Brittany Kvanvig bmk447

CS361 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?

   Because BLP unintentionally allows for covert channels, which violates the non-interference information flow policy.

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

   A can't interfere with B because neither dominate the other.

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

   No, because a covert channel counts as an interference.

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?

   If both A&B are high, if both A&B are low, or if B is high and A is low.

Lecture 18

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

   Because they are very vague and don't have specific instructions on how to implement them.

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

   L1, l2, l3,…,lk

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

   Most realistic systems have a lot of interferences that would violate a NI metapolicy.

Lecture 19

1. Explain the importance of integrity in various contexts.

A newspaper to protect its reputation. A bank to protect itself from a party taking money they don't have.

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

   Because the commercial software is more reputable than the free software in general.

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

   Separation of duty requires several subjects to authorize the same critical task. Separation of function requires the same subject to not be able to do two different critical tasks.

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

   It's important to keep track of who access to or was performing certain tasks in case of an emergency integrity breach.

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

   He's concerned about separation of function. (Teller's don't write the software they're using, programmers don't use actual customer's data, etc)

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

   Newspaper articles written by a reputable newspaper.

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.

   Highly reliable, little sensitivity: census. Little reliability, higher sensitivity: anonymous tip of bomb location.

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

Expert (physics) dominates student (physics) because the sensitivity is higher and the categories are the same. Novice in art and physics: even though art and physics is a superset of physics, novice does not dominate expert, so novice (art,physics) doesn't dominate expert (physics).

Student (art) dominates a novice() because of the higher sensitivity label.

3. Construct the NI policy for the integrity metapolicy.

   Low integrity can't taint high integrity, but high integrity can bleed down to low integrity.

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

   They must be treated separately.

Lecture 21

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

   It is the exact opposite. All you do is change the arrows.

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

   Because neither categories are a superset of the other.

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

   No.

Lecture 22

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

   The subjects are easily corrupted by low integrity information. They can't discern integrity levels of information.

2. Are the subjects considered trustworthy? No.

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

   Subject can filter bad information by themselves.

4. Are the subjects considered trustworthy?

   Yes.

Lecture 23

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

Both deal with development, but SD concerns confidentiality and ID concerns integrity.

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

Because it gives them the ability to move software from development to production

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

No, because they don't have access to the system programs in development (SSD).

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?

Consistency among various components of the system state.

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

Bank balances

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

Bank candy bowl

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

Certification deal with internal matters. Enforcement deal with outside users.

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

(Brittany, withdrawal/deposit/view money in account, {brittany's account})

Lecture 25

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

Because United Airlines and American Airlines are competitors and the consultant could potentially leak important information that could benefit one and harm 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

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

   Both GM & Microsoft

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

   The Chinese Wall policy depends on the subject's history with certain conflict classes. The BLP model doesn't.

Lecture 26

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

   Much easier to administer this system for a very large company.

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

   Authorized roles are any role the person could possibly take on, while the active role is the one they are currently assuming.

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

   Roles are the positions and transactions are the things that role can do.

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

   They aren't as flexible when people change roles. They're much slower having to determine access on an individual vs role basis.

Lecture 27

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

Because most subjects don't have any access to most 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 permissions based on attributes of subjects and objects. (This is what we did for BLP.)
    2. Associate the permissions with objects. This is called an *access control list* (ACL).
    3. Associate the permissions with subjects. This is called a *capability-based system*.

Lecture 28

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

    They both understand the encoding scheme

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

    To know the bandwidth of the channel

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

    Because otherwise the information is meaningless

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

    To make the interaction more efficient and doesn't draw as much attention to the channel by keeping the bandwidth small.

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

    If the receiver knows the answer to a question, the answer doesn't need to be asked at all. If an answer is required, however, one bit would be sufficient to verify the answer.

Brittany Kvanvig bmk447

Lecture 29

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

   N bits; 4 bits; 7 bits.

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

   If there were only two possibilities (dawn or dusk): only 1 bit. But if much more uncertainty (attack at any time) many more bits are needed.

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

   4 bits, because each 2^4 = 16.

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

   Log2(256) = 8.

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

   Most communications don’t have a specific set of outcomes possible, so you can’t have a binary tree representation of the possible answers.

Lecture 30

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

   Discrete bits are finite. Continuous bits are an average 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.

   You send 1000 messages. 99.5% are ok. So that’s 995 messages that take one bit, plus 5 that use 5 bits, which is 1020 total bits compared to the naïve encoding which would cost 4000 bits total.

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

   You can assign the most likely result to a very efficient coding so the average bits transmitted is lower.

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

   0: ok, 10: error 1, 110: error 2, 1111: error 3.

   30% error 1, 30% error 2, 39% error 3, 1% ok.

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

   You use less bits on average per instruction.

Lecture 31

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

   “24680246802”

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

   1, 0, 10, 11, 100, 101

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

   So the message is less likely to misread or misinterpreted

4. Why is a lossless encoding scheme desirable?

   Because it protects the integrity of the message being sent

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

   Because it’s not streaming

Lecture 32

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

-(1/8 log2 (1/8)+ 1/8 log2 (1/8)+ 1/8 log2 (1/8)+ 1/8 log2 (1/8)+ 1/8 log2 (1/8)+ 1/8 log2 (1/8)+ 1/8 log2 (1/8)+ 1/8 log2 (1/8))= -(log2(1/8))= 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?

-(1/5log2(1/5)+4/5log2(4/5))= -(-.4644 + -.2575) = 0.7219

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

It gives you the lower limit on encoding efficiency of a language.

Lecture 33

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

Since the coin is biased, certain pairs of flips have a higher probability than others. So giving the higher probability pairs a lower number of bits brings the average number of bits sent below 1.

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

27 is the result of multiplying the probabilities by 16 to find the number of bits sent in an average set of 16 pairs of flips.

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

1: 000	6/22	18
2: 001	6/22	18
3: 100	3/22	9
4: 101	3/22	9
5: 110	2/22	6
6: 111	2/22	6

4. What is the entropy of this language?

66/22 = 3

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

1: 00	6/22	12
2: 01	6/22	12
3: 10	3/22	6
4: 11	3/22	6
5: 110	2/22	6
6: 111	2/22	6

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

   Average bits sent per instruction is lower.
   48/22 = 2.181818