Role Based Access Control Case Study

James Early
Christopher Harris
Nafees Qamar
Bastian Tenbergen

October 2021

Role Based Access Control

Background

Modern organizational infrastructures are ubiquitous and are the backbone of organizations' productive environment. Many employees deal with the infrastructure, which consists of terminal computers, network switches and gateways, internet routers, internal and external servers as well as a plethora of services such as email or purchase order fulfillment. Ensuring that the proper personnel have access to the proper devices and services is just as important for productivity as it is to ensure that no unauthorized parties, internal and external, gain access to valuable resources.

Case Study Overview

In this case study, we will explore the challenges and solutions for a fictional university department regarding access control for personnel and network infrastructure. Before you begin, you should develop an understanding of Discretionary Access Control (DAC, see [1]), Mandatory Access Control (MAC, see [2]), and Role Based Access Control (RBAC, [3]). Be sure to read Chapter 14 in the CyBOK v1.1 as well as Chapters 11 and 12 in [4].

Student Instructions

Task 1:

Give an example Role-Based Access Control (RBAC) specification that cannot be expressed using Discretionary Access Control (DAC).

Task 2:

Assume you need to develop an RBAC policy for the class materials in an online course. Briefly describe the components of RBAC using an example of an online course you have taken in the past.

Task 3:

Describe a potential misuse of the resources from your example from Task 2 by one of the users (for instance, another faculty/student) that the access control model prevents.

Task 4:

Consider the scenario where an organization allows its employees to access confidential customers' data via a web site. To login to the website, employees use their last name and a password. For simplicity, the same password is assigned to all employees, and then delivered via unencrypted email. Describe a misuse of the web application by a malicious attacker. Explain the:

- Motivation
- Opportunity
- Method

What security technologies would you recommend mitigating the above misuse and why?

Task 5:

Indicate the read/write privileges for the following scenario of university departments: Let

- F1, F2 be faculty at Computer Science (CS); F3 Faculty at Electrical Engineering (EE); F4 Faculty at Human Computer Interaction (HCI); F5 faculty of all three departments.
- Resources r1 belong to CS; r2 to EE; r3 to HCI;
- Students s1, s2, s3, s4 belong to CC; s5, s6, s7 to EE; s1, s8 to HCI

Task 6:
Build an RBAC model to enforce the question 5 BLP (Bell–LaPadula model, [5]) rules. Note that the BLP model is another implementation of MAC.

Instructor notes

This case study may be assigned as a formative homework assignment, whole or in part, for a module on access control and authorization. The example solutions below are indications of what could minimally be considered correct for full points. Point values for tasks are at the instructor's discretion, depending on the grading rubric assigned in the course. Five points per task usually allow for a discretionary point system, e.g., 5 points for an excellent solution, 4 points for a good solution, and 3 points for an acceptable solution, with <3 points awarded for varying degrees of incompleteness. The instructor may consider doubling the point value for tasks 5 and 6 due to their more comprehensive nature.

Example solution

Task 1:
An example of Role-based Access Control that cannot be expressed using DAC is dynamic separation because DAC-based access control paradigms can only separate static duties. An example where dynamic separation is required is a scenario, where employees are supervised by some manager, but may in turn also supervise other subordinate employees. In contrast, statically separated privileges may entail access to facilities by employee location.

Task 2:
For example, the course CSC333/HCI530 "Privacy / Cybersecurity / Cryptography" at the State University of New York at Oswego is an online course typically offered during the summer session by one or two instructors. Each instructor manages the learning experience for up to 20 students per section using the online learning platform "Blackboard." The RBAC components there are:

- **Users:** students enrolled in the course, the instructors, and possible teaching assistants.
- **Roles:** Undergraduate or graduate students, teachers
- **Sessions:** Other roles a user can have. For example, a student in the course could be a teaching assistant in another course, or an instructor my herself take a course as a student at the same university.
- **Privileges:** Read, write access for users. For example, instructors have write access to assignment descriptions and due dates, while students only have read access to this item.
- **Privileges in the Session:** This includes all privileges and all inherited ones.

Task 3:
A potential misuse could be if a student achieves access to the date field governing the due date of the assignment. This student could extend their own solution preparation deadline, or perhaps disable read access for other students to some resources.

Task 4:
(Note, the following example is, of course, entirely fictitious)

- **Motivation:** Stewart, an employee, is angry that he was overlooked for a promotion that ultimately went to his colleague Theresa.
- **Opportunity:** One day, when Theresa went to lunch, Stewart sees that Theresa's office door is not closed and locked, but slightly ajar. Her computer is not locked, but her user account is logged in.
- **Method:** Since no one is in sight, Stewart decides to look up Theresa's account password in hopes to gain access to her account from his own workstation.
- **Mitigating Security Technologies:**
    1. A physical access dongle that locks the computer when not plugged in to the USB port of the computer might lock Theresa's workstation.
    2. A self-closing, self-locking door would prevent unauthorized office access.
    3. Employees must be required to change the delivered password at the first log-in to ensure that the unencrypted password is changed immediately, hence preventing misuse thereof.

Task 5:

Role	Read	Write
F1	R1	R1
F2	R1	R1
F3	R2	R2
F4	R3	R3
F5	R1, R2, R3	R1, R2, R3
s1	R1, R3	n/A
s2	R1	n/A
s3	R1	n/A
s4	R1	n/A
s5	R2	n/A
s6	R2	n/A
s7	R2	n/A
s8	R3	n/A

Task 6:

Here is a RBAC model that enforces the BLP rules for access control in a bank. The BLP rules call for a no read up, no write down approach. The main idea is to prevent higher level information from moving down.

Role	Read	Write
Manager	Customer, Teller, Loan Officer, Manager	Manager
Loan Officer	Customer, Teller, Loan Officer	Loan Officer
Teller	Customer, Teller	Teller
Customer	Customer	Customer

References

1. Wikipedia: "Discretionary Access Control." Online resource, last changed 1 October 2021. Available at: https://en.wikipedia.org/wiki/Discretionary_access_control, accessed 26 October 2021.

2. Wikipedia: "Mandatory Access Control." Online resource, last changed 17 March 2021. Available at: https://en.wikipedia.org/wiki/Mandatory_access_control, accessed 26 October 2021.

3. Wikipedia: "Role Based Access Control." Online resource, last changed 24 October 2021. Available at: https://en.wikipedia.org/wiki/Role-based_access_control, accessed 26 October 2021.

4. Ciampa, M.: "CompTIA Securit+ Guide to Network Security Fundamentals", 7th Edition, Cengage Learning, 2020. ISBN: 978-0357424377

5. Wikipedia: "Bell-LaPadula Model." Online resource, last changed 13 January 2021. Available at: https://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model, accessed 26 October 2021.