Name: Olamide Fayemiwo
EID: oaf226
CSLogin: ofaye
Email: olamide.fayemiwo@live.com

CS361 Questions: Week 2

Lecture 17

1. It complies with non-interference because the BLP model is transitive by the' dominates relation.'
2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?
   The NI policy would be that information cannot be sent to one another from the higher subject if the level of the subject is higher than another.
3. No, because there is no way to specify it.
4. In BLP, A will have the high level while B will have a low security.

Lecture 18

1. NI's policies better resemble metapolicies because it talks about the broad overview of what the goal is. It states that the flow of information can only be passed a certain way, from High to Low levels.
2. L's view would be the following instruction sequence: l1, l2, l3,…., lk
3. Interferences are benign, and it involves low-level system attributes so it is difficult to prove NI for realistic systems due to multiple potential interferences.

Lecture 19

1. Integrity is important when it comes to individuals; we all want to know that people are upright with us and have the quality of being honest. Integrity is also important when it comes to security because we do not want someone or a program that we wrote to write or modify any information that it is not authorized to do.
2. They would want to purchase commercial software because downloading a similar free available version can lead to malicious software being downloaded on your computer. Thissoftwarecan duplicate themselves as other processes and can have access and modify important data. It would be hard to detect and correct these unauthorized changes to data. Also, purchasing commercial software has more integrity than downloading it free off the internet.
3. Separation of duty involves having several different subjects being involved to complete a critical function while Separation of functions states that a single subject cannot complete complementary roles within a critical process.
4. Auditing is important when it comes to integrity because it involves recovering and accountability. Auditing helps in order for individuals to know where integrity has been compromised.
5. The level of access anyone can obtain to modify programs and data.
6. Integrity would be more important than confidentiality when it comes to grades. A student can check his/her grades with no problem but if the student can change his/her grades then integrity has been compromised.

Lecture 20

1. Highly reliable: New York Times Not Highly Reliable: Tabloid newspaper
2. Row 1: The Expert has a higher level of trustworthiness in the category because the student is possibly learning from the expert.
   Row 2: The level of trustworthiness is less than of the expert, although the novice knows two categories, the expert has more experience with physics
   Row 3: The student has more knowledge due to its level of trustworthiness than the novice
3. A path in the graph from L1 to L2 means that "information is allowed to flow" from level L2 to level L1. Information can flow "downward" in the lattice of security levels. It may only flow if L2 <= L1.
4. It means that confidentiality and integrity are independent issues.

Lecture 21

1. The Biba Integrity (Strict Integrity Policy) is called the "dual" of the BLP model because it has a Simple and *-property but it only opposite of the BLP model.
2. Subj3 and Obj3 is empty because the even though the subject level and the object level are the same thing, the categories are not identical.
3. The subject cannot access the object even if a subject satisfies confidentiality requirements because confidentiality and integrity are orthogonal issues.

Lecture 22

1. The assumption about subjects in Biba's low water mark policy is that they are going to read an object with a potential lower level.
2. The subjects are not considered trustworthy and this policy's goal is to decrease the integrity level of a subject unnecessarily.
3. No, the Ring policy makes the same assumption as the LWM policy which presumes that subjects are going to read objects with a lower level of integrity but it allows them to decide, it does not restrict them.
4. The subjects are considered trustworthy in a Ring policy because it feels like the subjects can filter what they read.

Lecture 23

1. They are not related to each other because they are for two different issues, one is for confidentiality and the other is for integrity.
2. System controllers need to have the ability to downgrade because they need to be able to move objects from the development stage to the production stage. They decide what can and cannot be moved from levels.
3. Yes, System controllers can modify development code/test data because they have a low confidentiality level which means that they can write up and they also have a high integrity level which means that they can write down and not lose integrity and still be highly reliable.
4. It underlies the weak tranquility because downgrade has the ability to change labels in a way that does not violate the spirit of security policy.

Lecture 24

1. The purpose of the four fundamental concerns of Clark and Wilson is to address the concerns of integrity and to build a way to have consistency among the components.
2. An example of CDIs in a commercial setting would be downloading software from a certified company, an accredited newspaper company, or network, or a professor.

3. An example of UDIs in a commercial setting would be downloading a software from an uncertified website, a tabloid newspaper.
4. Certification rules makes sure that a confirmation of certain standards are met before moving forward or after the procedure is complete while enforcement rules are required before any procedure.
5. User: customer at the bank who has identified him/her is actually the person (authentication); TP: Withdraw money from the customers bank account; CDI set: the customers bank account, important information etc.

Lecture 25

1. It would be a breach of confidentiality if a consultant was hired by two Airline companies because for one, they are in the same category ("need- to- know") and the consultant has access to private data and can definitely read and write and change the levels of security in both companies.
2. Yes, you will be able to access another file from GM again if you access another file from another conflict class, as long as it does not belong in the same conflict class.
3. The companies' files that are available for access according to the simple security rule are the files in the same company dataset that you have accessed previously or if the company file belongs to an entirely different conflict class.
4. The difference between the Chinese Wall policy and the BLP model is that the CWP addresses a specific concern which is the conflict of interest by a consultant or contractor.

Lecture 26

1. The benefits of associating permissions with roles is that permissions are like subsets of roles, it is consent so associating it with roles means that there has to be consent or authorization in order for a person to complete the job function (role). For example the role of a teller has the permission to service a bank customer.
2. Authorized roles are allowed to fill at various times while active roles are currently occupied.
3. Role authorization states that a subject's active role must be an authorized role for that subject while a transaction authorization states that a subject can execute a transaction only if the transaction is authorized for one of the subject's active roles.
4. The disadvantages that standard access control policies have when compared to RBAC is that it is difficult to figure out which files a user has access to when it comes to access control and it does not support large data and/or changes.

Lecture 27

1. You would not want to build an explicit ACM for an access control because it will be difficult for the matrix to account for a large population (data)
2. **Storing permissions with objects**: Access control List;
   Storing permissions with subjects: Capability-based system;
   Computing permissions on the fly: Maintain a set of rules based on attributes of subjects and objects.

Lecture 28

1. The receiver must have a certain amount of bits enough to quantify the information content of the message the sender is transmitting.
2. One would want to quantify the information content of a message because we might want to know how much information can be transmitted.

3. The sender and receiver must have some shared knowledge and an agreed encoding scheme because it is an effective way to communicate between both sender and receiver.
4. The sender would not want to transmit more data than the receiver needs to resolve uncertainty because the receiver might not be able to handle the bit of data coming in because there is no more space to allocate.
5. One bit of data is needed to quantify the information content.

Lecture 29

1. a. n-bit
   b. 4 bytes
   c. 4 bytes
   d. 4 bytes
2. It depends on the receiver's level of uncertainty because after it resolves the uncertainty, we will know the actual content of the information.
3. logbase 2(16) = 4 because that would be the longest path if there are 16 leaves on the tree.
4. 8 bits is contained in a message from a space of 256 messages
5. Few circumstances are ideal because it is hard to know how much space is needed to send these transmissions. The sender and receiver must agree on an encoding before.

Lecture 30

1. The first one is a binary digit and the second one is a quantity of information
2.

Message	Code
M0	0000
M1	0001
M2	0010
M3	0011
M4	0100
M5	0101
M6	0110
M7	0111
M8	1000

3. It takes 995 because that is the number of messages that would be message number 10, then it takes (5 * 5) because there are 5 more messages to take and 5 as the binary number
4. It leads to a more efficient encoding because you will know how often a message appears in an arbitrarily long sequence of messages.
5.

Message	Code
M0	000000
M1	000001
M2	000010
M3	000011
M4	000100

6. Finding an optimal encoding means using fewer bits to transmit the message but we do not know how much bitsthe receiver can hold to get the messages being transmitted.

Lecture 31

1. "2468"
2.

Roll	Naïve	Code 1	Code 2
1	000	0	0
2	001	10	01
3	010	110	10
4	011	1110	110
5	100	11110	1110
6	101	11111	1111

3. It is necessary because you want to be able to recover the entire original sequence of symbols from the transmission if needed. Basically you want it to be lossless.
4. A lossless encoding scheme is desirable because it makes sure that the entire original sequence of symbols can be recovered.
5. Morse code does not satisfy our criteria for encoding because it has a break in the encoding according to the definition of streaming.

Lecture 32

1. h = -(8(1/8) * log (1/8))
2. h = -(4/5 * log 4/5 + 1/5 * log 1/5)
3. Knowing the entropy of a language is important because it measures the average information content of symbols and it also sets a lower limit on encoding efficiency.

Lecture 33

1. This is so because the probability of getting a H is already ¾ so having it twice turns it into 9/16 and so on.
2. It is 27 because we are counting the number of bits created for each result
3. Naïve encoding

Symbol	Probability	Naïve
1	2/12	000
2	2/12	001
3	3/12	010
4	3/12	011
5	1/12	100
6	1/12	101

4. h = -(2 * (2/12) * log (2/12) + 2*(3/12) * log(3/12) + 2*(1/12) * log(1/12))
5.

Symbol	Probability	Encoding 1
1	2/12	00
2	2/12	01
3	3/12	10
4	3/12	110
5	1/12	1110
6	1/12	1111

6. 2 1's take 2 * 2 = 4 bits

2 2's take 2 * 2 = 4 bits

3 3's take 3 * 2 = 6 bits

3 4’s takes 3 * 3 = 9 bits
1 5 takes 1 * 4 = 4 bits
1 6 takes 1 * 4 = 4 bits

Everything is equal to 31 bits for encoding 1
The naïve encoding would use 36 bits for 12 rolls