Tolu Kalejaiye
tok76
tok76
tkalejaiye@utexas.edu

HOMEWORK 2

Lecture 17

1. No, it doesn't. It is possible to take any MLS policy and make it an NI policy. However, to do this, the BLP policy must be made intransitive.
2. It would just be two unconnected subjects, as there is no relation between the sets. They're both at clearance level *Secret* but *Crypto* and *Nuclear* have no connection.
3. Yes. If I have A → B and B → C as my relations, I can still have covert channels between A and B or B and C, I just couldn't have one between A and C directly.
4. A – low, B – high.

Lecture 18

1. The NI policy is very abstract. It just defines the flow of information and doesn't have rules about which subjects can read/write objects.
2. L1,l2,l3,…lk.
3. Interferences are very common in real systems, some interferences are benign, and you would have to include several low level system attributes.

Lecture 19

1. The importance of integrity is to ensure that trust is maintained to produce/protect/modify data.
2. The integrity of the commercial software is likely to be higher than that of the freeware, as the commercial software probably has to go through some sort of certification or testing.
3. Separation of duty relates to the tasks in a process being divided into different categories. Separation of function relates to each function required for the process being handled by separate parties.
4. To insure that there are no discrepancies or missing data at the end of a process.
5. The ideas are those of people being able to freely manipulate data they should not be able to manipulate.
6. Take the scenario of a bank, where you may have a teller who is stealing money. Integrity is more important than confidentiality here because it's more important to ensure that money brought in/out is accounted for. The main concern is not that no one knows how much money is in the bank.

Lecture 20

1. Highly Reliable/Little Sensitivity – A sportscaster on ESPN reading off the scores of today's World Cup games.
   Not Highly Reliable/Great Sensitivity – The National Enquirer saying that Barack Obama has left his wife for Hillary Clinton.
2. Row 1 – Expert dominates Student because he/she is a more reliable source about physics than someone who is just learning it.
   Row 2 – A novice in physics cannot know more than an expert in physics, and therefore cannot dominate in the relationship.
   Row 3 – Art student dominates because a novice in nothing.
3. L → H
4. It means that they must be treated separately, not grouped into the same labeling set.

Lecture 21

1. Because it is the inverse of the BLP model.
2. Because they do not share the same subset of categories
3. It may still be able to read the object, but not write to it.

Lecture 22

1. The assumption is that a subject will read information regardless of its integrity level.
2. No, they aren't considered trustworthy.
3. Yes, it assumes that subjects will filter the information they receive.
4. They are considered more trustworthy than subjects in LWM.

Lecture 23

1. No they aren't. SD is a confidentiality category, and ID is an integrity category.
2. Because at some point, the product needs to move from development to production (after development is done). This requires a downgrade of its confidentiality.
3. Yes. The system controller's integrity level is higher than that of the development code/test data. Writing down is allowed.
4. Weak tranquility

Lecture 24

1. They believed commercial security has its own unique concerns and should have its own model.
2. CDIs could be things like an order placed by a company for some sort of supplies, or an invoice of goods sold.

3. A possible UDI could be the information that was written/typed onto the invoice or order. Once it is entered, it becomes a CDI.
4. The certification rules are in place to make sure that the integrity metapolicy is followed, whereas the enforcement rules are in place to ensure that proper authorization is had to perform these certifications.
5. A banker (user) is authorized to cash(tp) a bank customer's check(cdi).

Lecture 25

1. Because the consultant could inadvertently leak information about one airline to it's competitor, the other airline.
2. Yes, because these companies are not in the same conflict class.
3. Microsoft and either Bank of America, Citicorp, or Wells Fargo but not all three.
4. The Chinese Wall policy is concerned with conflicts of interest between companies, and permissions change based on a history of accesses. The BLP model is concerned with the confidentiality and integrity of files within a system/company.

Lecture 26

1. This allows for one person to hold multiple roles if necessary, whereas a subject is singularly defined.
2. Active roles are the roles you are currently undertaking. Authorized roles are all the roles you could potentially occupy.
3. They're subsequent levels of authorization. Role authorization says you can only take on an active role that is one you're authorized to take. After that is verified, transaction authorization says that you can only perform transactions allowed by your current active role(s).
4. RBAC is more applicable to real world/commercial situations where a person may have more than one role within a company. It is also easier to administer, as the permissions for a role are the same for anyone with that role in their set of authorized roles.

Lecture 27

1. Storing the matrix exclusively is normally expensive and unnecessary. One could use an ACL instead.
2. Use an access control list, use a capability-based system, and maintain a set of rules to compute access permission.

Lecture 28

1. The receiver must have some shared knowledge or encoding with the sender.
2. Possibly to determine what channel works best to transmit the information.
3. This is because if we are transmitting information in some encoded fashion, the receiver needs to be able to decode it to read the information. If the

receiver doesn't know about the encoding used by the sender, then the receiver cannot open the message.

4. Because the size of the information could exceed the capability of the channel being used. It's also inefficient.
5. 0. The receiver already knows the answer, so a message doesn't need to be sent and the data never needs to be encoded.

Lecture 29

1. a. n bits b. 1 bit c. 2 bits d. depends on the receiver's level of uncertainty
2. Because there are several ways the message could be transmitted, we need to know how much of the message the receiver already knows/can discern. Then we know the amount of the message that needs to be considered.
3. 4 bits. The information content of any message selected from a space of K messages should be $\log_2 K$. In this case, K = 16.
4. $\text{Log}_2 256 = 8$
5. A message could be very extensive, and possibly contain several parts that need decoding.

Lecture 30

1. The first meaning is the typical binary digit version where bits represent numbers. The second is a measure of storage capacity.
2.

Message	Code
M0	0000
M1	0001
M2	0010
M3	0011
M4	0100
M5	0101
M6	0110
M7	0111

3. Under the new encoding, we transmit 1 bit for M10 and 5 for all the others. Since we know 995 out of 1000 messages will be M10, we only need to calculate the other 5 messages out of a possible combination of 5 bits. Thus, we have 995 + (5*5) = 1020 bits.
4. As witnessed in the above question, it allows you to use fewer bits, because it reduces the number of probabilities to consider.
5.

Messages	Code
M0	10000
M1	10001
M2	10010
M3	10011

6. Vastly improved speeds of the transmission of information.

Lecture 31

1. “2468482”
2.

Roll	Code
1	1
2	10
3	101
4	1010
5	10101
6	101010

3. You don’t want to have two pieces of information with the same encoding because then you won’t know what it should translate to when decoding.
4. To ensure that no information is lost during transmission and that vital pieces of the message aren’t lost, thereby changing the meaning of the message.
5. It isn’t prefix-free. For example, Morse for ‘E’ is the prefix of the Morse for ‘S’.

Lecture 32

1. $-\log_2(1/8) \approx 2.07$
2. $-((4/4)\log_2(4/4)) = 0$
3. Because it can tell us the lower bound on encoding efficiency.

Lecture 33

1. Because these are the probabilities listed in the table. We’re still using the weighted coin, so the probabilities were initially skewed. For example, the probability of getting H is ¾, so the probability of getting HH would be H*H = ¾ * ¾ = 9/16.
2. Multiply the count by the number of bits in their respective codes and the sum is 27.
3.

Result	Code
1	0
2	10
3	110
4	1110
5	11110
6	111110

4. $-(2((6/20)\log(6/20)) + 2((3/20)\log(3/20)) + 2((1/20)\log(1/20))) \approx 1.59$
5.

Result	Code
1	0
2	1
3	01

4	10
5	001
6	100

6. By predicting the probabilities associated with each possible result, we can use less bits for the rolls that are more likely to occur, thereby using fewer bits overall.