### 

### **3413ICT Network Security**

### **Workshop – 11B**

|  |
| --- |
| **Review Questions:**   * Explain and differentiate between the following access control policies: Discretionary access control (DAC), Mandatory access control (MAC), and Role-based access control (RBAC).   **Discretionary access control (DAC):** Controls access based on the ***identity*** of the requestor. It is called ***discretionary*** because an entity may have rights to enable other entities to access the resources  **Mandatory access control (MAC):** Controls access based on comparing the security labels of the objects with security clearances of the entity. ***Mandatory:*** an entity that has the clearance to access a resource may not, just by its own volition, enable other entities to access the resource  **Role-based access control (RBAC):** Controls access based on the roles of the user and on rules defining what accesses are allowed to users in the given roles   * Explain the following terms: * Access matrix:   subjects in one dimension  objects in the other dimension  each entry specifies access rights of the specified subject to that object     * Access control list (ACL):   Determine which subjects have which access rights, to a particular resource     * Capability ticket   A capability ticket specifies authorized object & operations for a particular user     * You are given the following access matrix     What is the access control list for “File 1”?  UserA, UserB, User C   * For the same access matrix given in Question 3, what are the capability tickets for Users B and C, respectively?   UserB: Read  UserC: Read, Write   * The relationship between users and roles are represented by the set of all possible pairs (*u*, *r*), where *u* is a user and *r* is a role. Suppose a company has 200 staff members (each staff member is a user) and 50 distinct roles. How many pairs, (*u*, *r*), does this company have?   50 x 200 = 10000  *Suppose a group of 10 users are assigned with 5 roles. There are 10 files that these users can access (Note that different users may be able to access different files with different permissions). For the following two matrices, users are represented by U1,…, U10; roles are represented by R1, …, R5; and files are represented by F1, …, F10. Answer the following Questions (6)-(8) based on these matrices.*           * Compare users U1 and U2, in terms of numbers of files that they can access and types of permissions by which they can access these files.   **U1: R1, R3, R5**  **R1: F1 (RWE), F2(RW), F6®, F9® R3: F4(RWE), F7® R5: F3(RW), F7®, F9(R,E)**  **# of unique files: 5**  **U2: R2, R3, R4 R2: F2(R,E), F4®, F8® R3: F4(RWE), F7®**  **R4: F2®, F6(RWE), F10®**  **# of unique files: 5**   * For each of the users U3, U4, and U5, list all the files that this user can access as well as the types of access rights.   **U3:R3**  **F4 (R,W,E), F7®**  **# of files: 2**  **U4:R1, R2**  **R1: F1(RWE), F2(RW), F6®, F9® R2: F2(RE), F4®, F5(RE), F8®, F10®**  **# of files:8**  **U5:R2, R3**  **R2: F2(RE), F4®, F5(RE), F8®, F10®**  **R3: F4(RWE), F7®**  **# of files:6**   * Among the 10 users, who can access the maximum number of files? What files can this user access? For each of these files, by what permissions can this user access it?   U10   * Explain what a constraint is in a RBAC model. List and explain the three types of constraints in the RBAC reference models that we have studied.   A defined relationship among roles, or a condition related to roles. Three types of constraints:    **Mutually exclusive roles** are roles such that a user can be assigned to only one role  The set of mutually exclusive roles should have non-overlapping permission (that is, for this type of roles, any permission can be granted to only one role)  The purpose is to increase the difficulty of collusion among individuals to thwart security policies    **Cardinality** refers to setting a maximum number with respect to roles  **Prerequisite** dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role – used to structure the implementation of the least privilege.   * In real-world applications, a role can be defined as a combination of official position and job function. Suppose an organization has 10 official positions and 20 job functions. How many different roles does this organization have?   10 x 20 = 200 roles   * The BLP model was developed for data confidentiality. Is this model effective to protect data integrity? Why or why not? |

Users with the same write permissions will be able to modify the file. The integrity of the file may change based on the number of users with access to the file. The BLP model does not protect data integrity, but provides access control to files that can be modified by multiple other users.