Name: Terry Liang
EID: twl378
CSID:tliang
Email: liang810612@hotmail.com

Assignment2

Lecture 17

1. No. Because NI policy is not transitive.
2. They would not be able to interfere with each other.
3. No. Because it specify which subjects are allowed to interfere with which other subjects.
4. B has a higher level than A.

Lecture 18

1. NI policies is an expressive, intuitive policy that mimics the confidentiality metapolicy.
2. L1,l2,l3, …,lk, ….
3. There are lots of interferences in real system, most involve low-level system attributes, many interferences are benign.

Lecture 19

1. We need to know if we can trust certain context and believe it's legit. We need to know what the correct information are and what are not.
2. Because they have more confidence in those commercial software that have the ability to produce/handle information.
3. Separation of duty: several different subjects must be involved to complete a critical function.

   Separation of function: a single subject cannot complete complementary roles within a critical process.

4. It is about recoverability and accountability require maintain an audit trail.
5. The subjects might write something that would benefit him or herself.
6. In the bank, the transaction made by the teller and the program that the teller is using should not be created by the same teller.

Lecture 20

1. A only classified-level person but with professional on military strategies.

   A top secret general and tell information about physics.
2. Row1: physics expert is more reliable than student

   Row 2: a Novice with knowledge of physics and art is not as reliable with a physics expert

   Row 3: a student that know about art can at least teach the novice who knows nothing.
3. Anything that the low integrity subject do should not has effects visible to high integrity object. HO -> SL

   Low integrity object should not have effect visible to SL. OL -> SH
4. They should not be related to each other. They require different sets of labels and can be enforced separately.

Lecture 21

1. Because it is using simple integrity property and integrity *-property that are similar to BLP.
2. Because they have different contents that cannot be evaluated in this control policy.
3. If we were to protect both integrity and confidentiality, then no.

Lecture 22

1. A subject's integrity level falls if it ever read low integrity information.
2. No.
3. It assumes the subject can properly filter the information it receives.
4. Yes.

Lecture 23

1. Yes.
2. It allows system controllers to move software from development to production.
3. Yes.
4. The weak tranquility.

Lecture 24

1. Commercial security has concerns on consistency.
2. The transaction balanced, the account number.
3. Number of chairs in the banks, or the cookies provided in the bank
4. Certification is that the results have to follow the certification rules and Enforcement is the rules need to follow during procedures.
5. (user, TP, { CDI set})

Lecture 25

1. Because the consultant might be able to read some information that is disadvantage to the other airlines.
2. Yes.
3. Bank of America, Wells Fargo, Citicorp
4. Chinese Wall Policy is designed to address a very specific concern: conflicts of interest by a consultant or contractor.

Lecture 26

1. It is easier to administer.
2. Active roles is what currently occupies. Authorized roles is allowed to fill at various times. The set of active roles is a subset of authorized roles.
3. Role authorization: a subject's active role must be an authorized role for that subject.

   Transaction authorization: a subject can execute a transaction only if the transaction is authorized for one of the subject's active roles.
4. It is harder to administer, and are not more appropriate to the organization.

Lecture 27

1. Because it is expensive and usually unnecessary.
2. Access control list, capability-based system, a set of rules to compute access permissions "on the fly".

Lecture 28

1. Sender has either a yes or a no, the receiver knows that sender has one of those two possibilities.
2. We want to know how much information can be transmitted over a specific covert channel.
3. So they know what the information being sent represent.
4. Because there is a limited bandwidth of the channel.
5. Just 1 bit. Use 1 to represent yes.

Lecture 29

1. N-bit, 4 bits, 7 bits.

2. Because the receiver might have uncertainty on whether it is at dawn or dusk, or what time during the day, or which day.
3. 4 bits.
4. 8 bits.
5. Because they might be many uncertainties that the receiver will have.

Lecture 30

1. Bit1 means the binary digit and bit2 means a quantity of information.
2. 000,001,010,011,100,101,110,1113
3. Because we let message 10 to be only 1 bit, and the others are represent in 5 bits. On average, 95% will be message 10 so it’s 995 bits. And the other five messages would be 5*5 bits.
4. Because we can use less bits to represent message that would be appearing in a higher percentage.
5. 11000,10000,100001,10101.
6. We are sure of the on average of a message. We are certain of what every bits of information means.

Lecture 31

1. 2222.
2. 0,10,110,1110,11110,11111.
3. If there are more than 1 possible decoding, there will be uncertainty.
4. Because we do not want information changed after it is being sent to the receiver.
5. For example, E and S might cause some confusion when receiver reads it.

Lecture 32

1. $-\log(1/8) = 3$
2. $-(1/4*\log(1/4)+3/4*\log(3/4) = 0.7219$

3. It sets a lower limit on encoding efficiency.

Lecture 33

1. The efficiency will be better than 1 flip.
2. Because HH is 9*1 bits HT is 3 *2 bits , TH is 3 * 3 bits ,and TT is 1 *3 bits = 27
3. 000,001,0110,011,100,101
4. About 2.295
5. 1=> 0 , 2 => 10 , 3 => 110, 4 => 1110 , 5 => 11110, 6 => 11111
6. Yes, the naïve encoding requires 60 bits and mine requires only 49 bits.