Lecture 17

1. Computer Systems that compile with BLP also comply with non-interference since any MLS policy can be written as a NI Policy.
2. A and B can not interfere with each other
3. if the NI policy is strong there should be no covert channels since subjects can only interfere with correct subjects. How ever the more limited the view is the more chances there are for covert channels to exist. So it is possible depending on the amount that is in the view.
4. A would have to be low and B would have to be high for A->B.

Lecture 18

1. NI policies are more like metapolicies since there are no specific policy rules or mechanisms like BLP. It is therefore more abstract and more like a metapolicy.
2. L1, L2, L3,...,Lk.
3. It is difficult to prove NI since there are many interferences in real systems. Low level system attributes and conditions such as encrypted files make it more difficult.

Lecture 19

1. Integrity is important for making sure information is left intact with the proper information. It is important in commercial industries such as banking, law, and hospitals which require records to be correct at all times.
2. Someone may opt to purchase commercial software over freely available versions due to the persuasive degree of integrity. Free could be seen to be less trustworthy than commercial software.
3. Separation of duty requires more than one subject to complete one function. Separation of functions requires that a subject can't hold two complementary roles.
4. Auditing is important so that you have the ability to place accountability and possibility of rolling back issue and restoring things to previous states.
5. NO user written programs, test on non production systems using contrived data, moving from development to production requires a special person, process must be controlled and audited, managers and auditors must have access to system states and logs.
6. Integrity would be more important in the commercial world such as in banks or law offices.

Lecture 20
1. Nutrition labels are highly reliable with little sensitivity and patient volunteered information is not so highly reliable but has greater sensitivity.
2. Experts are greater than students, Novice is less informed than an expert, and Students tend to know more than Novices.
3.
4. We should treat confidentiality and integrity separately since they are different goals. High security clearance for confidentiality does not always equal high trustworthiness for integrity. Therefore we need two different labels.

Lecture 21

1. Bilba Integrity is the dual of BLP since things are essentially flipped. Instead of read down write up it's read up write down for integrity.
2.

3. No both sets of labels must pass.

Lecture 22

1. Biba's low water mark policy assumes subjects can become corrupted by untrustworthy data.
2. Subjects are not considered trustworthy at least not always.
3. Ring policy assumes subject is able to differentiate between low and high integrity information.
4. The subjects are considered trustworthy in the ring policy for the most part since they are expected to use their own common since.

Lecture 23

1. Yes the SD and ID categories are related to each other. SD is just the confidentiality potion while the ID is the integrity portion.
2. It is important for system controllers to have the ability to downgrade so that when development is done it's able to be used by lower production.
3. Yes since they are at a higher level than development code.
4. Weak Tranquility underlies the downgrade ability.

Lecture 24
1. The purpose of their four fundamental concerns is to help establish an integrity policy for commercial settings with a focus on consistency.
2. Examples of CDIs in commercial settings include hospital records, legal documents, dreamworkds new unreleased film.
3. Examples of UDIs in a commercial setting include Ice chips in hospitals, water from a drinking fountain.
4. Certification is concerned with verification that operations meet rules while enforcement looks to ensure those certification requirements are met and proper authorization is met.
5. Our system administration has permission to add or delete programs from different computers that we can't. (System Admin, TP, {programs}).

Lecture 25

1. the consultant may carryover confidential information from American Airlines to United Airlines. They are competing companies so this could be damaging.
2. Since GM and Microsoft are not competing and not in the same conflict class they would be able to access another file from GM.
3. Anyone from outside the GM conflict class are available for access. So Bank of America is an example of an acceptable company.
4. The difference is permissions change dynamically and depend on the history of accesses.

Lecture 26

1. Benefits of roles rather than subjects include no need to go person by person to assign levels. Easier to maintain for example if something needs to be added to the tellers duties.
2. Authorized roles are roles they may occupy at some point. Active roles is a subset of authorized roles that describes the roles they are doing at the moment.

3. role authorization are the roles for which the subject is authorized to do. The transaction authorization are the tasks a subject is authorized to do.
4. Some disadvantages include more time consuming and difficult to administer. More constraining for commercial purposes (read a file instead of “open an account”). Does not as easily recognize that subjects can have various functions. Not very easy to move between roles with same identity.

Lecture 27

1. ACMs are usually very sparse since most subjects don't have access to many objects.
2. Access control list, capability based system, permissions on the fly.

Lecture 28

1. For yes or no questions the receiver must have an agreed upon meaning for a 1 or 0 valued bit. Therefore must be a set number of bits for the answer.
2. One may want to quantify the information content of a message to know how much information to expect and what to expect. You may not know where the message starts and stops otherwise.
3. To understand the stream of info coming in. A stream of bits may simply look like a stream of random normal bits if you don't understand the encoding scheme.
4. More data then needed to resolve uncertainty can be a waste, confusing, and more noticeable.
5. If the receiver knows it will be “yes” then no bits are needed as you already have your answer. If you were unsure between say “yes” and “no” then you would needed 1 bit minimum.

Lecture 29

1. first message: n-bit binary = n bits, second message: single decimal digit = 4 bits, third message: a two decimal number = 7 bits.
2. The info contained depends on how much we need to send. If the receiver knows the info is about the time (dawn or dusk) of the attack then “dawn” is all that's needed (aka 1 bit).
3. 4 bits because 2^4 = 16 and you just assign one message to each bit pattern.
4. 8 bits for 256 messages. If you sent 256 messages * 8 bits = 2048.
5. Sending information is not always ideal since we may not know exactly how much information is needed so we may have to revert to a less optimal option such as ASCII for “the attack is at dawn” instead of just 1 for “dawn” or 0 for “dusk.”

Lecture 30

1. Bit can mean a discreet number while the other is a continuous measurement.
2. M0 = 000, M1 = 0001, M2 = 010, M3 = 011, M4 = 100, M5 = 101, M6 = 110, M7 = 111.
3. Since M0 has 99.5% probability, of the thousand messages 995 will be M0. We can assign 0 (or 1 bit) to M0. This gives 995 bits. We will then need 5 bits for the 5 non M0's (1 signal bit and 4 choose bits).
4. We can have a lower bit number for high probability messages which will lower the total number of bits.
5. M1 = 100 M2 = 101, M3 = 110, M4 = 111.
6. If it is possible to find an optimal encoding that means there is a bound on the smallest number of bits that someone can use for a situation.

Lecture 31

1.
2. 1 = 1, 2 = 10, 3 = 110, 4 = 1110, 5 = 11110 6 = 11111
3. An encoding must be uniquely decidable so that confusion over what is meant is avoided. Also good to avoid arbitrary “look-ahead.”
4. Lossless encoding is desirable so that information is not lost and the whole message and meaning get across to the receiver.
5. Morse code is not prefix-free encoding. For example take e and s in Morse code. E = . S = … does a transmission of … equal three Es or does it mean an S?

Lecture 32

1. Entropy of an 8 sided die is 3.
2. Entropy of the language is .7219 bits.
3. Entropy is important for giving us the theoretical lower bound on the number of bits necessary to send the message. This in turn gives us the optimal solution to the efficient encoding problem.

Lecture 33

1. In slide three you transmit more information with less overall bits. So you wait till you have flipped twice to send information instead of every flip. You combine the probabilities of each possible pair. Then you give the one with the largest probability the lowest possible number of bits and the next largest probability the next lowest and so on.
2. Using the probability you find the expected number of flips for each possibility which gives you your count. Use that number times the number of bits used for that flip possibility (the code). Add them all up and that give you 27 bits with the probabilities and efficient coding scheme.
3. On slide 5 the naïve encoding is 3 bits.
4. The entropy of this language is 2.295
5.1 = 0, 2 = 10, 3 = 110, 4 = 1110, 5 = 11110, 6 = 11111
6. Uses 49 bits with the probabilities than the 60 bits that the naive encoding uses.