Chapter 73
Privacy-Aware Organisation-Based Access Control Model (PrivOrBAC)

Nabil Ajam
Institut Télécom, Télécom Bretagne, France

Nora Cuppens-Boulahia
Institut Télécom, Télécom Bretagne, France

Fréderic Cuppens
Institut Télécom, Télécom Bretagne, France

ABSTRACT

In this chapter, the authors propose the expression and the modelling of the most important principles of privacy. They deduce the relevant privacy requirements that should be integrated in existing security policy models, such as RBAC models. They suggest the application of a unique model for both access control and privacy requirements. Thus, an access control model is to be enriched with new access constraints and parameters, namely the privacy contexts, which should implement the consent and the notification concepts. For this purpose, the authors introduce the Privacy-aware Organisation role Based Access Control (PrivOrBAC) model.

1. INTRODUCTION

The enforcement of a privacy policy is still an open issue. One challenge is the expression of a privacy policy in information systems using existing security policy models. It is not sure that proposing a new model for privacy will be commonly accepted because it will cause a huge upgrade of existing solutions. Since privacy requirements are generally mixed with an ordinary access control, we aim to enhance existing access control models to include privacy needs.

Related works, which proposed a privacy-aware model, have the drawback of including only a subset of the privacy requirements. Even if we share the same objectives as (Ni et al. 2007), (Masoumzadeh and Joshi 2008), (Yang et al. 2008), and (Byun et al. 2005) in using an access control model to ex-

DOI: 10.4018/978-1-4666-2919-6.ch073

press privacy requirements, they mainly focused on purpose specification, explicit consent and obligation. They do not care about data anonymisation, for example. On other hand, sometimes they need to extend their language to express some contexts such as the owner age and the current time as it is done in (Ni et al. 2007).We propose the embedding of the most important privacy requirements within a single model, the OrBAC model, namely owner consent, data obfuscation, provisional obligation, and other environment contexts such as temporal, spatial and prerequisite ones (Ajam et al. 2009). Minimal modifications are introduced into it since we aim an easy upgrade of existing information systems, which use the OrBAC model, towards a privacy-aware model.

In this chapter, we thus propose to use the OrBAC model enhanced by some concepts to model privacy policies. First, we focus on modelling the requirements of the data owner consent before delivering the sensitive data. The subscriber defines that he must be notified before terminating the access. The access is delayed until the satisfaction of this condition.

Then, the accuracy of the sensitive data is usually underestimated within privacy models. We design an object hierarchy based on predefined accuracy levels. For this, we propose a derivation rule of sensitive objects. So, a data owner can define authorizations based on different object accuracies. Furthermore, access control models usually permit the access to the stored data based on the role of the requester. We propose to extend this concept to take into account the purpose of the access. For this, we take advantage of the OrBAC user-declared context. We also propose in this work to model the provisional obligations after accessing personal information.

Third parties must notify the data controller about further usage of collected data. Then, we extend OrBAC contexts to model the communication state between the subject and the data owner. This state indicates if the owner initiated a call to the service provider, so this fact can be considered as an implicit consent and the sensitive information can be authorized to be accessed. Also, we extend the spatial context to constrain the access based on the area of the object and not only on subject location. To validate our approach, we show how the resulting model can be used to model the privacy policy for a location-based service. This can be applied within a mobile operator organization.

This chapter is organised as follows. Section 2 lists the privacy requirements that will be deployed through access control models. Section 3 presents the OrBAC model. Section 4 is dedicated to our privacy-aware OrBAC model. Section 5 presents a use case of location service and how a privacy policy is specified through our privacy-aware OrBAC model. Section 6 details related works and the advantage of our proposal. And concluding remarks are presented in section 7.

2. MODELLING MOTIVATION

We illustrate in this section the issues related to private data management and how to use a privacy policy to specify privacy requirements. We assume that the private data are collected by mobile operator networks since we focus, in our work, on sensitive data such as location and presence of mobile subscribers that only the network operator can collect. At this stage we do not care about means used to collect data. Collected data concerns operator's subscribers (see Figure 1).

The information is stored within operator's information system. The later should implement the OrBAC model to enforce the privacy policy defined by the subscribers. Service providers request that information to offer enhanced services. So, the operator should manage the access to services.

2.1 Privacy Requirements

We can identify the following goals of the privacy policy: