Lena Ko
CS361
LK5399
ko.lena92@gmail.com
Questions Week 2

Lecture 17

1. Any MLS policy can be turned into a non-interference policy. This is because Si can interfere with Sj if Sj interferes with the level oif Sj.

2.

3.No, interference policy restricts who can interfere with who, therefore limiting channels.

4. A and B could either be both high, both low, or B as high and A as low.

Lecture 18

1. The NI policies better resemble metapolicies because they show that confidentiality should take place without the use of rules. There are no rules about subjects reading/writing which objects, like policies.

2. l1, l2, l3, ….,lk

3. Proving NI for realistic systems is difficult because interferences are very common and including everything L could ever observe is a lot.

Lecture 19

1. Integrity is concerned with who can write or modify information. One may be more inclined to believe a source more depending on its integrity. For an object, integrity is a characterization of trustworthiness. The more integrity something has, the more one is more likely to believe it. For a subject, integrity measures the confidence one placeds in its ability to produce.

2. A company may opt to purchase commercial software rather than download a similar free version because it is more trustworthy, has more integrity. It is difficult to trust a free available version and rely that it will work as well as the commercial software.

3. Separation of Duty states that several different subjects must be involved to complete a function while separation of function states that a single subject cannot complete more than one role within a process.

4. Auditing proves how much integrity a commercial setting has.

5. Lipner raises integrity concerns based on the idea that integrity is more important than confidentiality in commercial settings. Commercial security controls are often discretionary, procedural, and decentralized rather than mandatory and centralized.

6. Integrity may be more important than confidentiality in gradebooks. It is more important that the grades are not changed rather than its confidentiality.

Lecture 20

1. Highly reliable with little sensitivity: patient allergy data
   Low reliability with high sensitivity: anonymous poll data

2. An expert in physics has greater integrity than a Student in physics so the expert dominates the student. A Novice in Physics and Art has less integrity than in Expert in Physics so the Expert dominates the Novice. The student of Art has greater integrity than the Novice in nothing so the student dominates the Novice.

3. In terms of integrity, a high level subject could interfere with a low level subject, but not vice versa. Information should not flow up.

4. Confidentiality and integrity or orthogonal issues because they do not relate, and you have to deal with them separately.

Lecture 21

1.It is the exact opposite of the BLP model.

2. They have different categories so it is impossible to compare them.

3. Access is only allowed if both the confidentiality and integrity requirements pass.

Lecture 22

1. Biba assumes that subjects' levels can be changed, and they float down if they read information, showing they are not trustworthy.

2. No, subjects aren't considered trustworthy. Therefore, they float lower than the information that they read.

3. The ring policy believes that the subject can read any object.

4. The subject is considered trustworthy and capable of filtering out bad information.

Lecture 23

1. SD refers to programs under development category and ID refers to the development category under integrity, so yes.

2. Downgrade means to move software from the development to production which means changing the label.

3. A system controller can modify development code/test data.

4. weak tranquility

Lecture 24

1. David Clark and David Wilson argued that commercial security has its own unique concerns so there should be another model. The main concern is consistency among the components of the state. The four fundamental concerns are a part of reasonable commercial integrity.

2.CDI: bank balances, checks

3.UDI: candy from a bowl

4.Certification Rules lay out how the system certifies that a particular data object is in a valid state. Enforcement Rules make sure that already-certified data object stays certified (maintains its integrity) as the system interacts with it.

5. A banker must have permission to withdraw and deposit a person's account.

Lecture 25

1. Someone who is involved in two separate entities of the same category has a conflict of interest. He may carry some sensitive information.

2. Yes, the GM files are of the same company within the same conflict class.

3. If it is the same company datasets as the object has already accessed or belongs to a completely different conflict class.

4. BLP is more of a vertical model, subjects have access to read down only if the subject has a greater level than the object. The Chinese wall policy is more horizontal. Subjects can read information as long as it doesn't cross the wall of different conflict classes.

Lecture 26

1. A subject can have multiple roles, which gives them many transactions, activities that someone in that roles is permitted to carry out. Flexibility.

2. Authorized roles can be filled at various times and active roles are the ones that are currently occupied.

3. Role authorization means that a subject's active role must be authorized role for that subject, and a transaction authorization means a subject can only execute a transaction if the transaction is authorized for one of the the subject's active roles.

4. Roles are more flexible than standard access control policies. Everyone in one role has the same permissions, are more appropriate to the organization, one subject has various functions, and allows a subject to transition between roles without changing identity.

Lecture 27

1. You wouldn't build an explicit ACM for an access control system because in realistic systems, most systems don't have access to most objects.

2. Storing permissions with subjects: Access control list (ACL): Any request by subject S for access A to object O, check whether A is in the Set of P in the pair S,P on O's access control list.

Storing with subjects: capability -based system: Each subject S maintains a collection O,A meaning that S has a current permission to perform access A to object O, capability is type of ticket. Possession of a capability is de facto, no access check is required.

Computing permissions on the fly: no storage.

Lecture 28

1. The receiver needs to know how to interpret a 1 or 0, and which means yes or no.

2. It may be easier to manage the information of a message, more efficient.

3. Sender and receiver must have some shared knowledge and an agreed encoding scheme in order to effectively communicate and interpret the answer.

4.You need to think about the bandwidth of the channel, the capacity a channel can hold.

5. 1 bit, you could send a bit of 0 for no and a bit of 1 for yes.

Lecture 29

1. 4 bits of information in each.

2. If the only uncertainty were whether dawn or dusk it takes one bit, if the attack could have come anytime during the day takes questionable bits, and if the day was uncertain that would also take questionable bits.

3. 4 bits,
Each bit could be either of 2 messages

4. log2 256= 8

5. In ideal situations, each bit transmitted can reduce the uncertainty by half, but most do not.

Lecture 30

1. bit as a discrete binary number and bit as a continuous quantity of information

2. 000,001,010,100,111,110,101,011

3. 995 messages are good messages + the 5 extra messages for each bad messages

4. Knowing the prior probabilities of messages lead to a more efficient encoding because we are able to decide the minimum number of bits needed to encode a message.

5.10001,10010,10100,11000

6. It would have to be the best code possible for that message.

Lecture 31

1.2,4,6,4,2

2. 0,1,10,101,010,000,

3.An encoding must be uniquely decodable so that a message is not decoded into the wrong message.

4.Lossless is desirable because you may want to recover the original sequence of symbols.

5. It is not streaming, there is a break between each letter so the receiver can't distinguish those possiblities.

Lecture 32

1. -(1/8 * log 1/8 + 1/8 * log1/8)= -(-3/8 + -3/8)= ¾

2. -(4/5 * log 4/5 + 1/5 * log 1/5)= ~0.722

3. It defines how optimal your coding is by measuring average information content of symbols in the language.

Lecture 33

1. According to the probability out of 16 double flips HH has 9/16, HT and TH has 3/16, and TT has 1/16

2.By multiplying the number of bits in the code by the count gives us expected number of bits.

3. 000,001,011,100,101,110

4.

1 3/22 9
2 3/22 9
3 6/22 18
4 6/22 18
5 2/22 6
6 2/22 6

5. -(3/22log3/22+3/22log3/22+6/22log6/22+6/22log6/22+2/22log2/22+2/22log2/22)

5. 0,10,110,111,1110,1111

6. Naive code would be 66/66 while this code would be 52/66.