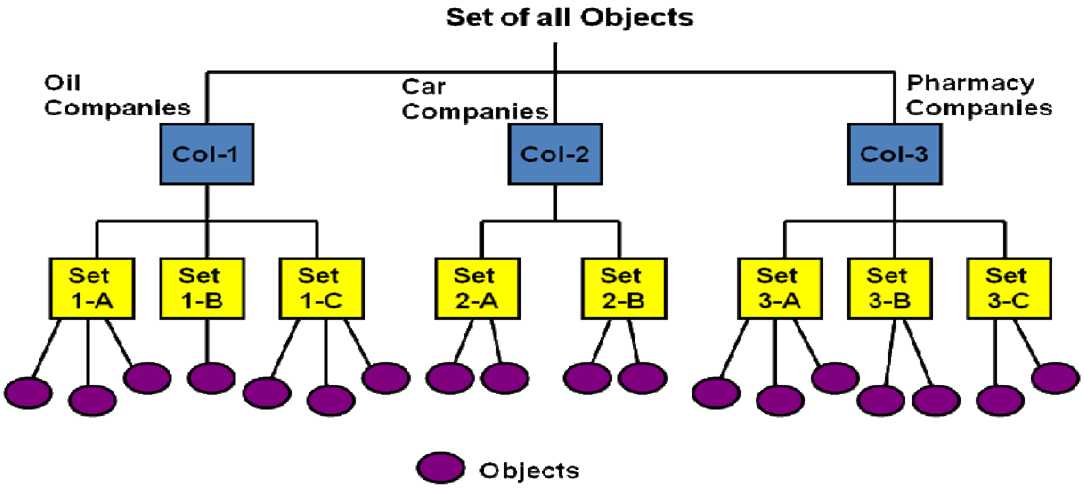
CSC 439/539 Advanced Information Security, Spring 2013, Instructor: Dr. Meghanathan
Sample Questions on Module 5: Access Control Models

1) Briefly state and explain the Read and Write rules of the Bell-LaPadula Confidentiality Model and the Biba Integrity Model?
2) What would be the UNIX command (along with the arguments) to set the following access rights for a text file A.txt
   a. Read, Write and Execute permission for the Owner of the file, Read and Execute permission for the users in the same group as the owner, Read permission for others
   b. Read and Write permission for the Owner of the file, Read permission for the users in the same group as the owner, Execute permission for others
3) What access permissions does a user needs to have to a folder in the UNIX OS to be able to:
   (a) List the contents of the folder
   (b) Create new files in that folder
   (c) Change his current working directory to the folder
4) What are the two primary disadvantages of the Discretionary Access Control Model? Explain with suitable example.
5) Briefly explain the Read rule, the original Write rule and its drawback, as well as the revised Write rule (including how it fixes the problem with the original Write rule) for the Chinese wall model.

Sample Solution: With the original Write rule, the second restriction ("No object has been read by S which is in a different data set to the one on which write is performed.") implies that the subject S should not have read objects from more than one data set in order to be able to do a write. This also implies that the subject S can write only to one data set. Overall, this means that in order to have Write access on a particular data set, the subject can have both Read and Write access only to that data set (called the native data set to which the Subject has access to by default). This would have severe access restrictions to even Read from other data sets.

The refinement to the Write rule is to be able to write objects that are sanitized (all proprietary, identification and sensitive information are removed) and that can be read. So, the Conflict of Interest (CoI) restriction is still maintained (according to the Read Rule); and if a Subject wants to write objects from one data set to another, provided the object is sanitized and the target (destination) data set to which Write is performed does not have any Conflict of Interest with data sets that have been already read.

6) Consider the data classification shown below. Assume a Subject S has so far accessed the following objects in the data sets of the different classes of Conflict of Interest:



(a) An object in the Data Set 2-B
(b) An object in the Data Set 3-A

Can the subject S read an object from the Data Sets in the following order? Explain why or why not?

(c) An object in the Data Set 1-C
(d) An object in the Data Set 2-A
(e) An object in the Data Set 3-A
(f) An object in the Data Set 1-A
(g) An object in the Data Set 3-B

7) For the data classification diagram shown in Question 6, assume the objects are sanitized. Also, assume as in Question 6, let the user be considered to have already accessed an object in data set 2-B and 3-A.

   (a) Can the Subject write an object from Data Set 1-A to Data Set 2-B?
   (b) Can the Subject write an object from Data Set 2-A to Data Set 3-C?

Sample Solution:
The basic idea is to validate whether the subject has "read" access to both the originating source data set from which an object is read and the target destination data set to which the object is written to. The "Read" rule ensures that both the source and destination data sets do not have any CoI with those that have been alread "read".

The subject S has already accessed objects from CoI-2 and CoI-3 (i.e., from data sets 2-B and 3-A).

(a) The subject wants to read an object from 1-A and write it to data bset 2-B.
Answer: The subject can read an object from 1-A (because the subject has not read any objects from any data set so far in the CoI-1). The subject can write to 2-B because the subject has already read an object from 2-B (so the subject has read access to 2-B), and the object is considered to be sanitized.

(b) The subject wants to read an object from 2-A to 3-C
Answer: The subject cannot read an object from 2-A (because the subject has already read an object from 2-B that is in the same Conflict of Interest as of 2-A). There is no need to check for "read" access to 3-C, since the "read" access check for the originating data set (2-A) itself has failed.

8) Explain why there needs to be a second condition: “No object has been read by S which is in a different data set to the one on which write is performed,” for the original Write Rule of the Chinese wall model? Why just the first condition (checking for read access) is not sufficient? Illustrate using an example.

Sample Solution: Look at the example illustrated in the slides to explain why the second condition is there for the original Write rule.

Let a subject John has already accessed objects in 1-A and 2-A (two different CoI classes - so fine). Let another subject Jane has already accessed objects in 1-B and 2-A. So, if the Read rule is only followed, if

John wants to read an object from 1-A and write to 2-A, he could do so, because he is reading from the same data set that he has already read. However, the object now gets written to a different CoI (2-A). Jane who has read objects from 2-A can now read this object and write it back to 1-B. As a result, an object of 1-A is now in 1-B (Note that 1-A and 1-B are in the same conflict of interest).

With the second condition of the Write rule - an object cannot be read from one data set to any other data set within the same CoI or even in different CoI. Of course, this is a much stricter restriction.

9) What is Sanitization? What is the modified Write rule of the Chinese wall model?
10) Explain the motivation to use the RBAC model for large database systems compared to the DAC and MAC models.
11) Explain the following terminologies related to the RBAC model:
    (a) RBAC Session
    (b) Core RBAC
    (c) Hierarchical RBAC
    (d) Constrained RBAC
12) When do you say that a role *r* dominates another role *r*' according to the RBAC model?
13) Explain the principle behind Multi-Level Secure (MLS) databases and how it could lead to polyinstantiation? You can choose an appropriate simple example to put forth your explanation.

Sample Solution: If a user is denied permission to add a record (differentiated using primary keys) that is already there in the table, at a higher privilege level, then the user will infer that the record with the higher privilege level is there in the table – because even though he cannot see the record when he lists the contents of the table, he was not allowed to add a record with the same primary key. To avoid such an inference in MLS databases, we allow a user at a lower privilege to add a record (based on a primary key for which a record at a higher privilege already exists in the database) in the table. So, we now have a situation where there are two or more records with the same primary key (referred to as Polyinstantiation). We are thereby violating the traditional rule of databases that there can be only one record with a particular primary key.

14) What is the difference between visible and invisible polyinstantiation?

Sample Solution: Invisible Polyinstantiation corresponds to giving permission for a lower privileged user to add records at clearance levels lower than those that are currently in the database. When a lower-level user queries for all the records in the database, he can only see records at his clearance level or lower level. The records at privilege levels higher than the security clearance level of the querying user are not displayed.
Visible Polyinstantiation corresponds to giving permission for a higher privileged user to add records at clearance levels higher than those that are currently in the database. When a higher-level user queries the database, he can see both the low-level records as well as those created by him at the higher-level. Hence, the name “Visible” polyinstantiation.

15) Assume a database has 4 records (rows), each represented at a unique security clearance level. Consider the four security clearance levels to be: Top Secret, Secret, Confidential and Unclassified. The primary keys and the security clearance level of the 4 records are shown below.

Primary Key	Security Clearance Level
PK1	Top Secret
PK2	Secret
PK3	Confidential
PK4	Unclassified

(a) If **invisible polyinstantiation** is the only form of polyinstantiation that is allowed, then list all the possible records (with their primary key and the security clearance level mentioned) that could be entered into the database in addition to the above 4 records.

(b) If **visible polyinstantiation** is the only form of polyinstantiation that is allowed, then list all the possible records (with their primary key and the security clearance level mentioned) that could be entered into the database in addition to the above 4 records.

(c) If both invisible and visible polyinstantiation are allowed, what would be the maximum number of records that could be in the database and justify your answer?