Chapter 3
Leveraging Access Control for Privacy Protection: A Survey

Anna Antonakopoulou
National Technical University of Athens, Greece

Georgios V. Lioudakis
National Technical University of Athens, Greece

Fotios Gogoulos
National Technical University of Athens, Greece

Dimitra I. Kaklamani
National Technical University of Athens, Greece

Iakovos S. Venieris
National Technical University of Athens, Greece

ABSTRACT

Modern business environments amass and exchange a great deal of sensitive information about their employees, customers, products, et cetera, acknowledging privacy to be not only a business but also an ethical and legal requirement. Any privacy violation certainly includes some access to personal information and, intuitively, access control constitutes a fundamental aspect of privacy protection. In that respect, many organizations use security policies to control access to sensitive resources and the employed security models must provide means to handle flexible and dynamic requirements. Consequently, the definition of an expressive privacy-aware access control model constitutes a crucial issue. Among the technologies proposed, there are various access control models incorporating features designed to enforce privacy protection policies, taking mainly into account the purpose of the access, privacy obligations, as well as other contextual constraints, aiming at the accomplishment of the privacy protection requirements. This chapter studies these models, along with the aforementioned features.

DOI: 10.4018/978-1-61350-501-4.ch003

INTRODUCTION

The recent technological advances in the data processing and communication capabilities of information technology spur an information revolution that brings significant improvements to the citizens' quality of life and new potentials for business organizations, including operational efficiency, increased quality of products and services, as well as capabilities for innovation. On the other hand, they pose serious risks on privacy, meaning the "*claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (Westin, 1967); the personal data collection scale is augmented, information access, processing, aggregation, combination and linking are facilitated, new types of data are collected and the service provision chain is becoming complex, involving multiple actors exchanging and sharing data. More than a century after the seminal essay identifying that privacy as a fundamental human right was endangered by technological advances (Warren & Brandeis, 1890), citizens have never before in history been so concerned about their personal privacy and the threats posed by emerging technologies (Gallup Organization, 2008).

On the other hand, the protection of privacy has evolved to a salient issue and a business requirement also for organizations that constitute personal data collectors and processors. As trust is spotlighted at the core of social order, the adoption and consumption of their products and services is determined by the perception of risk and benefit on behalf of the potential users. Hence, from the organizations' point of view, the recognition of the importance of privacy protection is motivated by the business losses due to privacy violations and mishaps that support users' mistrust: economy faces setbacks because of the risks to privacy (Acquisti, 2010). Moreover, the privacy domain is a legislated area (Solove, 2006); several countries, e.g., Canada and the members of the European Union, have adopted data protection laws, which generally reflect the fundamental principles, set forth by the Organization for Economic Co-operation and Development in its milestone guidelines (OECD, 1980). Therefore, regulatory compliance and the potential of sanctions constitute the primary reasons to motivate businesses for the adoption of fair business practices with respect to personal information management.

In order for business organizations to engender trust to their customers, as well as to achieve compliance with the privacy legislation, they adopt data management practices that are reflected by privacy policies. Recently, several frameworks have emerged for the formalization of privacy policies specification, while programs of "privacy seals" are frequently joined as confidence-building measures. Nevertheless, privacy policies and seals by themselves are not effective from an operational point of view; a critical challenge concerns the automation of their enforcement or, in other words, their realization by technical means and their integration with the underlying Information and Telecommunication Technology (ICT) systems.

One of the most important technologies enabling the enforcement of fair data practices is access control. In fact, what any privacy violation certainly includes is some access to personal data and, intuitively, access control constitutes a fundamental aspect of privacy protection. Traditional access control models, such as the Discretionary Access Control (DAC) (NCSC, 1987), the Mandatory Access Control (MAC) (Pfleeger, 1997) and the Role-Based Access Control (RBAC) (Ferraiolo et al., 2001; Sandhu et al., 1996) fail to meet the requirements stemming from the fundamental privacy principles (OECD, 1980) that demand the incorporation of different criteria in access control decisions, rather than just *which user*, having *which role*, is performing *which action* on which *data object*. In that respect, the development of access control models specifically tailored towards privacy protection has been the focus of intense research in the last few years.