Neil Jones
EID: nj2977
CSID: nfjones
email: neil.franklin.jones@gmail.com

Week 2 Questions

Lecture 17:

1. No, it is possible for the system to ignore its related NI policy.

2. A B (no link)

3. No, NI policies govern all information flow.

4. (H, H), (L, H), (L, L)

Lecture 18

1. They don't contain specific rules for who can read/write particular objects.

2. l1, l2, …, lk

3. It is difficult to account for all possible flows of information.

Lecture 19

1. It is important because data ought to be reliably correct.

2. They may require software to conform to a specific architecture.

3. Duty: Several people must be involved to complete a function.
Function: A single person cannot complete complementary roles in a critical process.
If you have both then you need multiple people and none of them can fill more than one role in the process.

4. It determines if data has been compromised and who is responsible if it is.

5. The movement of systems from machine to machine while maintaining data integrity.

6. The purchase history of a customer must always maintain its integrity in the database.

Lecture 20

1. New York Times, A CIA report on prospective terrorist cells

2. If L1 = (A, {B}) and L2 = (C, {D}), L1 dominates L2 only if A >= C and B >= D

3. S_L cannot alter information of a higher integrity level.

4. One does not affect the other. They are independent concepts.

Lecture 21

1. The rules are flipped. The direction of domination flips.

2. Neither dominates the other.

3. No.

Lecture 22

1. Subjects integrity levels can be lowered through reading bad information.

2. No.

3. Subjects won't be corrupted by reading bad information.

4. Yes.

Lecture 23

1. No, they are orthogonal.

2. New additions may corrupt the system and cause the need for a rollback.

3. Yes.

4. Soft Tranquility

Lecture 24

1. To maintain the integrity of data and keep track of who has done what in the system as well as ensuring that all subjects are who they say they are.

2. Bank balances, checks, etc.

3. Candy in a bowl, business cards, etc.

4. Certification: assertions about current system state.
   Enforcement: rules regarding system actions.

5. A bank teller altering the balance of a customer after a withdrawal.

Lecture 25

1. They could potentially share information about one company with another.

2. Yes, they are not in the same conflict class.

3. Any company that is in a different conflict class from the one previously accessed.

4. It manages conflict of interest between subjects and many systems instead of specifically managing subject object interaction within a particular system.

Lecture 26

1. You can separate your subjects into equivalence classes. It is much more efficient.

2. Active roles are the roles currently assumed. Authorized roles are those that may be assumed.

3. Role: the active roles of S are a subset of the authorized roles of S.
    Transaction: A transaction may only be completed if the transaction is in the set of transactions enabled by S's active roles.

4. They are too fine grained. There is the possibility that a subject may have a combination of labels which gives them more power in the system than they ought to have.

Lecture 27

1. It isn't necessary because it is cheap to compute it on the fly.

2. Access control lists, capabilities

Lecture 28

1. The receiver and sender must have agreed on a schema.

2. So we can tell how much information is being transferred.

3. So they can each tell what the other is “saying.”

4. It would be a waste of bandwidth to transfer unnecessary bits.

5. 1, either yes (1) or no (0).

Lecture 29

1. n bits
    4 bits
    7 bits

2. Where is the attack? What time specifically? The amount of uncertainty of the receiver defines the specificity of the message received.

3. 4, 2^4 = 16

4. 8 bits, 256 = 2^8

5. There will always be things that the receiver doesn't know. The method of sending information may not be totally reliable. We may have to use error correcting codes and thereby waste bandwidth on redundancy.

Lecture 30

1. 1: A quantum of digital information.
   2: An indistict small amount.

2. 000
   001
   010
   011
   100
   101
   110
   111

3. 995 will be message 10 (0) and the other 5 messages take 5 bits each (5 * 5)

4. It allows us to calculate the expected value and assign bit patterns accordingly.

5. 100
   101
   110
   111

6. We will be transmitting the smallest amount of information required for the receiver to correctly interpret the message.

Lecture 31

1. 1238

2. 1: 000
   2: 001
   3: 010
   4: 011
   5: 100

6: 101

3. If a language isn't uniquely decodable, then the receiver will not know which symbols have been transmitted when they receive a duplicate code.

4. It ensures that all of the information intended to be transferred is sent in its entirety.

5. It is not uniquely decodable.

Lecture 32

1. $-8 * (1/8 * \log_{2}1/8) = 3$

2. $-(4/5 * \log_{2}4/5 + 1/5 * \log_{2}1/5) = 0.72$

3. It lets us know the lower limit of the encoding efficiency for the language.

Lecture 33

1. The probabilities are calculated from the product of the respective probabilities of each independent event.

2. Out of 16 flips we can expect each pattern to occur a number of times equal to the reciprocal of its probability. The sum of the reciprocals is 27.

3. 1: 000
2: 001
3: 010
4: 011
5: 100
6: 101

4. $-(2 * 6/10*\log_{2}6/10 + 2 * 3/10*\log_{23}/10 + 2 * 1/10*\log_{2}1/10) = 2.59$

5. 1: 00
2: 01
3: 100
4: 101
5: 110
6: 111

6. It is able to drop a bit for the highest probability symbols (1, 2).