**Chapter 4 – Access Control**

**TRUE/FALSE QUESTIONS:**

T F 1. Access control is the central element of computer security.

T F 2. The authentication function determines who is trusted for a given purpose.

T F 3. An auditing function monitors and keeps a record of user accesses to

system resources.

T F 4. External devices such as firewalls cannot provide access control services.

T F 5. The principal objectives of computer security are to prevent

unauthorized users from gaining access to resources, to prevent legitimate users from accessing resources in an unauthorized manner, and to enable legitimate users to access resources in an authorized manner.

T F 6. Security labels indicate which system entities are eligible to access certain

resources.

T F 7. Reliable input is an access control requirement.

T F 8. A user may belong to multiple groups.

T F 9. An access right describes the way in which a subject may access an object.

T F 10. The default set of rights should always follow the rule of least privilege or

read-only access

T F 11. A user program executes in a kernel mode in which certain areas of memory

are protected from the user’s use and certain instructions may not be executed.

T F 12. Any program that is owned by, and SetUID to, the “superuser” potentially

grants unrestricted access to the system to any user executing that program.

T F 13. Traditional RBAC systems define the access rights of individual users and

groups of users.

T F 14. A constraint is a defined relationship among roles or a condition related to

roles.

T F 15. An ABAC model can define authorizations that express conditions on

properties of both the resource and the subject.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_\_\_\_\_\_ implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.

A. Audit control B. Resource control

C. System control D. Access control

2. \_\_\_\_\_\_\_\_\_\_ is verification that the credentials of a user or other system entity are valid.

A. Adequacy B. Authentication

C. Authorization D. Audit

3. \_\_\_\_\_\_\_\_\_ is the granting of a right or permission to a system entity to access a system resource.

A. Authorization B. Authentication

C. Control D. Monitoring

4. \_\_\_\_\_\_\_\_\_\_ is the traditional method of implementing access control.

A. MAC B. RBAC

C. DAC D. MBAC

5. \_\_\_\_\_\_\_\_\_\_ controls access based on comparing security labels with security clearances.

A. MAC B. DAC

C. RBAC D. MBAC

6. A concept that evolved out of requirements for military information security is \_\_\_\_\_\_ .

A. reliable input B. mandatory access control

C. open and closed policies D. discretionary input

7. A \_\_\_\_\_\_\_\_\_\_ is an entity capable of accessing objects.

A. group B. object

C. subject D. owner

8. A(n) \_\_\_\_\_\_\_\_\_\_ is a resource to which access is controlled.

A. object B. owner

C. world D. subject

9. The final permission bit is the \_\_\_\_\_\_\_\_\_ bit.

A. superuser B. kernel

C. set user D. sticky

10. \_\_\_\_\_\_\_\_\_\_ is based on the roles the users assume in a system rather than the user’s identity.

A. DAC B. RBAC

C. MAC D. URAC

11. A \_\_\_\_\_\_\_\_\_\_ is a named job function within the organization that controls this computer system.

A. user B. role

C. permission D. session

12. \_\_\_\_\_\_\_\_\_\_ provide a means of adapting RBAC to the specifics of administrative and security policies in an organization.

A. Constraints B. Mutually Exclusive Roles

C. Cardinality D. Prerequisites

13. \_\_\_\_\_\_\_\_\_\_ refers to setting a maximum number with respect to roles.

A. Cardinality B. Prerequisite

C. Exclusive D. Hierarchy

14. Subject attributes, object attributes and environment attributes are the three types of attributes in the \_\_\_\_\_\_\_\_\_\_ model.

A. DSD B. RBAC

C. ABAC D. SSD

15. The \_\_\_\_\_\_\_\_\_\_ component deals with the management and control of the

ways entities are granted access to resources.

A. resource management B. access management

C. privilege management D. policy management

**SHORT ANSWER QUESTIONS:¸**

1. X.800 defines \_\_\_\_\_\_\_\_\_\_ as the prevention of unauthorized use of a resource,

including the prevention of use of a resource in an unauthorized manner.

1. An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures is a(n) \_\_\_\_\_\_\_\_\_\_ .
2. \_\_\_\_\_\_\_\_\_\_ access control controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.
3. \_\_\_\_\_\_\_\_\_\_ access control controls access based on the identity of the requestor and on access rules stating what requestors are or are not allowed to do.
4. The basic elements of access control are: subject, \_\_\_\_\_\_\_\_\_\_, and access right.
5. Basic access control systems typically define three classes of subject: owner, \_\_\_\_\_\_\_\_\_\_ and world.
6. A \_\_\_\_\_\_\_\_\_\_ access control scheme is one in which an entity may be granted access rights that permit the entity, by its own volition, to enable another entity to access some resource.
7. The \_\_\_\_\_\_\_\_\_\_ user ID is exempt from the usual file access control constraints and has system wide access.
8. A \_\_\_\_\_\_\_\_\_\_ is a mapping between a user and an activated subset of the set of roles to which the user is assigned.
9. Role hierarchies make use of the concept of \_\_\_\_\_\_\_\_\_\_ to enable one role to implicitly include access rights associated with a subordinate role.
10. A \_\_\_\_\_\_\_\_\_\_ dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role and can be used to structure the implementation of the least privilege concept.
11. There are three key elements to an ABAC model: attributes which are defined for entities in a configuration; a policy model, which defines the ABAC policies; and the \_\_\_\_\_\_\_\_\_\_ model, which applies to policies that enforce access control.
12. The three types of attributes in the ABAC model are subject attributes, object attributes, and \_\_\_\_\_\_\_\_\_ attributes.
13. A \_\_\_\_\_\_\_\_\_\_ is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber.
14. In digital identity systems, a \_\_\_\_\_\_\_\_\_\_ functions as a certification program.