Name: Ridwan Hoq
EID: rmh2376
CS Login: ridwan
Email: ridwanhoq@gmail.com

Lecture 17

1. If a model complies with BLP, then it complies with non-interference. This is true because you can create overlapping relations that emulate the transitive property of BLP.
2. $A \mapsto B$; $B \mapsto A$
3. Theoretically, no. An NI policy should ensure that actions cannot be observed by another subject that shouldn't have access to that information. Subjects observing a difference in state/information is how a majority of covert channels function. However, there could still be a covert channel that works without monitoring state.
4. There is only one combination: A must be low and B must be high.

Lecture 18

1. NI policies better resemble metapolicies than policies because it defines very general notions of information flow. It doesn't define specific read/write policies per subject/object. Rather, it just defines where information can (and can't) flow.
2. I1, I2, I3, … , Ik
3. Because most interferences are very low level or even benign. We would need to model the access model at some of the lowest levels of implementations which is very hard to do.

Lecture 19

1. Integrity is important where data must be correct and untampered with.
2. Commercial software might be preferred over freeware because it would be better supported and more trusted. There is more likely to be malicious software in the commercial software because the company producing the software would lose customers if their malware was detected.
3. Separation of duty requires multiple subjects to complete a critical function, while separation of function prevents a single subject to fulfill multiple roles in a critical function.
4. Auditing is important for integrity so that there is some level of accountability for any malicious actions that might occur.
5. Lipner outlines a model in which there are multiple environments in which a software must operate. When the software transitions between environments, Lipner points out that the integrity of the data must be unaffected.
6. Integrity of a rocket launch's calculations might be more important than keeping it confidential.

Lecture 20

1. Reliable but not sensitive: flight info
   Sensitive but not reliable: gossip
2.
   a. Expert dominates Student, because Expert has a higher level than Student
   b. Novice doesn't dominate Student because Student has a higher level than Novice
   c. Student dominates Novice, because Student has a higher level than Novice

3. High Integrity ↦ Low Integrity
4. They're orthogonal issues in the sense that they must be dealt with separately. Multiple types of models are necessary to ensure both confidentiality and integrity are preserved.

Lecture 21

1. The Biba model is dual of BLP because it enforces integrity in a similar fashion. However, it mandates that the integrity of information flow downwards, which is the opposite of BLP.
2. Because neither Subj3 and Obj3 dominate each other.
3. If both confidentiality and integrity are being enforced, then the subject cannot access the object.

Lecture 22

1. Biba assumes that subjects automatically get corrupted when they read information with lower levels of integrity.
2. Not really since their integrity becomes compromised upon reading the information even if they don't change their own state.
3. The Ring policy assumes that any subject will not compromise their own integrity just by reading/viewing information.
4. The Ring policy places more trust into subjects in that they will not willingly corrupt their own integrity. The Ring policy trusts that the subjects have enough common sense to filter out erroneous/wrong information.

Lecture 23

1. SD and ID are both labels that pertain to developers. However SD is a confidentiality label and ID is an integrity label.
2. System controllers need the ability to downgrade so they can move between development and production.
3. No system controllers could not modify (write) to development code/test data because the system controllers' confidentiality label dominates the development code/test data's confidentiality label.
4. Weak tranquility

Lecture 24

1. The purpose of the four fundamental concerns of Clark-Wilson is to ensure consistency among the components of the system state.
2. Examples of CDIs: Bank balances, credit card information, social security numbers
3. Examples of UDIs: Bank routing information, Teller's name, Bank phone number
4. Certification ensures integrity is preserved, whereas enforcement prevents integrity from being compromised
5. A bank teller is authorized to withdraw/deposit money to a bank user's account.

Lecture 25

1. Because American Airlines and United Airlines are competitors. If that lawyer had some sensitive information about American Airlines and shared it with United Airlines, it might put American Airlines at a competitive disadvantage.
2. Yes you would since Microsoft and GM are not within the same conflict class.
3. Bank of America, Wells Fargo, Citicorp, Microsoft

4. The Chinese Wall is different from BLP in the sense that it doesn't have levels of access but rather groups of access that prevent access if a previous group has been accessed.

Lecture 26

1. Makes organization management much easier since individuals don't have to be granted access uniquely which can be tedious and hard to maintain.
2. Authorized roles are the set of roles in which a subject is allowed to fill at various times whereas active roles are the roles in which a subject is currently filling. Active roles are a subset of authorized roles.
3. Role authorization checks to see if a given role exists within the set of authorized roles. Transaction authorization checks to see if a transaction be executed if that transaction is authorized for one of the subject's active roles.
4. Standard access policies are much less specific to organizations. Permissions are custom tailored to the the organization. Additionally, standard access policies must assign individuals permissions on a case by case basis rather than having access groups which are easier to manage and maintain. Also, with a standard access policy it much more difficult to switch between roles.

Lecture 27

1. It's pointless to store the ACM because most objects aren't accessible so a majority of the matrix would be useless.
2. Storing permissions with objects is called an access control list. Storing permissions with subjects is called a capability based system. Computing permissions on the fly is storing permissions implicitly through the rules of the access system.

Lecture 28

1. The receiver must know what information represents yes and what information represents no.
2. We might want to quantify the amount of information so that when the information is received, we can verify that the expected amount of information was received.
3. The sender and receiver must agree on an encoding scheme so that both parties know what each other mean.
4. Because the receiver might not be ready to process that information.
5. None because the receiver already knows the information being transferred.

Lecture 29

1. 12 bits of information
2. It depends on the level of uncertainty of the receiver because the amount of information that needs to be sent depends on what exactly the receiver doesn't already know.
3. 4 bits of information because there are 2^4 possibilities which is 16.
4. 8 bits of information
5. It is hard to define all possible messages that could be sent or received.

Lecture 30

1. Bit can mean either a binary digit or a quantity of information.
2.
    i. 000
    ii. 001

iii. 010
iv. 011
v. 100
vi. 101
vii. 110
viii. 111

3. Since on 995 of 1000 messages are going to be M10 and M10 is encoded in one bit with the other 5 messages encoded in 5 bits, it adds up to be 995 + (5 * 5).
4. Knowing the probability of a message being transmitted can help efficiency since you can adjust the length of a message's encoding depending on if the that message is likely. If a message being transmitted is very likely, then you'll want to encode that message very efficiently.
5.
   i. 0000001
   ii. 0000010
   iii. 0000011
   iv. 0000100
6. It would mean that there is no better encoding.

Lecture 31

1. "2486"
2.
   i. 0
   ii. 00
   iii. 000
   iv. 0000
   v. 00000
   vi. 000000
3. Unique decodability is necessary because you need to be able to distinguish between various encodings. If a encoding isn't unique, then there is ambiguity about what that encoding actually is.
4. A lossless encoding is desirable because that way no data is lost.
5. Morse code is not streaming because there are necessarily breaks in the encoding. Additionally, it isn't uniquely decodable.

Lecture 32

1. $h = -(\log \frac{1}{8}) = \log 8$
2. $h = -(\frac{1}{5} \log \frac{1}{5} + \frac{4}{5} \log \frac{4}{5})$
3. It is important to know the entropy of a language so that you can construct an efficient encoding for that language.

Lecture 33

1. Since flipping the coin 32 times is equivalent to flipping a coin 16 times twice, you can use those probabilities to calculate the how many times the following results would appear.

2. Given that encoding, we've got that many occurrences of each result, which sums up to 27 bits.
3.
    i. 001
    ii. 010
    iii. 011
    iv. 100
    v. 101
    vi. 110
4. h = -(6/20 log 6/20 + 6/20 log 6/20 + 3/20 log 3/20 + 3/20 log 3/20 + 1/20 log 1/20+ 1/20 log 1/20)
5.
    i. 1
    ii. 01
    iii. 001
    iv. 0001
    v. 00001
    vi. 000001
6.
    i. 1 * 6/20 = 6/20
    ii. 2 * 6/20 = 12/20
    iii. 3 * 3/20 = 9/20
    iv. 4 * 3/20 = 12/20
    v. 5 * 1/20 = 5/20
    vi. 6 * 1/20 = 6/20

    Sum = 50/20 = 2.5 bits on avg < 3 bits so it is better than the naive.