Chapter X

Privacy-Enhanced Identity Management for E-Services

Claudio Agostino Ardagna, Università degli Studi di Milano, Italy
Marco Cremonini, Università degli Studi di Milano, Italy
Ernesto Damiani, Università degli Studi di Milano, Italy
Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy
Fulvio Frati, Università degli Studi di Milano, Italy
Pierangela Samarati, Università degli Studi di Milano, Italy

ABSTRACT

This chapter introduces the concept of privacy-enhanced identity management for e-services supporting the user’s needs to protect their privacy and sensitive information. Business activities are increasingly based on the use of remote resources and e-services as well as on the interaction between different, remotely-located, parties. In this context, the electronic execution of private and/or sensitive transactions must fully preserve information privacy by managing in a trustworthy and responsible way all identity and profile information that is released to remote parties. In this chapter, we investigate the main problems concerning identity management for e-services and outline the features that the next-generation of identity management systems should provide for. State-of-the-art technology in the field of privacy-enhanced identity management systems is also compared with traditional public key

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
infrastructure (PKI) solutions. The analysis of the benefits of these modern identity management systems is presented and discussed with references also to the results of some experiences in the area of e-government, whose objective is the development of public administration privacy-aware e-services.

INTRODUCTION

The widespread diffusion of online services provided by public and private organizations, mostly driven by e-commerce and more recently by e-government applications, has stressed the need of more secure ways to authenticate and authorize users who need to access online resources (Feldman, 2000).

In particular, we can define authentication as any process by which we can verify that the users are who they claim they are. The most common way to enforce authentication is based on the use of a pair username-password. However, many other techniques can be used such as digital certificates, smart cards, retina scans, voice recognition, or fingerprints. Access control is, instead, concerned with evaluating every request submitted by users who have entered the system, to access data and resources to determine whether the request should be allowed or denied based on a specified policy (Ardagna & De Capitani di Vimercati, 2004; Ashley, Hada, Karjoth, and Schunter, 2002; Ashley, Hada, Powers, and Schunter, 2003; De Capitani di Vimercati & Samarati, 2001). Basically, a policy defines the rights granted to users to exercise actions (e.g., read, write, create, delete, and execute) on certain objects.

In this chapter, we focus first on authentication technologies and architectures that address the growing needs of security requirements in the scenario of business-to-consumers applications. Kerberos (Kohl & Neuman, 1993) proposed at the beginning of the 90s, is an example of a successful technology for authenticating requests for network resources. The great expansion of Web-based systems led to application environments that crossed the boundaries of real organizations. Cross-domain digital identities are then required as well as new procedures for user authentication must be adopted, when online services, resource stakeholders, and users are geographically and organizationally distributed. In this context, new solutions need to be proposed to address interoperability and scalability challenges, among which single sign-on (SSO) (De Clercq, 2002) and credential-based authentication play an important role. The public key infrastructure (PKI) (Arsenault & Turner, 2002) is a well-known method for providing credential-based authentication and digital signatures solutions to electronic business and government applications by means of certification authorities hierarchies and the support of cross-certificates. When e-government systems were being designed, PKIs seemed to be the best answer to satisfy their requirements, such as the possibility for national or regional governments to establish root CAs aimed at improving the interoperability among