Auto-Evaluation / Review Questions
(Access Control)

1. In the study context of Access Control, what means the AAA (or triple A) context?
2. Define what means a MAC Access Control policy.
3. Give an example of a manifestation of a MAC based access control policy
4. What means the term "discretionary" in a DAC (Discretionary Access Control) policy?
5. Present the difference between RBAC and ABAC access control policies.
6. Try to characterize the access control model implemented in work-assignment #2 in terms of MAC, DAC, RBAC or ABAC policy model. Why?
7. In a DAC policy model (but also for the generic case of ABC or RBAC), permissions can be described in different ways: access control matrix, access control lists or capabilities (or capability-based tickets).
    a. What are the differences of those types of access control means to describe permissions?
    b. In your work-assignment #2, how do you characterize the expression of privileges?
8. Define what is a Protection Domain. How is implemented the notion of protection domain in an UNIX based operating system (ex., Limux).
9. A user owning a file myfile (that is an executable file) executes the following command in the linux shell:

    1) chmod 750 myfile
    What permissions will result from the command execution?

    2) chmod 4750 myfile
    What permissions will result from the command execution? What is different compared with 1)?

    3) chmod 2750 myfile
    What permissions will result from the command execution? What is different compared with 1) and 2)?

    4) Supposing now a directory called mydir owned by a certain user. If the owner executes the following command what is the effect in terms of access control ?

    chmod 1750 mydir

10. In a RBAC model, in what consists to support role hierarchies?
11. In RBAC models, what is considered as RBAC reference models and tipology, ex., RAC0, RBAC1, RBAC2, RBAC3 and what are the differences in terms of RBAC entities, hierarchies and constraints?
12. What means the notion of mutually exclusive roles in a RBAC policy model?
13. What means the cardinality of an RBAC policy model?
14. What means the notion of pre-requisite role in a RBAC policy model?
15. In a ABAC model, what are the types of attributes that can be involved?

    - - -

16. List and define the three classes of subject in an access control system.
17. In the context of access control, what is the difference between a subject and an object?

18. Suggest a way of:
    a. implementing protection domains using access control lists.
    b. implementing protection domains using capability tickets.

    Note: you need in both cases a level of indirection

19. Assume a system with N job positions. For job position i, the number of individual users in that position is U_i and the number of permissions required for the job position is P_i.
    a. For a traditional DAC scheme, how many relationships between users and per- missions must be defined?
    b. For a RBAC scheme, how many relationships between users and permissions must be defined?

20. UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?