CS361 Question 2: fa3365; Freda, Anderson

NAME: Freda Anderson
EID: FA3365
CS LOGIN: Freda
EMAIL: Freda.ander@gmail.com

Questions Week 2

Lecture 17

1. If a computer system complies with the BLP model, does it necessarily comply with non-interference? Why or why not?
    a. No, it might not comply with non-inference. As shown in our original covert channel example, there is a way for SH to talk to SL.
2. What would the NI policy be for a BLP system with subjects: A at (Secret:Crypto), B at (Secret: Nuclear)?
    a. We should still have the same read and write rules, but the create and destroy methods should be different. For instance, let there be a file system within this BLP implemented so that Secret: Crypto and Secret: Nuclear can both create an object with the same name, but stored in different places. Then implement a system where subjects without clearance cannot see levels of that file system.
3. Can covert channels exist in an NI policy? Why or why not?
    a. I don't think a storage covert channel could exist. But there are other types of covert channels – for instance, power, time, levels of broadband….so, yes, a covert channel could exist.
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. 3 – both A and B could be low, or high or A could be low and B could be high

Lecture 18

1. Why do NI policies better resemble metapolicies than policies?
    a. NI and metapolicies are both very abstract. Policies are more concrete in the fact they tell how to implement the goals of the metapolicies.
2. What would be L's view of the following actions: h1, l1, h2, h3, . . . , hj, l2, l3, . . . , lk
    a. L1, l2, l3 …. lk
3. What is difficult about proving NI for realistic systems?
    a. There are so many variables involved and so many ways H could potentially talk to L without security measures involved.

Lecture 19

1. Explain the importance of integrity in various contexts.
    a. Integrity relates to how much you trust an entity to produce, protect or modify data. For instance, in our previously implemented BLP model – we enabled anyone with lower confidentiality clearance to modify data. In this instance, we could potentially have the janitor modify or delete the war plan. We probably wouldn't get very far in the war.

2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?
    a. There is an idea that if you pay for something it is a better quality than the free version – meaning the paid software would produce better/cleaner data than that of the free software.
3. Explain the difference between separation of duty and separation of function.
    a. Separation of duty involves several subjects; separation of function involves one subject
4. What is the importance of auditing in integrity contexts?
    a. Tests integrity – potentially allows systems to revert back to a secure state.
5. What are the underlying ideas that raise the integrity concerns of Lipner?
    a. It sounds like Lipner is using a system to check the results of code a programmer comes up with. Using existing software and testing on nonproduction systems will (maybe) run tests that the programmer didn't think about.
6. Name a common scenario where integrity would be more important than confidentiality.
    a. Development of code

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. Highly reliable with little sensitivity – information published in a textbook
    b. Not reliable with great sensitivity – an anonymous call about a terrorist threat
2. Explain the dominates relationships for each row in the table on slide 4.
    a. An expert will have more reliable information than a student; same category
    b. A novice will not have more reliable information than an expert; categories not dominant
    c. A student will have more reliable information than a novice; categories are dominant
3. Construct the NI policy for the integrity metapolicy.
    a. (From slides) Don't allow information to "flow up" in integrity. AKA don't allow bad information to taint good information.
4. What does it mean that confidentiality and integrity are "orthogonal issues?"
    a. We have to treat them separately.

Lecture 21

1. Why is Biba Integrity called the "dual" of the BLP model?
    a. It works fairly similar to BLP (information flows differently and the two systems solve different issues). Uses Simple Integrity and Integrity* properties as opposed to simple security and * property.
2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
    a. There is no dominates relation. Subj 3 can't read Obj3 because Obj3 is below Subj3. CAN'T WRITE BECAUSE H HAS A?
3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?
    a. Not in the Biba model

Lecture 22

1. What is the assumption about subjects in Biba's low water mark policy?
    a. The subject takes on the minimum integrity level – they can be tainted.
2. Are the subjects considered trustworthy?
    a. No, they can be tainted.
3. Does the Ring policy make some assumption about the subject that the LWM policy does not?
    a. It assumes that subjects can filter out untrustworthy information.
4. Are the subjects considered trustworthy?
    a. Yes, they can decide what is true or not.

Lecture 23

1. Are the SD and ID categories in Lipner's model related to each other?
    a. In the sense that they are both programs under development – SD is confidentiality and ID is integrity
2. Why is it necessary for system controllers to have to ability to downgrade?
    a. Code can move out of development
3. Can system controllers modify development code/test data?
    a. It can modify the security level of the code/test data
4. What form of tranquility underlies the downgrade ability?
    a. Weak tranquility

Lecture 24

1. What is the purpose of the four fundamental concerns of Clark and Wilson?
    a. Authenitcation
    b. Audit
    c. Well-formed transactions
    d. Separation of Duty
2. What are some possible examples of CDIs in a commercial setting?
    a. Change of personal employee information
3. What are some possible examples of UDIs in a commercial setting?
    a. Quantity of an object in stock
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?
    a. There could be a conflict of interest where a contractor gives secure information from one company to another.
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?
    a. Yes, because it belongs to an entirely different conflict of interest class.

3. Following the previous question, what companies' files are available for access according to the simple security rule?
    a. Files that are in the same company datasets as the objects already accessed by the subject
4. What differences separate the Chinese Wall policy from the BLP model?
    a. The Chinese Wall is not about confidentiality but about a specific subset of confidentiality - conflict of interest.

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects?
    a. More flexible – subjects can assume many roles
2. What is the difference between authorized roles and active roles?
    a. Active – what the subject is currently working as
    b. Authorized – what the subject could potentially work as
3. What is the difference between role authorization and transaction authorization?
    a. A subject can only authorize a transaction if the transaction is authorized for one of the subject's active roles for which the subject has been authorized.
    b. Role authorization is checking if the subject can take on a role – transaction authorization is checking if an action can
4. What disadvantages do standard access control policies have when compared to RBAC?
    a. More flexible
    b. Easier to administer
    c. Appropriate to organization
    d. Recognizes subjects can have multiple roles
    e. Allows subjects to easily change roles

Lecture 27

1. Why would one not want to build an explicit ACM for an access control system?
    a. There are common alternatives.
2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.
    a. You can compute it on the fly with the rules
    b. ACL – create a list with the object
    c. Capabilities – store with the subject the permissions he is allowed

Lecture 28

1. What must be true for the receiver to interpret the answer to a "yes" or "no" question?
    a. The sender and receiver must have some shared knowledge, included in an agreed encoding scheme.
    b. The smallest bit to transmit a yes or no is 1 and 0.
2. Why would one want to quantify the information content of a message?
    a. The smaller the message size, the more certain the receiver can be.
3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
    a. The receiver must know how to decode and get the message.

4. Why wouldn't the sender want to transmit more data than the receiver needs to resolve uncertainty?
    a. More chances there are to mess up/corrupt the message.
5. If the receiver knows the answer to a question will be "yes," how many bits of data quantify the information content? Explain.
    a. Just 1. Let Yes be 1 and No be 0.

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?
    a. Log n (complete binary tree)
    b. Log 3 at most
    c. Log 10 at most
2. Why does the amount of information contained in "The attack is at dawn" depend on the receiver's level of uncertainty?
    a. It depends of the receiver's uncertainty – If they are unsure about dusk or dawn, it is just one bit; time of day, n bits; ….
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
    a. Log2 (n) if we let each node in a complete binary tree be a message.
    b. Many more bits if we have to transmit the message
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."
    a. Discrete – a 0 or 1
    b. Continuous – a quantity of information
2. Construct the naive encoding for 8 possible messages.
    a. Sending in 4 bits as a binary representation of decimal numbered messages
3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.
   On Average
    a. 995 times we will only be sending 0
    b. 5 times we will be sending some form of 5 0's and 1's
    c. There will be 995+(5*5) bits sent in total (on average)
4. How can knowing the prior probabilities of messages lead to a more efficient encoding?
    a. We will make the messages most likely to be sent with the smallest amount of bits
5. Construct an encoding for 4 possible messages that is worse than the naïve encoding.
    a. 1 = 0001
    b. 2 = 0011
    c. 3 = 0111
    d. 4 = 1111
6. What are some implications if it is possible to find an optimal encoding?
    a. Optimal encoding would imply that we could send the least possible amount of bits for any given message.

Lecture 31

1. Name a string in the language consisting of positive, even numbers.
    a. “1234”
2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.
    a. “1”, “2”, “3”, “4”, “5”, “6”
3. Why is it necessary for an encoding to be uniquely decodable?
    a. Because if it is not one to one, how will the receiver know what was sent?
4. Why is a lossless encoding scheme desirable?
    a. In case information is lost, it is still possible to recover the entire original sequence of symbols from the transmission.
5. Why doesn’t Morse code satisfy our criteria for encodings?
    a. If the data is streaming, we can’t separate letters.

Lecture 32

1. Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).
    a. $H = -8(1/8 \log(1/8))$
2. If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?
    a. $L = 1/5 \quad H = 4/5$
    b. $E = -(1/5 \log(1/5) + 4/5 \log(4/5))$
3. Why is knowing the entropy of a language important?

Lecture 33

1. Explain the reasoning behind the expectations presented in slide 3.
    a. The coin is unbalanced. It lands on heads ¾ of the times so ¾ * ¾ = 9/16 and ¾ * ¼ = 3/16 and ¼ * ¼ = 1/16
2. Explain why the total expected number of bits is 27 in the example presented in slide 4.
    a. Count * |Code| = number of bits
3. What is the naive encoding for the language in slide 5?
    a. Binary code of decimal digits 1 – 6
4. What is the entropy of this language?
5. Find an encoding more efficient than the naive encoding for this language.
    a. 1 = 00
    b. 2 = 01
    c. 3 = 001
    d. 4 = 011
    e. 5 = 0001
    f. 6 = 0111
6. Why is your encoding more efficient than the naive encoding?
    a. You are sending less bits for values that are more frequently sent.