Chapter 57
Modelling of Location-Aware Access Control Rules

Michael Decker
Karlsruhe Institute of Technology (KIT), Germany

ABSTRACT

Access control in the domain of information system security refers to the process of deciding whether a particular request made by a user to perform a particular operation on a particular object under the control of the system should be allowed or denied. For example, the access control component of a file server might have to decide whether user "Alice" is allowed to perform the operation "delete" on the object "document.txt". For traditional access control this decision is based on the evaluation of the identity of the user and attributes of the object. The novel idea of location-aware access control is also to consider the user's current location which is determined by a location system like GPS. The main purpose of this article is to present several approaches for the modeling of location-aware access control rules. We consider generic as well as application-specific access control models that can be found in literature.

INTRODUCTION

With the advent of multi-user computer systems it was necessary to implement some kind of Access Control (AC) because not every user of such a system should have the rights to access all the data created by other users. Today virtually every serious software product developed for multi-user scenarios is equipped with some kind of AC. For example, contemporary operating systems like UNIX or Microsoft Windows support the definition of access rights for individual users or groups of users for individual files and directories.

Traditional access control is based on rules that evaluate the user's identity, group memberships he has and attributes assigned to the resources under the protection of the AC system. But the wide-spread availability of techniques to determine the approximate location of a mobile computer stimulated the idea to evaluate also (or even only) the user's location for access control decisions. Systems for the determination of the

DOI: 10.4018/978-1-60960-042-6.ch057

user's location are called "locating systems". The most prominent of these systems is the Global Positioning System (GPS) which was developed by the USA for military purposes, but nowadays it is also widely used for civil applications (Hoffmann-Wellenhof, Lichtenegger & Wasle, 2008). In the literature (e.g., Küpper, 2007; Roth, 2004; Hightower & Borriello, 2000) descriptions of many other location systems can be found, e.g., systems for indoor applications or which are extensions of wireless communication networks.

Access control which is combined with locating technology to improve the security of mobile applications this is termed "Location-Aware Access Control" (LAAC). Some authors use the term "location-based" access control for LAAC. However, we prefer the adjective "location-ware" because even a model for LAAC might include rules that are location-agnostic, for example, if only the access to documents classified as "Top Secret" should be subject to location-aware constraints.

LAAC represents a special form of Location-based Services (LBS). An LBS is an application that was designed to be used with a mobile computer that evaluates the location of at least one mobile user and adapts itself accordingly (Küpper, 2007). LAAC may prevent a user form performing a requested operation on a data object or service if he doesn't stay at a location where this is allowed and therefore also constitute an LBS.

The remainder of this chapter is organized as follows: we first familiarize with the basics of conventional (i.e., location-agnostic) access control. After a section which sketches several application scenarios for location-aware access control we will survey the most important LAACM to be found in the pertinent literature; these models are assigned to one of the following groups: DAC, MAC, RBAC and application-specific models. After a comparison of the different approaches we also consider the problem of location-spoofing and how to check inconsistencies in LAACM before we come to the obligatory conclusion.

BASICS OF CONVENTIONAL ACCESS CONTROL

Access Control (AC) is the process to determine if a given request made by a user should be allowed or denied (Samarati & di Vimercati, 2001). Such a user request is described by the triple *[subject, object, operation]*: the *subject* is the active entity (e.g., human user or computer program working on behalf of the user) that demands to perform the operation on the object (passive entity). The set of possible operations depends on the type of the object. For example, if the object is an electronic document then the set of possible operations might contain "read", "write", "delete" and "append", while for a service as protected object the only eligible operation is "execute". When LAAC is employed then the user's current location is added as fourth element to be considered for the access control decision.

An Access Control Model (ACM) is a data model especially designed to express the configuration and current state of an access control system. ACM act as layer between human users and the part of the information system that has to enforce what is defined in the ACM. Further, some ACM can be used to analyze if particular properties for a given configuration hold. Such a property could be "user Alice can never obtain the permission to read a particular file". An example for an ACM employed by many contemporary implementations is the so called "Access Control List" (ACL), where for each protected object a list is maintained, which enumerates the pairs of subjects and operations that are allowed on that object. ACM are usually classified into "Discretionary Access Control" (DAC), "Mandatory Access Control" (MAC) and "Role-based Access Control" (RBAC). In this chapter we follow this tradition and organize the discussion of generic LAACM based on this classification. When reading the pertinent publications from the area of both conventional and location-aware access control one may get the impression that DAC,