COURSE PROJECT

Discretionary Access Control

Instructions

The goal of this project is to apply the concepts we cover in this course to an example system. You should continue working on the same system that you used in the previous two courses.

In **Part One**, you will define an authorization relation for your system.

In **Part Two**, you will identify which parts of your authorization relation can be implemented with capabilities and design a capability scheme for your system.

In **Part Three**, you will design the remaining enforcement mechanisms for the rest of your authorization relation.

Except as indicated, use this document to record all your project work and responses to any questions. At a minimum, you will need to turn in a digital copy of this document to your facilitator as part of your project completion. You may also have additional supporting documents that you will need to submit. Your facilitator will provide feedback to help you work through your findings.

Note: Though your work will only be seen by those grading the course and will not be used or shared outside the course, you should take care to obscure any information you feel might be of a sensitive or confidential nature.

Complete each project part as you progress through the course. Wait to submit the project until all parts are complete. Begin your course project by completing Part One below. A Submit Assignment *button can be found on the final course project assignment page online. Information about the grading rubric is available on any of the course project assignment pages online. Do not hesitate to contact your facilitator if you have any questions about the project.*

Part One

Authorization Relation

The first step is to define an authorization relation for your system. To do so, first identify the users in your system and the commands in your system. Then specify which users are authorized to invoke which commands. Is your policy an example of discretionary access control (DAC)?

The system I have been working on is the electronic voting system, specifically the online voting system. The users of the system include

1. Electoral commissioners
2. System administrators
3. Eligible voters

Commands in the system include

1. Vote, that is casting a ballot: an individual is authorized to vote if he or she is eligible and has login credentials to access the voting system.
2. Grant access to electronic voting server
3. Grant access to server room
4. Monitor access to server and server room
5. Revoking access to server room
6. Access election data
7. Access election results
8. View election results

Which users are authorized to invoke which commands depend on their roles or functional requirements in the system.

1. An eligible voter can **vote** when they are authorized to do so.
2. System administrator in consultation with the head of electoral commissioners can **grant access** to the voting system for eligible voters
3. System administrator can **grant access** to the server room.

4. Senior security officers **monitor** the entrance of the server room
5. System administrator can **revoke access** to server room
6. All principals can view election results.

We have learned that discretionary access control (DAC) is an access control policy that is enforced over all subjects and objects in an information system or restricted area where the policy specifies that a subject that has been granted access to information or restricted area can

(i) pass the information to other subjects or objects;

(ii) grant its privileges to other subjects;

(iii) change security attributes on subjects, objects, information systems, or system components;
(iv) choose the security attributes to be associated with newly-created or revised objects; or

(v) change the rules governing access control.

From the characteristics of DAC, the voting system can not qualify as a DAC. Another form of access control like a mandatory access control will make the system more secure since the system has sensitive data.

We can focus on the lists of system administrators and electoral commissioners and physical tokens for access doors to server room.

An authorization policy for accessing the doors to the server room to let the administrators and electoral commissioners have physical tokens that they can use to access open the doors of the server room.

Commands in this part of the system include

1. I**ssue physical tokens:**

   The management of the system will create a department that will handle the creation and distribution of plastic ID cards to administrators and the electoral commissioners. The cards will be created and given to them on the same day; they will also have to choose their PINs upon creation.

2. **Grant access** to secure doors:
   This is an automated system.
   A user will need to insert his or her plastic card in a device that is installed to lock the door of the secure room. This device contains the credentials of the administrators and

electoral commissioners. The user will need to enter his or her PIN. IF there is a match, the door will be open; it will not open otherwise.

3. **Monitor**

   A team of security officers as well as security cameras will be at the door of the server room to ensure there is no spoofing.

4. **Revoke access**

   The management has the right to revoke access to the server room.

5. **Audit**

   The management can audit who has access to the server room.

Again since this is a very sensitive system, it will not be advisable to adopt discretionary access control.

Part Two

Authorization With Capabilities

Now you need to decide which parts of your authorization policy should be authorized by capabilities. You should then design a capability scheme to authorize those components. Feel free to revise some of your designs from Part One, if appropriate.

We have learned that a capability specifies an object and a set of operations that are authorized on that object and authorization is the process of giving someone the ability to access a resource.

The part of the authorization policy that could be based on capabilities are the **access election data** and **view election results**.

The election data and results are owned by the electoral commissioner and the system administrator. In order to access the election data, there should be a capability list that each user has access. The capability list could be a list of users and tokens that will be use to access data. With these capabilities, the system is able to check it the user is allowed to interact with the data. A user's capability can be revoked at the discretion of the owners. We note that data access is only limited to officials a the electoral commission. However result access can be extended to the public.

Part Three

Implementing Authorization

The final step is to design an authorization enforcement mechanism for the remaining parts of your authorization policy. Feel free to revise some of your designs from Part One and Part Two, if appropriate.

We learned that implementing an authorization means deciding how to represent whether principal P is authorized to perform operation op on object O, for all relevant P, op, and O.

In the electronic voting system, it would be good to implement the access control list.

In this implementation, a list of eligible voters together with their login credentials and capability to vote and to view election results, will be stored in a database. This will serve as a control access list.

To vote, an eligible voter need to enter their login in credentials. The system does authentication as a reference monitor to determine whether or not the user is eligible to vote. It the the user is eligible, authorization is granted.

To view election results, the user also needs to go through the same process of providing login credentials in order to view the results.

We note that in this implementation, the users cannot share the privileges they enjoy as eligible voters.

The same process is required for the electoral commissioners, only that they have elevated privileges. They can access election data and also view the election results..

REFERENCE

The lecture materials

To submit this assignment, please refer to the instructions in the course.