?