Chapter 7.10
Access Control in Mobile and Ubiquitous Environments

Laurent Gomez
SAP Research, France

Annett Laube
SAP Research, France

Alessandro Sorniotti
SAP Research, France

ABSTRACT

Access control is the process of granting permissions in accordance to an authorization policy. Mobile and ubiquitous environments challenge classical access control solutions like Role-Based Access Control. The use of context-information during policy definition and access control enforcement offers more adaptability and flexibility needed for these environments. When it comes to low-power devices, such as wireless sensor networks, access control enforcement is normally too heavy for such resource-constrained devices. Lightweight cryptography allows encrypting the data right from its production and the access is therefore intrinsically restricted. In addition, all access control mechanisms require an authenticated user. Traditionally, user authentication is performed by means of a combination of authentication factors, statically specified in the access control policy of the authorization service. Within ubiquitous and mobile environment, there is a clear need for a flexible user authentication using the available authentication factors. In this chapter, different new techniques to ensure access control are discussed and compared to the state-of-the-art.

INTRODUCTION

Ubiquitous computing is the computing paradigm that refers to scenarios in which computing is omnipresent, and particularly in which devices that are traditionally perceived as dumb are endowed with computing capability (Stajano, 2002). The use of context information represents a significant benefit for applications in the highly dynamic environments addressed by ubiquitous computing. The deployment of collaborative mobile applications in ubiquitous environments is accompanied by an increasing demand on security. In addition to technical challenges, ubiquitous environments raise security issues such as access control for resources shared between mobile applications. Access control represents a real challenge due to the highly dynamic nature of communications, where former unknown partners communicate in an ad-hoc way.

Access control is a standard security technique to control the access to resources in a system. It consists of a set of mechanisms and processes that allow the definition of access control rules - the authorization policy - and the enforcement of these rules (Samarati, 2001). Access control is the process of granting permissions in accordance with an authorization policy. An authorization policy states “who can do what to what”. The “who” is a subject, the first “what” is an action, and the other “what” is a resource. In a context-aware authorization policy the context is taken into account as additional constraint. The statement can be extended as follows: “who can do what to what under which circumstances”. The circumstances correspond to the context of the application.

The availability of context information allows reconfiguration and enhancement of a system and application security, depending on the changing context. Context-aware security is defined as a dynamic adaptation of security policies according to the context. For instance, context information can be used to automatically reconfigure security mechanisms in order to provide a predefined level of security and, at the same time, to optimize the use of resources. As a concrete example, email messages sent by mobile workers using a public WLAN hotspot as an access point for their PDA can be automatically encrypted, whereas the same messages could be sent in plain text when they connect to a secured access point in his office.

SCENARIOS

In the following section, the challenges of access control in ubiquitous and mobile environments are highlighted in 2 different scenarios.

Scenario 1: Remote Healthcare Monitoring

The use of context-aware security techniques is illustrated in the following e-health scenario: an application constantly monitors the health and well-being of elderly at home. The elderly are wearing body sensors, which register several measurements related to the physical condition, like heart rate, oximetry (SpO2), blood glucose level and body temperature. The homes of aged people are equipped with ambient sensors, delivering additional information about the activities of the monitored subject and of the environment. All measurements are forwarded to a backend application and stored permanently there as part of the personal medical records. Since these medical records contain sensitive data, access to the data has to be controlled.

In the e-health example, medical records can be accessed by people in different roles such as: general practitioners, gerontologists (specialist for diseases and problems specific to old people), and nurses. But often the role concept alone is not sufficient to control access to the medical data. Additional criteria, like the relationship between patient and doctor or context information, e.g. the health status or location, have to be considered. Normally, only family doctors can access the entire personal medical record of a patient. But in an emergency situation, any physician, who is close to the patient, can get access to the data. An emergency situation can be described as a complex type of context information derived from the body sensor readings. The proximity of two individuals also represents complex context information, calculated out of the position gained, for example, by GPS sensors.