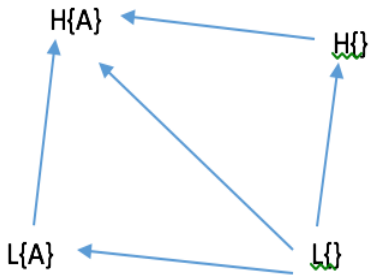
Week 3 Questions

Lecture 11

1. I would give the subjects high levels and the objects a level that is lower than the subjects'. Since you can read down, this would ensure that the subject's level was higher.
2. Building an access control matrix for a BLP system would not be a good idea because it would be huge for most realistic systems.

Lecture 12

1. 

2. To find the greatest lower bound, find the lowest level, then find the greatest amount of attributes available. To find the least upper bound, find the highest level, then find the least amount of attributes available.
3. The upward flow in the lattice really is the metapolicy because what we really care about is to constraint the flow of information among the different levels. The upward flow shows the flow of information from low to high and any other flow violates the security goals.

Lecture 13

1. The metapolicy is a flow only from L to H. BLP rules only allow you to read down and write up, which means that information can
2. The READ operation satisfies BLP because it satisfies the Simple Security Property and does not violate the *-Property. The WRITE operation satisfies BLP because it satisfies the *-Property and does not violate the Simple Security Property. Neither operation violates Strong or Weak Tranquility Property; they do not change levels.
3. The CREATE operation satisfies BLP because it does not violate Simple Security Property or *-Property, and neither Tranquility Property because it is creating the object and setting the level. Therefore, the level has no been changed and Tranquility Properties has not been violated. The DESTROY operation satisfies BLP because it satisfies *-Property and does not violate the Simple Security Property. The subject has permission to modify the object.
4. There must be a flow, occurring via a system resource, within a system that violates the security metapolicy.
5. The DESTORY will get rid of the object so that the two subjects can do the process of transferring of information for SH to SL again.
6. No, in the first case, the file has a value of 1 after the write and in the second case, the file has a value of 1 after the write.

7. SL does the same thing in both cases because it trying to determine if SH is sending it information. By writing to the file in both cases, you can tell if the file can be written to or not, which would tell you if SH is trying to send information.
8. SH does different things to send a bit of information from SH to SL. Yes, depending on what SH does, information may or may not be sent to SL.
9. If SH creates a file before SL can, SL can only write to the file. If SL can read or not read the file, this would signal to SL whether SH is trying to send it information or not. This violates the metapolicy because we are trying to prevent information from flowing from top to bottom.

Lecture 14

1. Two humans talking over coffee is not a covert channel because it is not flow between two subjects within a system.
2. No, because there is no flow of information from SH to SL. SL cannot read from F0 since it is a high level object. There is not way for SH to indicate that it was trying to send a bit of information to SL.
3. It is in the system state.
4. It is in the ordering or duration of the events on the system.
5. It is in the system state and in the ordering of events on the system.
6. It is in the flow of a program.
7. A termination channel may have a low bandwidth because there may not be many computations that terminate.
8. The low level object must be able to sense power consumption and the high level object must be able to modulate the power consumption.
9. A computer.

Lecture 15

1. A covert channel may be putting out one bit of information at a time, but covert channels on real processors can operate at a thousand bits per second.
2. It is infeasible to eliminate every potential covert channel because there are many different covert channels. You may not think of all the different channels to eliminate.
3. You can introduce noise into the channel to limit bandwidth, or modify the system implementation to eliminate the covert channel.
4. There are two processes. Process 1 can create and delete objects, while process 2 can only read the objects.
5. For process 1 to send information to process 2, it can create an object that process to will read and interpret as either 0 or 1.

Lecture 16

1. The operation does not tell you directly that a file has been created; it has been inferred. Create needs to tell you that a file exists to know for certain that "file existence" has been Referenced. There is no way for the receiver to get this information.
2. When R and M are in the same row, it says that there is a mechanism to reference AND modify, which leaves open a potential channel to be exploited.
3. No, this does not indicate a potential covert channel because each column is referring to a single operation. Under a READ operation, if you had a R under file existence and M under file size, there is no shared attribute for a subject to modify and reference.
4. Creating a SRMM table gives a systematic way to investigate potential covert channels.