Week 2 Questions

Lecture 5

1. A metapolicy for a military database could be to protect confidential national security information. A metapolicy for a cell phone network is to protect information being sent through its network.
2. A metapolicy may be too general to provide adequate guidance, so a policy may be necessary to give more details to accomplish the metapolicy. For example, if the metapolicy was to protect a Facebook user's password, the metapolicy does not detail how it should be protected—just that it did need to be protected.
3.
    a. Only the student is able to see his or her grades, unless he/she grants permission for a parent to also see them.
    b. The registrar's office may change a grade for a student if a grade change is necessary.
    c. A professor may change a grade for a student only if that student is in his/her class.
4. Yes, a student may want his/her parent to be able to see his/her grades. So the policy would have to take that into consideration.
5. A likely metapolicy would be to protect students from identity theft.
6. The metapolicy gives you some direction to what you will be protecting. If you don't understand the metapolicy, you will not know how to go about protecting something. The policy will seem arbitrary without knowing the metapolicy.

Lecture 6

1. Military security is mainly about confidentiality because there is a large amount of information at many different sensitivity levels that need to be made sure that they are being read by the correct person with the correct clearance level. Yes, there are but we are only concerned with confidentiality at the moment.
2. The major threat is that information could end up being accessed by the wrong people. For example, the war plan is highly-sensitive information and you would not want the janitors to see that.
3. The proviso is there because our main concern is to protect information from users not authorized to see it. We are just making sure documents—that have already been finalized—are seen by the people who have access.
4. The labels used have a hierarchical and categorical component. The hierarchical component will show the sensitivity of the document. The categorical component indicates the type of information that is in the document.
5. We assume that whoever has put the labels on the documents has the clearance to see every document. It is not part of our concern because we are just trying to ensure that the information is being classified correctly.
6.
    a. The base softball game - UNCLASSIFIED
    b. The cafeteria is serving chopped beef - UNCLASSIFIED
    c. Col. Jones got a raise - CONFIDENTIAL
    d. Col. Smith didn't get a raise - CONFIDENTIAL
    e. Normandy invasion is schedule for June 6 - TOP SECRET
    f. Enigma codes have been broken - TOP SECRET
7. Personnel, War, Base
8. You want to label a highly sensitive document with the highest appropriate level because you do not want someone, who does have appropriate access level for the non-sensitive information in

the document, to also be able to access the highly sensitive information. By labelling a document with all categories in the document, only the people who work in both categories are able to see that document. This ensures that a person from Crypto can see what they are working on in Nuclear.

Lecture 7

1. A label can be affixed to a human by an identification card with their clearance information listed.
2. Labels on documents indicate how sensitive the information inside is. However, labels for humans indicate how trustworthy that person is—if we can trust them to look at highly classified information or not—and their need for the information.
3. The documents are the files that are on the computer; a file's permissions can be set to just the user, the group, or to everyone to see. The humans are the computer user.
4. The Principle of Least Privilege makes sense because you do not want to give someone information that they do not need to do their job. If you don't give them that information, they can't leak that information.
5.
    a. The individual has a higher clearance than the sensitivity of the document as well as the categorical clearance for crypto. Therefore he is allowed to access the document.
    b. The individual does not have a high enough clearance compared to the sensitivity of the document therefore he can't access it.
    c. The individual has a higher clearance than the document sensitivity and there are not categorical identifier therefore the individual has access to the document.

Lecture 8

1. The introduction of these vocabulary terms expands the view a little to encompass more items, not just military documents and military officers and employees.
2. The levels are hierarchical so they can be greater than or equal to, or less than or equal to making it reflexive. The levels are transitive because it is a hierarchy. If top secret is greater than secret and secret is greater than unclassified, then top secret is greater than unclassified.
3. There are security labels that do not dominate each other. Top Secret: Cyrpto and Top Secret: Nuclear do not dominate each other.
4. The labels would have to be identical to dominate each other.
5. If the person's clearance level is higher than the document's sensitivity level and the person has the categories of the document, then the person can read it.
6. It is "only if" because this is just a necessary condition, not a sufficient condition. There may be other security constraints in place that would not allow the person to read the document.

Lecture 9

1. Simple Security only ensures confidentiality for read access. To ensure confidentiality, we also need to restrict write access.
2. We need to make sure the information is not being written in the wrong place. i.e., a Top Secret document getting written to an Unclassified folder.
3. Computers have programs that are executing these processes for us. The user may be trusted to write information however we do not know if the program has malicious code in it that will leak information.
4. If the subject's level is lower than the object's, the subject can write up to the object.
5. Both subject and object dominate each other.

6. The General can have to accounts, one high-level and another low-level, so that the general can use the low-level account to send orders to the private.
7. Yes, it would be a problem of integrity that the corporal can overwrite the war plan. Another label can be created to specify which level you need to be in order to write to a document.

Lecture 10

1. A subject's level can be downgraded if the subject will not carry residual high-level information down; this would not violate the *-Property. Upgrading a subject's level would be bad because it would allow a low-level subject to now be able to read higher-level information, which would violate the Simple Security property.
2. There are times when a high-level subject may need to write to a lower-level subject or object. Using strong tranquility would not allow this and would violate the *-Property.
3. If an object is at Top Secret level and it is lowered to Unclassified level, now everyone is able to access and read the information. The information may be highly-sensitive information that is not wanted to be known to everyone yet. If the plans for D-Day were released before it happened, then the storming of Normandy would not have been a surprise and may not have been successful.
4. For a downgrade to be secure, the object must not have high-level information that would be carried down to the lower-level.