ACSESS CONTROL SYSTEM FOR THE BANK: DESIGN AND IMPLEMENTATION

Bushra Jabber Mohammed Jawad
Scientific adviser – asst. lecturer Abbas Fadhil Mohammed Ali
Computer Science Department – College of Science Kerbala University
bushra_comp@yahoo.com, abbaszain2003@ yahoo.com

Abstract

The access control system is a system used for protected information in many international companies. There are many ways to protect information, on of then by using the passwords that we use in this research. In this paper, access control system for a bank was presented.

1. Introduction

The primary purpose of security mechanisms in a system is to control access to information. Until the early 1970, it was not generally realized that two fundamentally different types of access controls exit. Discretionary access control is the most common: users, at their discretion, can specify to the system who can access their files. Under discretionary access controls, a user (or any of the users, programs or processes) can choose to share files with other users.
Under nondiscretionary or mandatory access control, users and files have fixed security attributes that are used by the system to determine whether a user can access a file. The mandatory security attributes are assigned or automatically by the operating system, according to strict rules. The attributes cannot be modified by users or their programs. if the system determines that a user's mandatory security attributes are inappropriate for access to a certain file, then nobody-not even the owner of the file-will be able to make the file accessible to that user [1].

2. Access control lists

One of the most effective access control schemes, from a user's perspective, is the access control list, or ACL. The access control list identifies the individual users or groups of users who may access the file. Because all the access control information for a file is stored in one place and is clearly associated with the file, identifying who has access to a file, and adding or deleting names to the list can be done very efficiently. Disadvantage of an access control list scheme is performance: the access control list has to be scanned each time any user accesses (or opens) a file. But with suitable defaults and grouping of users, access control lists rarely require more than a handful of entries. The only performance penalty might be due to there being an extra disk I/O required to fetch the ACL each time a file is opened. This could have a noticeable impact on systems where large numbers of files are opened in a relatively short time. Another disadvantage is storage management: maintaining a variable-length list for each file results in either a complex directory structure or wasted space for unused entries. This tends to be a problem only for systems having huge numbers of very small files (typical of the way in which Unix systems are used). Largely because of the complex management required, only a few systems provide the most general form of access control list. If performance is a problem, one approach is to employ a combination of owner/group/other and access control lists. The access control list is only used for files where the granularity of owner/group/other is insufficient to specify the desired set of users [2].

3. Capability list

Another type of access control is the capability list or access list. A capability is a key to a specific object, along with a mode of access (read, write, or execute). A subject possessing a capability may access the object in the specified mode. At the highest levels in the system, where we are concerned with users and files, the system maintains a list of capabilities for each user. Users cannot add capabilities to this list except to cover new files they create. Users might, however, be allowed to give access to files by passing copies of their own capabilities to other users, and they might be able to revoke access to their own files by taking away capabilities from others (although revocation can be difficult to implement). This type of access control, while much better than passwords, suffers from a software management problem. The system must maintain a list for each user that may contain hundreds or thousands of entries. When a file is deleted, the system must purge capabilities for the file from every user's list. Answering a simple question such as "who has access to this file?" requires the system to undergo a long search through every user's capability list.

The most successful use of capabilities is at lower levels in the system, where capabilities provide the underlying protection mechanism and not the user-visible access control scheme [3].

4. Access Control Techniques

Access control techniques are sometimes categorized as either discretionary or mandatory.

4.1 Mandatory access control

Mandatory access controls prevent some type of Trojan attacks by imposing access restriction that cannot be bypassed, even indirectly. Under mandatory controls, the system assigns both subjects and objects special security attributes that cannot be changed on

request as can discretionary access control attributes such as access control lists. The system decides whether a subject can access an object by comparing their security attributes. A program operating on behalf of a user cannot change the security attributes of itself or of any object, including objects that the user owns. A program may therefore be unable to give away a file simply by giving other users access to it. Mandatory controls can also prevent one process from creating a shared file and passing information to another process through that file.

Many different mandatory access control schemes can be defined, but nearly all that have been proposed are variants of the U.S. department of Defense's multilevel security policy consequently, it is difficult to discuss mandatory controls apart from multilevel security. A few general concepts, however, apply to all mandatory policies [4].

Mandatory controls are used in conjunction with discretionary controls and serve as additional (and stronger) restriction on access. A subject may have access to an object only if the subject passes both discretionary and mandatory checks. Since users can not directly manipulate mandatory access control attributes, users employ discretionary controls for their own protection from other users. Mandatory controls come into play automatically as stronger level of protection that cannot be by passed by users through accidental or intentional misuse of discretionary controls.

(MAC) is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information.

A multilevel system is a single computer system that handles multiple classification levels between subjects and objects.

- Sensitivity labels: In a MAC-based system, all subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.
- Data import and export: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of MAC-based systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times [5].

Two methods are commonly used for applying mandatory access control:

A. Rule-based access controls: This type of control further defines specific conditions for access to a requested object. All MAC-based systems implement a simple form of rule-based access control to determine whether access should be granted or denied by matching:

- An object's sensitivity label
- A subject's sensitivity label

B. Lattice-based access controls: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object [1].

4.2 Discretionary access control

Discretionary access control (DAC) is an access policy determined by the owner of a file (or other resource). The owner decides who is allowed access to the file and what privileges they have.

Two important concepts in DAC are:

- File and data ownership: every object in a system must have an owner. The access policy is determined by the owner of the resource (including files, directories, data, system resources and devices). Theoretically, can an object without an owner is left unprotected. Normally, the owner of a resource is the person who created the resource (such as a file or directory).
- Access rights and permissions: These are the controls that owner can assign to individual users or groups for specific resources [7].

Discretionary access controls can be applied through the following techniques:

- An access control lists(ACLs) name the specific rights and permission that are assigned to subject for a given object. Access control lists provide a flexible method for applying discretionary access controls.
- Role-based access control assigns group membership based on organizational or functional roles. This strategy greatly simplifies the management of access rights and permissions:

Access rights and permission for object are assigned any group or, in addition, to individuals. Individuals may belong to one or many groups. Individuals can be designated to acquire

Cumulative permissions (every permission of any group they are in) or disqualified from any permission that isn’t part of every group they are in [1].

References

1. Lipner, S. B. Non-discretionary controls for Commercial Application. In proceeding of the 1982 symosium on security and privacy, 2001
2. U.S. federal standard 1037C, 2001
3. Saltzer, J. H.; and Schroeder; M. D. The protection of Information in computer system, 2004
4. Blotcky, S. Lynch, Kaland Lipner; S. "SE/VMS: Implementation mandatory security in VAX/VMS. In proceedings of the 9th National computer security conference, 2000.
5. Darcy, K., How to Deploy an Advanced Building Access System, 2007.
6. U. S. National Information System Security Glossary, 2006
7. Campbell, J. P. Door – Access – Control System Based on finger – vein Authentication, 2006