Chapter XXXVII
Access Control Models

Romuald Thion
University of Lyon, France

ABSTRACT

Access control, or authorization, is arguably the most fundamental and most pervasive security mechanism in use today in computer systems. In computer systems, to grant authorization is to determine whether a subject can access resources. Informally speaking it is to decide "who can do what." Access control is critical to enforce confidentiality (only authorized users can read information) and integrity (only authorized users can alter information) in computer systems, preventing hackers and cyber-terrorists from reading and modifying sensitive files. Several access control models have been proposed since 1960 up today: from simple access matrix to task based access control through military models. Each one providing a different way to organize and express users' privileges. For example, the role based access control model aggregate privileges thanks to the concept of role: all users receive permissions only through the roles to which they are assigned. We first introduce the purpose of access control, then we describe models in use today, their specificities and the mechanisms which they rely on. The end of the this chapter is dedicated to current issues on access control.

INTRODUCTION

Information knowledge has been acknowledged for a long time in warfare. For example, Tzu's section III. Attack by Stratagem (1910) describes the importance of knowledge:

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. (Verse 18)

This quotation points out that information knowledge is among the most important factors in winning a war, this quotation is a 2,500 year old introduction to information warfare. Information warfare means a

strategy for acquiring an enemy's information, while defending one's own. It is a kind of warfare where information and attacks on information and its system are used as a tool of warfare.

Common mechanisms enhancing security and protecting one's own information are cryptography, *authentification,* or *authorization*. This topic focuses on a particular aspect of security mechanisms: authorization, also known as access control. This concept, in its broadest sense, came about prior to computer science; chests, locks, fences, and guards have always been used to protect valuable information from foes.

Access control has been used since the very beginning of distributed systems in which multiple users can share common resources. With the increased dependence of defense on computer systems, the U.S. Department of Defense (DoD) investigated the vulnerability of government systems in the late 1960s, leading to the first definitions of access control principles. Researchers also considered the problem. For example, Lampson's (1974) access control matrix is the first formal mathematical description of what access control is. The DoD investigation led to a definition of multilevel access control, relating to classified documents, such as unclassified, confidential, secret, and top-secret, identifying clearly the separation between authorization and authentification. From then on, access control has been abundantly studied, extended, and commercialized to fill the security gap of computer systems, and is a major tool for preventing cyber terrorists from accessing sensitive data.

THE PURPOSE OF ACCESS CONTROL

In computer systems, access control denotes whether a *subject* (e.g., process, computer, human user, etc.) is able to perform an *operation* (e.g., read, write, execute, delete, search, etc.) on an *object* (e.g., a tuple in a database, a table, a file, a service, and, more generally, any resource of the system) according to a *policy*. These concepts are commonly encountered in most access control and computer security literature. The right to carry out an operation on an object is called permission. *Access control policies* define the subjects' permissions in a computer system, in order to enforce the security of an organization. One of the fundamental best practices in security is developing, deploying, reviewing, and enforcing security policies.. These policies are organized according to an access control model. The model may add intermediate concepts between subjects and permission to organize policies. Intermediate concepts are chosen among tasks, groups, roles, or confidentiality labels, for example. They aim at making policies, management, and definition easier, fitting in as best as possible with the internal structure and needs of the protected system (Ferraiolo, Kuhn, & Chandramouli, 2003).

Informally speaking access control means to decide "who can do what." Access control is arguably the most fundamental and most pervasive security mechanism in use in computer systems.

Information security risks are commonly categorized into:

- **Confidentiality:** Information must be kept private; only authorized users can read the information.
- **Integrity:** Information must be protected from being altered; only authorized users can write the information.
- **Availability:** Information must be available for use.

The purpose of access control is to preserve the confidentiality and integrity of information and, to a lesser extent, availability. Access control aims at providing only useful permissions to subjects, thus avoiding improper writing (mainly related to integrity) and reading (mainly related to confidentiality) operations. Access control is not as obviously related to availability, but it has an important role. A cyber terrorist who is granted unauthorized access is likely to bring the system down (Ferraiolo et al., 2003). Moreover, access control provides protection against