Haoshu Yuwen
Hy2892

Questions: Week 2

Lecture 17
1. No. We clearly have shown that with the BLP model, covert channels may exist to pass information from high to low. Since non-interference requires that high should never be able to communicate with low in any way, BLP can possibly violate non-interference.

2. A should not interfere with B and B should not interfere with A.

3. No by definition if it is implemented correctly.

4. A could by low and B could be high. Or A and B could both be high or both be low.

Lecture 18
1. They resemble meta-policies because non-interference only specifies who can interfere with whom in the abstract. It says nothing about functionality: A cannot write to B or B cannot write to A etc.

2. l1, l2, l3 …. Lk

3. It's difficult to prove for realistic systems because L's view must be the same for any sequence of instructions. If the sequence were set like in question 2, then it would be simple.

Lecture 19
1. Integrity is important in that data is content sensitive. Wrong data is as bad if not worse than no data. For example, integrity is very important in student grades. If anyone could change them, then the grades lose total meaning as a measure of academic achievement.

2. Just like the newspaper example, paid software tends to have more credibility than freeware. For example, paid virus scanners like Norton most likely have more bility Even if reputable, free software has the association of being limited.

3. Separation of duty demands that multiple actors are required to accomplish one action where as separation of function demands that a single actor may not accomplish more than one role in a critical process.

4. It allows you to detect errors in integrity.

5. Integrity is often more important than confidentiality, violations of integrity can be done internally, integrity relates to credibility, users commonly use programs written by others, applications are developed on contrived data, etc.

6. Again in the case of grades, letting unauthorized access is not as bad as inaccurate reporting or unauthorized modification.

Lecture 20

1. High credibility low sensitivity: Kanye West claims his baby is doing great.
Low credibility high sensitivity: Army private Josh claims the D-day invasions will occur in Canada.

2. Row 1: A physics expert dominates a student in physics.
Row 2: A novice in physics does not dominate an expert in physics.
Row 3: A student in physics dominates a novice in physics.

3. A can interfere with B if A dominates B.

4. Orthogonal implies that the two issues are not related. Just because something is credible does not necessarily make it sensitive and vice versa.

Lecture 21

1. Biba is almost exactly the same as BLP in terms of policy in that simply replace the word security level with integrity level and flip relations and you have Biba instead of BLP.

2. Subject 3 cannot read or write Object 3 since subject 3 is not knowledgeable for topic C.

3. No.

Lecture 22

1. The assumption is that if a subject reads a level lower than itself, it may be "corrupted" and its integrity level will be lowered.

2. No

3. The assumption is that the subject has the common sense to filter out bad information.

4. Yes

Lecture 23

1. Yes

2. Application developers and system developers do not have access to production data. If they need production data, that data must be downgraded.

3. Yes

4. Weak tranquility

Lecture 24

1. To address the differences between the needs of military security and commercial security.

2. Bank account balances and Checkbooks

3. Mints at a dentist's office and acorns on the lawn

4. Certification rules are rules that checks whether data is valid. Enforcement rules prevent actions that would possibly affect the integrity of the data.

5. The cashier at Walmart is not allowed the change the price of a computer to 5 dollars.

Lecture 25

1. American Airlines and United Airlines are direct competitors. A consultant may bring sensitive information between the two companies and cause an unfair advantage for one or the other.

2. Yes

3. You can access a company's files if you have not already accessed another company's files that belonged to the same conflict class.

4. Unlike BLP, the Chinese Wall policy deals with conflicts of interests. It doesn't deal with confidentiality within your company.

Lecture 26

1. It's more efficient. Instead of assigning everyone a long list of permissions, associate the permissions with roles and instead assign roles.

2. Authorized roles are roles that an individual may do at some point that's not necessarily now. Active roles are roles the individual is actively engaged in at the current moment.

3. The role authorization is basically a more general version of transaction authorization.

4. RBAC is easier to administer and in RBAC, transitions are made much easier.

Lecture 27

1. It's not very efficient considering most commercial operations have thousands of subjects and thousands of objects. It's much easier to just calculate on the fly.

2. Access Control List, Capability Based System, on the fly

Lecture 28

1. The receiver must know that the sender has two alternative options.

2. That way, you can calculate how much information there is and how much/fast information is being passed.

3. If no agreed encoding scheme exists, then regardless what the sender sends, the receiver may not understand the data, which is the equivalent of receiving no data at all.

4. For starters, it wastes space.

5. In the context of the yes or no question, 1 bit.

Lecture 29

1. n bits, 4 bits, 7 bits, 176 bits in ASCII

2. We can easily cut down the number of bits used if we use special encodings. Therefore, the size of the message depends on the receiver's knowledge of the sender's algorithm.

3. 4 bits. The receiver knows that there are only 16 possible messages. Therefore, we can simply order the messages and send a number corresponding to that message instead of the actual message.

4. 8 bits

5. Information transfer is a very dynamic process. Therefore, methods suitable for one situation may not be suitable for another.

Lecture 30

1. In computer science, a bit represents one piece of binary data, either one or zero. In the colloquial sense, a bit is synonymous with "some," and therefore the exact quantity is not known.

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

3. Under the naïve encoding 1000 messages would take 5000 bits because each message is 5 bits. However, if the receiver and sender agree that the message represented by 00000 is cut down to 0, it cuts down the size significantly.

4. If we know a message is more likely, then we can specifically encode that message as something short and efficient which would cause the information transfer in general to be more efficient.

5. “message 1” “message 2” “message 3” “message 4”

6. If it’s possible to find an optimum encoding, then a third party actor can easily determine what your encoding is.

Lecture 31

1. “2468”

2. 0 00 000 0000 00000 000000

3. If a message in not uniquely decodable, then multiple message would appear the same to the receiver and the receiver would have no way to decipher what the sender meant.

4. A lossless encoding means that you can easily get back to the original message from the encoding. Without this, messages may get distorted with noise.

5. It does not fulfill the streaming requirement.

Lecture 32

1. Log 8

2. –(.8*log.8 + .2*log.2)

3. It allows you to pick a minimum encoding scheme.

Lecture 33

1. Because those are the expected values. Expected values are calculated by probability multiplied by the value of event.

2. Because not every message is created equal in terms of bit length. Because we know that HH is the most likely outcome, we make it the shortest.

3. 000 001 010 011 100 101

4. 5 = .0833 | 3 - .1667 | 1 = .25
-2 (.0833*log.0833 + .1667*log.1667 + .25*log.25)

5. 0 10 110 101 1110 11111

6. This is more efficient cause it will use less bits.