Sean Villars
stv223
stvillars8@gmail.com

Lecture 17
1. If a computer system complies with the BLP model, does it necessarily comply with non-interference? Why or why not?
Yes, all BLP models are non-interference models, but not necessarily the other way around. BLP allows for information to only flow in one direction at a time and that is the same with non interference.

2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?
A and B cannot interfere with each other.

3. Can covert channels exist in an NI policy? Why or why not?
Yes, there are other covert channels such as system and timing channels that could subvert the non-interference policies.

4. If the NI policy is A−> B, in a BLP system what combinations of the levels “high” and “low” could A and B have?
B is high A is low

Lecture 18
1. Why do NI policies better resemble meta policies than policies?
Because the purpose of NI is to not restrict flow of information between specific subjects and doesn’t really tell you how to go about to doing that.

2. What would be L’s view of the following actions: h1, l1, h2, h3, . . . , hj, l2, l3, . . . , lk
l1, l2, l3...lk

3. What is difficult about proving NI for realistic systems?
A lot of low level interferences occur that are hard to prove.

Lecture 19
1. Explain the importance of integrity in various contexts.
When reading a magazine, you base the credibility of the story on the integrity of the publishing magazine. When referring to objects, integrity is the amount of trustworthiness it has. A subjects integrity level is the amount of confidence you place in them to handle information.

2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?

The company might have a solid reputation and they might not want to spend the time verifying the source code of an open source system.

3. Explain the difference between separation of duty and separation of function.
Separation of duty has to do with several different subjects being involved to complete a critical function while separation of function is where a single subject cannot complete complementary roles within a critical process.

4. What is the importance of auditing in integrity contexts?
To double check that the integrity policies are enforcing the integrity stability that they are supposed to.

5. What are the underlying ideas that raise the integrity concerns of Lipner?
Giving people too broad of control over critical processes.

6. Name a common scenario where integrity would be more important than confidentiality.
Banking systems, I wouldn't mind as much if someone saw the $50 in my bank account but would very much mind if that got changed to $1

Lecture 20
1. Give examples of information that is highly reliable with little sensitivity and information that is not so highly reliable but with greater sensitivity.
Stock prices for the first, and business rumors such as mergers acquisitions etc.

2. Explain the dominates relationships for each row in the table on slide 4.
It is the same for confidentiality, high dominates low if low is a subset of high.

3. Construct the NI policy for the integrity metapolicy.
The NI policy would be to not let info flow up. Only let info flow down as to not let low integrity info taint high integrity info.

4. What does it mean that confidentiality and integrity are “orthogonal issues?”
They are almost opposite, but meet in the middle.

Lecture 21
1. Why is Biba Integrity called the “dual” of the BLP model?
Because it is the opposite of the BLP model.

2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
Because object3 is not a subset of subject 3, does not dominate, subject 3 cannot access any of its info.

3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?
No

Lecture 22
1. What is the assumption about subjects in Biba's low water mark policy?
You are initially trustworthy, but if you deal with information that is lower than you then you lose some of your trustworthiness.

2. Are the subjects considered trustworthy?
Somewhat, they can lose their trustworthiness though, float down.

3. Does the Ring policy make some assumption about the subject that the LWM policy does not?
It puts more trust regarding confidentiality, but the same amount for integrity.

4. Are the subjects considered trustworthy?
In regards to confidentiality, yes.

Lecture 23
1. Are the SD and ID categories in Lipner's model related to each other?
Yes, they both have to do with development, but SD deals with confidentiality and ID deals with integrity.

2. Why is it necessary for system controllers to have to ability to downgrade?
In order to ship code out to production.

3. Can system controllers modify development code/test data?
Yes, only programs under development. Not systems programs in development.

4. What form of tranquility underlies the downgrade ability?
Weak tranquility. It does not violate the spirit of the security policy.

Lecture 24
1. What is the purpose of the four fundamental concerns of Clark and Wilson?
To ensure the utmost integrity and consistency in a commercial environment.

2. What are some possible examples of CDIs in a commercial setting?
Funds in a bank account.

3. What are some possible examples of UDIs in a commercial setting?
Surveys that a company has.

4. What is the difference between certification and enforcement rules?
Enforcement is how to carry out the certifications.

5. Give an example of a permission in a commercial setting.
Teller is allowed to access a customer's account.
Lecture 25
1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?
Because they know internal information of both companies who are competitors with each other.

2. In the example conflict classes, if you accessed a file from GM, then subsequently accessed a file from Microsoft, will you then be able to access another file from GM?
Yes because they are not related and are not competitors.

3. Following the previous question, what companies' files are available for access according to the simple security rule?
All of them.

4. What differences separate the Chinese Wall policy from the BLP model?
In Chinese Wall, if you have read you also have write access.

Lecture 26
1. What benefits are there in associating permissions with roles, rather than subjects?
Less overhead. You can define a few roles and set all of the security properties of the roles and then assign people to roles instead of evaluating each individual person.

2. What is the difference between authorized roles and active roles?
Authorized roles are all the roles a person has, and active is the role they are currently occupying.

3. What is the difference between role authorization and transaction authorization?
Role authorization is if a person is allowed to occupy the role. Transaction authorization is whether the person's role is authorized to carry out the transaction.

4. What disadvantages do standard access control policies have when compared to RBAC?
They aren't as efficient or practical as RBAC.

Lecture 27
1. Why would one not want to build an explicit ACM for an access control system?
It is very inefficient and can quickly grow to be enormous.

2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.
Access control list, capability-based system, on the fly.

Lecture 28
1. What must be true for the receiver to interpret the answer to a “yes” or “no” question?
That there is an agreed upon scheme as to what a yes or no is.

2. Why would one want to quantify the information content of a message?
So they can build systems accordingly and create efficient ways of delivering the messages.

3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
If they didn’t then they wouldn’t know what to do with all of the 1’s and 0’s

4. Why wouldn’t the sender want to transmit more data than the receiver needs to resolve uncertainty?
Sending less data is more efficient.

5. If the receiver knows the answer to a question will be “yes,” how many bits of data quantify the information content? Explain.
none, if they know it will be yes then they don’t need to know any more information.

Lecture 29
1. How much information is contained in each of the first three messages from slide 2?
n bits, the rest depend on the encoding scheme. If it is just the naive scheme then a single digit would be 4 bits, double digit would be 7 bits, and the last one depends on ascii or unicode etc.

2. Why does the amount of information contained in “The attack is at dawn” depend on the receiver’s level of uncertainty?
They might know there will be an attack, just not when. They might not know if there is an attack at all. Therefore the amount of info is what is needed to resolve uncertainty.

3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
4 bits if we are using the naive scheme. 2^4 is 16

4. How much information content is contained in a message from a space of 256 messages?
8 bits of information.

5. Explain why very few circumstances are ideal, in terms of sending information content.
Something could get lost which could ruin the information.

Lecture 30

1. Explain the difference between the two connotations of the term “bit.”

One refers to the discrete bit, 1 or 0, and the other refers to a bit as a chunk of information (continuous).

2. Construct the naive encoding for 8 possible messages.

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

3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.

Because of the entropy formula. We know that one message has a much higher probability of being received so we encode it as a single bit.

4. How can knowing the prior probabilities of messages lead to a more efficient encoding?

Because we can then encode them with less bits.

5. Construct an encoding for 4 possible messages that is worse than the naive encoding.

111111111, 111111110, 111111101, 111111011

6. What are some implications if it is possible to find an optimal encoding?

The entropy formula will give you the lower bound and you can go from there.

Lecture 31

1. Name a string in the language consisting of positive, even numbers.

2426246264262

2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.

00, 01, 10, 110, 1110, 1111

3. Why is it necessary for an encoding to be uniquely decodable?

Because otherwise you might misinterpret a message.

4. Why is a lossless encoding scheme desirable?

Because of course you don’t want to lose information!

5. Why doesn’t Morse code satisfy our criteria for encodings?

Because it doesn’t satisfy the prefix rule.

Lecture 32

1. Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).

2.079

2. If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?

$-(1/5 \log 1/5 + 4/5 \log \tfrac{4}{5}) = .5$

3. Why is knowing the entropy of a language important?
It tells you the lower limit of encoding efficiency.

Lecture 33
1. Explain the reasoning behind the expectations presented in slide 3.
Since they are two flips, you multiply the probabilities together.

2. Explain why the total expected number of bits is 27 in the example presented in slide 4.
Summation of the number expected * the number of bits to encode.

3. What is the naive encoding for the language in slide 5?
000, 001, 010, 011, 100, 101

4. What is the entropy of this language?
$-(\tfrac{3}{5} \log \tfrac{3}{5} + 3/10 \log 3/10 + 1/10 \log 1/10) = 0.89$

5. Find an encoding more efficient than the naive encoding for this language.
0, 10, 110, 101, 100, 111

6. Why is your encoding more efficient than the naive encoding?
Because it uses less bits