Privacy-Aware Access Control System: Evaluation and Decision

Claudio Agostino Ardagna, Sabrina De Capitani di Vimercati, Eros Pedrini, and Pierangela Samarati

Università degli Studi di Milano

14.1 Introduction

The success of the Web as a platform for the distribution of services and dissemination of information makes the protection of users’ privacy a fundamental requirement. The privacy issues affect different aspects of today’s Internet transactions, among which access control represents the most critical. An important step towards the protection of privacy is then the definition of a privacy-aware access control system that, in addition to server-side resources protection, provides users with solutions for preserving their privacy and managing their data. Although considerable work has been done in the field of access control for distributed services [AHK+03, AHKS02, BS02a, eXt05, Wor02], available access control mechanisms are at an early stage from a privacy protection point of view. This situation reflects the fact that in the last years the variety of security requirements focused on addressing server-side security concerns (e.g., communication confidentiality, unauthorized access to services, data integrity). Here, we focus on the development of a privacy-aware access control system regulating access to resources and protecting privacy of the users.

Generally speaking, an environment well-suited for users that need a private and secure way for using e-services should support at least the following basic requirements.
• **Privacy.** A digital identity solution should be respectful of the users’ rights to privacy and should not disclose and manage personal information without explicit consent.

• **User-driven constraints.** In addition to traditional server-side access control rules, users should be able to specify constraints and restrictions about the usage that will be made of their information once released to external parties.

• **Minimal disclosure.** Service providers must require the least set of credentials needed for service provision, and users should be able to provide credentials selectively, according to the type of online services they wish to access.

• **Interactive enforcement.** A new way of enforcing the access control process should be defined based on a negotiation protocol aimed at establishing the least set of information that the requester has to disclose to access the desired service.

• **Anonymity support.** As a special but notable case of minimal disclosure, many services do not need to know the real identity of a user. Pseudonyms, multiple digital identities, and even anonymous accesses must be adopted when possible.

• **Legislation support.** Privacy-related legislation is becoming a powerful driver towards the adoption of digital identities. The exchange of identity data should not violate government legislations such as the Health Insurance Portability and Accountability Act (HIPAA) or Gramm-Leach-Bliley Act (GLB).

In the following, we present the prototype of a privacy-aware access control system, which supports the above requirements and integrates traditional access control mechanisms with release and data handling policies. In particular, we focus our discussion on policy evaluation and composition. Our privacy-aware access control system deals with five main key aspects: i) **resource representation**, ability to specify access control requirements about resources in terms of available *metadata* describing them; ii) **subject identity**, the evaluation of conditions on the subject requesting access to a resource often means accessing personal information. This raises a number of privacy issues, since electronic transactions (e.g., purchases) require release of a far greater quantity of information than their physical counterparts; iii) **secondary use**, although users provide personal information for use in one specific context, they often have no idea on how such personal information may be used subsequently. Users should be able to define restrictions on how their information will be used and processed by external parties; iv) **context representation**, context information is a set of metadata identifying and possibly describing entities of interest, such as subjects and objects, as well as any ambient parameter (including location) concerning the technological and cultural environment where a transaction takes place. As far as policy enforcement is concerned, context contains information enabling verification of policy conditions and,