Chapter 20
Deploying Privacy Improved RBAC in Web Information Systems

Ioannis Mavridis
University of Macedonia, Greece

ABSTRACT
Access control technology holds a central role in achieving trustworthy management of personally identifiable information in modern information systems. In this article, a privacy-sensitive model that extends Role-Based Access Control (RBAC) to provide privacy protection through fine-grained and just-in-time access control in Web information systems is proposed. Moreover, easy and effective mapping of corresponding components is recognized as an important factor for succeeding in matching security and privacy objectives. Such a process is proposed to be accomplished by capturing and modeling privacy requirements in the early stages of information system development. Therefore, a methodology for deploying the mechanisms of an access control system conforming to the proposed Privacy Improved Role-Based Access Control (PIRBAC) model is presented. To illustrate the application of the proposed methodology, an application example in the healthcare domain is described.

INTRODUCTION
The evolution of information and communication technology (ICT) has significantly increased security and privacy concerns. A common practice with potential impact on citizens’ privacy is that Web application data are likely collected, stored and processed without any consent of data subjects. However, in case such data are characterized as personal information a number of privacy issues are raised for data subjects, which usually are individuals or consumers.

Privacy awareness is increasing from the practice of modern organizations that utilize Web applications to collect, store and process private information of users, usually gathered from monitoring their behaviour, in order to provide more personalized and competitive services. Moreover, modern organizations, which are likely utilising ICTs to provide goods and services, aim to build
trust based on good privacy practices, and finally utilize privacy as a differentiating factor for their brand names and a way to attract more customers (Powers, 2002).

In the literature, capturing and modeling privacy requirements in the early stages of information system development is proposed as essential to provide privacy protection especially to consumer data (He & Anton, 2003). Privacy protection can be achieved by enforcing privacy policy rules within online and offline data processing systems of an organization. Nowadays, most organizations have a privacy policy posted on their websites. Due to separation of duties in an organization between security and privacy staff, privacy policies are usually defined as high-level natural language descriptions by the organization’s privacy officer. Similarly, a security policy is usually defined by the security officer as a set of rules and procedures that regulate how the organization manages and protects enterprise data. Practical security is primarily related to access control policies and mechanisms that govern authorizations of users to gain access to stored application data. However, high-level natural language privacy policy descriptions are difficult to be enforced directly via access control. Furthermore, privacy requirements are often not reflected in the design and implementation of access control policies. As a result, a gap exists between security and privacy protection that is exacerbated by conflict of interests between stakeholders, system developers and administrators, and consumers.

Privacy is defined as “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, 1968). Analyzing this definition, the following words or terms can be isolated and further analyzed: “when”, “how” and “to what extent”. “When” introduces a situation or process that takes place in a particular time period and aims to the accomplishment of a specific purpose. “How” focuses on the operations running during and after access to data, either requested by the data user or imposed by the system, as well as the conditions under which private information is accessed. The term “to what extent” refers to the amount of data accessed in order to form the private information that is finally communicated to others.

The important roles of purposes, conditions and obligations in developing efficient systems for privacy protection in modern information systems, are pointed out in the proposed by Powers (2002) elements of a privacy policy. Specifically, these elements are data users, operations, data types, purposes, conditions and obligations. Data users are the individuals that are requesting to access data. Operations are used to define access control rules specifying permitted actions on data objects. Data types are likely concerned as high-level definitions of data collections, such as patient insurance information. Purposes are the reasons for which data accesses are requested and actually represent the goals to be accomplished by performing particular organizational tasks, as for example sending a special offer by email. These goals are likely expressed by high-level processes or applications, e.g. marketing. Conditions are prerequisites to be met in order for an operation to be performed. Obligations are additional operations to be performed after a particular access is permitted.

It is widely acceptable that neither the classic access control approaches of Mandatory Access Control (MAC) and Discretionary Access Control (DAC) nor the nowadays commonly applied Role-based Access Control (RBAC) were intended to support privacy protection. According to Wang et al. (2007), the main difficulty arises from the fact that traditional access control models are focusing on which subject, either identified by its identity or classified by its attributes (rank, roles, etc), is allowed to perform which operation on which data object. However, privacy protection requires taking care of which type of data is accessed