CS361 Intro to Computer Security Daniel Rosenwald
Young, Bill June 19, 2014

EID: dpr447
CS login: randose
Email: danielrosenwald@gmail.com

Week 2

Lecture 17

1. No, because BLP only deals with information flow, while non-interference is a more discrete term that takes covert channels into account as well.
2. The NI policy would simply be reflexive – A and B would not be connected by any arrows.
3. No, covert channels cannot exist in an NI policy because the relationships are explicitly stated that information flow can only occur along the arrows, thus eliminating the system with which covert channels can be made.
4. They could both be Low, they could both be High, or A could be Low while B is High.

Lecture 18

1. NI policies better resemble metapolicies because they are nicely abstract. They explicitly state the flow of information, and therefore also implicitly state the non-flow of information in its complement.
2. L would see l1, l2, l3, …., lk
3. The more inclusive a view is, the fewer ways H has to interfere with L. So, in theory, including every single component would eliminate interferences from H to L. However, it's difficult to provide NI for realistic systems because eliminating all channels of potential interference in a real system would most likely eliminate that system's functionality.

Lecture 19

1. Integrity is important to supplying and modifying data, as it controls the allowance of authorizations. It's also important in separating assets.
2. Because the actions of a company can sometimes affect millions of people, they would buy a commercial software because a lot of hard work goes into making those systems secure and integral as compared to freeware on the market.
3. Separation of Duty differs from separation of function in that while the former requires a group to complete an action, the latter ensures that one person cannot perform multiple roles within the group.
4. Auditing is important in the event of something bad occurring, it provides solid information with which to work and resolve the issue.
5. Lipner's concerns with integrity lie with the foundational separation of function concept of integrity. He's worried that those who do jobs should not also write the software that they use for those jobs.

6. In the commercial world, such as in the context of a bank, integrity is more important than confidentiality.

Lecture 20

1. A highly reliable, low sensitivity piece of information could be the IP address that you get directed to when you type “google.com” into your address bar on a web browser. The reverse could be the timing, in milliseconds, that a government network triggered a nuclear bomb.
2. In row 1, label 1 dominates label 2 because they share the same area of expertise, meaning technically that label 2’s areas are a subset of label 1’s, and label 1 is of a higher level. So, it dominates. In row 2, even though the subset condition is satisfied, the sequential level of label 1 does not trump that of label 2. Novice < Expert, so there is no domination. Finally, row 3 is a dominates relationship because the empty set is a subset of all sets, and student is higher than novice.
3. We don’t want bad information to “taint” good information. So, the NI metapolicy for integrity it would be: information can only flow down in integrity.
4. It means that they are two separate issues that only tangentially intersect. Therefore, they both require their own set of labels and rules of information flow (metapolicy).

Lecture 21

1. Biba Integrity is called the “dual” of the BLP model because their policies are the “inverse” of each other.
2. The entry for Subj3 – Obj3 is blank because their need-to-know categories are disjoint sets, so neither category dominates the other.
3. No. Your operation should satisfy both sets of requirements to allow an access.

Lecture 22

1. The assumption is that the subject is only as good as the information it reads. Not much credit to the subjects.
2. The subjects are not considered trustworthy.
3. It kind of assumes the opposite, where the subjects are entirely trustworthy and will not be influenced by lower-integrity information.
4. Yes, they are considered more trustworthy.

Lecture 23

1. Although they are categories for two separate components of security, namely confidentiality and integrity, they are related. They designate to each component of security that this object or subject is being developed or development-related.
2. System controllers need to downgrade in order to move products from development to production.

3. No!
4. The downgrade signifies weak tranquility – which literally means that labels can be changed.

Lecture 24

1. The purpose of the four fundamental concerns of Clark and Wilson is to establish a basic reasonable commercial integrity model. Authenticate to be identified properly, audit to keep track of modifications, well-formed transactions so as to only manipulate data in constrained ways, and finally separation of duty to make sure only certain people can do certain things.
2. CDIs could be cash at a bank, inventory at a sporting goods store, or services provided at a day spa.
3. UDIs could be freebies given out or other such insensitive material.
4. Certification is different from enforcement in that the former provides a set of rules to implement and follow and while the latter provides constraints under which to operate.
5. (Teller, Withdraw, {Client's account balance}).

Lecture 25

1. Because the consultant could carry some proprietary information that is sensitive within the industry.
2. Yes.
3. Any file from the current company (GM), or any file from a company who doesn't conflict with GM.
4. Unlike the BLP model, the Chinese Wall policy tackles the issue of a conflict of interest by a consultant or contractor.

Lecture 26

1. Benefits include delegating a set of permissions to an entire group, rather than individual cases. This allows management of a large company possible.
2. Active roles are those being done now, while authorized roles are those that an individual can take up at some time.
3. Role authorization and transaction authorization are different because one ensures the individual is allowed to take on a role, and the next ensures that one of the individual's roles allows a certain transaction to be made.
4. They aren't as easy to administer as RBAC. Also, they're pretty general, whereas RBAC makes roles a lot more specific to allow realistic functions within a company.

Lecture 27

1. Because in realistic systems, most subjects don't have access to most objects.
2. Access control list (ACL), capability-based system, "on the fly".

Lecture 28

1. The sender must only send one bit, however the receiver must be listening for that bit and also understand how to interpret the data sent.

2. In order to see exactly how much data is being transmitted.
3. Because that’s how the receiver will know a message is being sent and the sender will know the message is being received. There needs to be a protocol, as in with any transfer of information.
4. The sender wouldn’t want to transmit more data than the receiver needs because it is useless. We only need to send as much data as is necessary.
5. Just 1. A yes or no question warrants a simple 1-bit answer, a 1 representing yes and a 0 representing no.

Lecture 29

1. n bits of information, 4 bits of information, 7 bits of information.
2. Because the information content of a message is the amount of uncertainty it solves.
3. Just 4 bits, because each message could be encoded to a 4-bit string which can represent 16 different possibilities.
4. 7 bits.
5. Very few are ideal because we would like the freedom to say whatever we want when sending messages, and therefore our encoding will be a lot less efficient.

Lecture 30

1. The second definition of bit is a continuous flow where the first is a discrete binary digit.
2. 000, 001, 010, 011, 100, 101, 110, 111
3. For 1000 messages, 995 of them will be a 1-bit message of “0” and for 5 out of 1000 it will be a 5-bit message of the error code. So, 1020 bits are used for 1000 messages or 1.02 bits per message.
4. If we know prior probabilities, we can streamline our message to rely on the recurrence of certain common messages, thus cutting their bit count down and reducing the amount of bits needed in the more common messages.
5. 000000, 000001, 000010, 000011
6. If it’s possible to find an optimal encoding it means we can verifiably prove that there are no better encodings.

Lecture 31

1. “28462”
2. 1: 00, 2: 01, 3: 10, 4: 110, 5: 1110, 6: 1111.
3. It should be uniquely decodable so the receiver can recover – unambiguously – what the sender intended to say.
4. Lossless encoding is desirable because we want to make sure the receiver gets the entire transmission.
5. Morse code doesn’t satisfy our criteria for encoding because it is not streaming, and it is also prefix-free.

Lecture 32

1. –(1/8 * log(1/8) + … + 1/8 * log(1/8)) = 3

2. –(4/5 * log(4/5) + 1/5 * log(1/5))
3. It’s important to know the entropy of a language because it tells you that you can’t find an encoding that does better on average than the entropy.

Lecture 33

1. We get those expectations by multiplying the chances of getting the first flip by the second. So, HH is 9/16 because of ¾*3/4 and so on.
2. You get the total of 27 by adding up the amount of each result * the number of bits its encoding uses.
3. 1: 000, 2: 001, 3: 010, 4: 011, 5: 100, 6: 101.
4. –(6/20 * log(6/20) + 6/20 * log(6/20) + 3/20 * log(3/20) + 3/20 * log(3/20) + 1/20 * log(1/20) + 1/20 * log(1/20)).
5. 1 and 2 are both 6/20, 3 and 4 are both 3/20, and 5 and 6 are both 1/20. So, if 1: 00, 2: 01, 3: 100, 4: 101, 5: 110, 6: 111, we’d have a more efficient encoding. 2*6 + 2*6 + 3*3 + 3*3 + 3*1 + 3*1 = 48. So, by using this language we would have an average of 48/20 = 2.4 bits per message.
6. My encoding is more efficient because it delegates less bits to the most common messages, thereby reducing the average.