Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

May 29, 2023

Chapter 4 - 6 Review

Question

4.2 How does RBAC relate to DAC and MAC?

RBAC, or role-based access control is defined as “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 (Stallings & Brown, 2018. p. 109). This means that RBAC grants access to let’s say a file based on two things, the role that the user has, and if the role has permission to the file. MAC, or mandatory access control, on the other hand uses security labels which tells how sensitive or critical what is attempted to be accessed is and what security clearance is able to access the files, however, just because someone has access to a file does not mean that it can allow other users to access that same file (Stallings & Brown, 2018. p. 109). DAC, or discretionary access control, on the other hand, controls who can access what based on the identity of the requestor as well as access rules which states what the requestor is able to or in some cases not able to access and do (Stallings & Brown, 2018. p. 109). With DAC, a user is able to give access to another user to the same file if they have permission to do so (Stallings & Brown, 2018. p. 109). By looking at the definitions of RBAC, MAC, and DAC, it is clear

that they have some overlap in how they handle permissions and who can access what. For example, with an RBAC, users have roles and rules which states what they can and can't access, with an MAC there are security labels and anyone with clearance can access, similar to a role, and with a DAC it is based on their identity and access rules, similar to how a RBAC has each user have a role and rules within it saying what they can or can't access.

4.3 List and define the three classes of subject in an access control system

The three classes of subject in an access control system are: owner, group, and world (Stallings & Brown, 2018. p. 110).

Owner – The owner class of subject in an access control system defines who the creator of the resource, such as a file is, however, for a system resource who is listed as the owner may also be the system administrator, and in the cases of project resources the owner may be a project manager, project administrator, or another person may be assigned as the owner (Stallings & Brown, 2018. p. 110).

Group – The group subject defines a set, or group, of users who may have access rights to the file which is being looked at and if a user is in the group this may give them access rights to the project, it is also possible and often where a user belongs to multiple groups (Stallings & Brown, 2018. p. 110).

World – The world subject is the group of users with the least amount of access, and is granted to users who can access the system but may not necessarily be included in the subjects of owner or group (Stallings & Brown, 2018. p. 110).

4.4 In the context of access control, what is the difference between a subject and an object?

Within the context of access control, a subject is defined as “an entity capable of accessing objects” (Stallings & Brown, 2018. p. 109). Further, a subject “equates with that of process. Any user or application actually gains access to an object by means of a process that represents that user or application. The process takes on the attributes of the user, such as access rights.” (Stallings & Brown, 2018. p. 109). Simplifying this, a subject is the process, which is accessing something such as a file, however, the process represents a specific user or application such as an application with the right to access specific files.

An object is “a resource to which access is controlled” (Stallings & Brown, 2018. p. 110). Further simplifying this, the object is what the subject is trying to access, such as a file. However, an object can be almost anything such as records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, programs, bits, bytes, words, processors, ports, clocks, and network nodes (Stallings & Brown, 2018. p. 110).

4.5 What is an access right?

An access right is defined as “the way in which a subject may access an object” (Stallings & Brown, 2018. p. 110). In other words, these are the permissions themselves

which can be granted to users. These permissions can range from: read, write, execute, delete, create, and search (Stallings & Brown, 2018. p. 110).

Read – Having read access grants the user the ability to view information, such as a file, read access also grants the ability to copy or print, however, in some systems copy and print are separated permissions (Stallings & Brown, 2018. p. 110).

Write – Having write access allows a user to add, modify, or delete data in the thing which they are allowed the ability to access, such as a file, and by default includes read access (Stallings & Brown, 2018. p. 110).

Execute – Having execute access allows a user to execute, or to run, programs (Stallings & Brown, 2018. p. 110).

Delete – Having delete access allows the user to delete the specific thing in which they have access to, such as a file (Stallings & Brown, 2018. p. 110).

Create – Having create access allows the user to create new files, records, or fields (Stallings & Brown, 2018. p. 110).

Search – Having search access allows the user to list the files in a directory, and allows them to search through the directory (Stallings & Brown, 2018. p. 110).

5.1 Define the terms database, database management system, and query language

Database – A database is defined as “a structured collection of data stored for use by one or more applications. In addition to data, a database contains the relationships between data items and groups of data items” (Stallings & Brown, 2018. p. 149). In other words, this means that a database is a collection of data, such as personal information and employee information, which also contains the relationship between the different data items and groups of data items.

Database management system – A database management system is often a suite of programs which are used in order to build and maintain databases which will also often the ability to use querying functions (Stallings & Brown, 2018. p. 150).

Query language – A query language “provides a uniform interface to the database for users and applications” (Stallings & Brown, 2018. p. 150). However, I would also define it as a language which is used in order to perform queries, such as selecting rows if they meet certain criteria (Stallings & Brown, 2018. p. 150).

5.3 How many primary keys and how many foreign keys may a table have in a relational database?

A table can only have one primary key; however, a table can have as many foreign keys as it wants (Stallings & Brown, 2018. p. 152 - 153).

5.4 List and briefly describe some administrative policies that can be used with an RDBMS.

An RDBMS can have a large range of support for administrative policies, some of these policies are as follows: centralized administration, ownership-based administration, and decentralized administration (Stallings & Brown, 2018. p. 161).

Centralized administration – With a centralized administration there is often a small number of privileged users who can grant and revoke access rights to people and roles (Stallings & Brown, 2018. p. 161).

Ownership-based administration – With an ownership-based administration, the owner, or the creator of the table is who can grant and revoke access rights to the specific table (Stallings & Brown, 2018. p. 161).

Decentralized administration – With a decentralized administration, the owner of the table can grant and revoke authorization rights to other users, which will then allow them to grant and revoke access rights to the table to other people (Stallings & Brown, 2018. p. 161).

6.1 What are three broad mechanisms that malware can use to propagate?

Three broad mechanisms that malware can use to propagate are as follows: “infection of existing executable or interpreted content by viruses that is subsequently spread to other systems”, “exploit of software vulnerabilities either locally or over a network by worms or drive-by-downloads to allow the malware to replicate”, and “social

engineering attacks that convince users to bypass security mechanisms to install Trojan, or to respond to phishing attacks” (Stallings & Brown, 2018. p. 186).

6.2 What are four broad categories of payloads that malware may carry?

Four broad categories of payloads that malware may carry are as follows: “corruption of system or data files”, “theft of service in order to make the system a zombie agent of attack as part of a botnet”, “theft of information from the system, especially logins, passwords, or other personal details by keylogging or spyware programs”, and “stealthing where the malware hides its presence on the system from attempts to detect and block it” (Stallings & Brown, 2018. p. 161).

6.3 What characteristics of an advanced persistent threat give it that name?

There are three characteristics of an advanced persistent threat that give it its name, these are as follows: advanced, persistent, and threat (Stallings & Brown, 2018. p. 187).

Advanced – With an APT the attacker will use a wide variety of intrusion technologies and malware including building their own custom malware, however, the individual components of the attack may not be necessarily technically advanced they are selected carefully in order to work with the chosen target (Stallings & Brown, 2018. p. 187).

Persistent – With an APT, the attacker will be persistent, it may take an extended period of time to get what they want and to maximize their chances of success (Stallings & Brown, 2018. p. 187).

Threat – With an APT, they will pose a threat to the selected targets because of how they are organized, capable, well-funded, and their intent to compromise their chosen target (Stallings & Brown, 2018. p. 188).

In summary, an APT is also different from other attacks because of their careful target selection, their persistence, and often stealthy intrusion efforts over an extended period of time (Stallings & Brown, 2018. p. 187).

Problem

6.5 Consider the following fragment:

legitimate code

if data is Friday the 13th;

crash_computer();

legitimate code

What type of malware is this?

This is a logic bomb. A logic bomb is defined as “code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then

triggers some payload” (Stallings & Brown, 2018. p. 185). In this case, the injected code by the intruder is: “*if data is Friday the 13th; crash_computer();”*

This will run every time the program is ran, however, it will be dormant until the condition “if data is Friday the 13th;” which will then deliver the payload of “crash_computer();”. However more specifically, the book does not mention this, but this is a subcategory of a logic bomb and called a time bomb, which does the same thing as a logic bomb as it is a subcategory of a logic bomb but has a predetermined day that the selected payload delivers, acting as a sort of count down hence the name time bomb.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray