Open Source in Web-Based Applications: A Case Study on Single Sign-On

Claudio Agostino Ardagna, Università degli Studi di Milano, Italy
Fulvio Frati, Università degli Studi di Milano, Italy
Gabriele Gianini, Università degli Studi di Milano, Italy

ABSTRACT

Business and recreational activities on the global communication infrastructure are increasingly based on the use of remote resources and services, and on the interaction between different, remotely located parties. In such a context, Single Sign-On technologies simplify the log-on process allowing automatic access to secondary domains through a unique log-on operation to the primary domain. In this article, we evaluate different Single Sign-On implementations focusing on the central role of Open Source in the development of Web-based systems. We outline requirements for Single Sign-On systems and evaluate four existing Open Source implementations in terms of degree of fulfilment of those requirements. Finally we compare those Open Source systems with respect to some specific Open Source community patterns.

Keywords: access control; access methods; authentication; authorisation; distributed systems; Internet-based technology; Web-based applications

INTRODUCTION

The global information infrastructure connects remote parties, such as users and resources, through the use of large scale networks. Many companies focus on developing e-services, business, and recreational activities, such as e-government services, remote banking, and airline reservation systems (Feldman, 2000; Damiani, Grosky, & Khosla, 2003). In such a context, where the huge number of resources and services accessible on the Web leads to multiple log-on processes and identity profiles, a solution is needed to give to the users at least the illusion of having a single identity and a single set of credentials.

Furthermore, several regulations affecting e-services, such as the Sarbanes Oxley (SOX) directive and the Health Insurance Portability and Accountability Act (HIPAA), mandate provisions for maintaining the integrity of user profile data as an essential component of an effective security policy. HIPAA, for example, explicitly states that the companies are required to assign a unique profile for tracking
user identities to each user. Also, it mandates procedures for creating, changing, and safeguarding profiles. Traditional authentication policies do not even come close to fulfilling these requirements. Single Sign-On (SSO) (De Clercq, 2002) systems are aimed at simplifying log-on process, managing the multiple identities of each user, and presenting their credentials to network applications for authentication.

In the following, we put forward the idea of enriching existing e-services with a fully functional Open Source Single Sign-On (Buell & Sandhu, 2003) solution, allowing users to manage a single identity to access systems and resources. The motivation for focusing on Open Source software is that it is increasingly adopted as an alternative to proprietary solutions.

Many Web-based projects, in fact, are affected by budget, transparency, vendor lock-in, integration, and interoperability limitations that represent major crucial problems. The adoption of an Open Source approach can overcome these limitations. First, Open Source Software, although not necessarily free, is in most cases cheaper than proprietary software. Second, Open Source Software often adheres to open standards and it is conducted in public forums. Then, Open Source paradigm also guarantees supplier independence and avoids the lock-in problem: a lock-in situation, in fact, arises when software is proprietary; with Open Source Software data are not stored in a proprietary format, and it is possible for users to change between several different systems and suppliers. Finally, customization and re-use are simply addressable because source code is freely available and modifiable. Based on the above proprietary solution limitations, we can suggest that an important nonfunctional requirement for Web-based system could be implementing the entire application following the Open Source approach.

However, experience has shown that in some deployed systems based on Open Source operating system platforms a substantial amount of the application code, mostly used for access control and authentication related features, may belong to a proprietary application server (Ardagna, Damiani, Frati, & Montel, 2005). SSO systems need to be carefully operated to avoid becoming a single failure point for the whole infrastructure.

In this article, we describe a general model for Single Sign-On architectures focusing on the central role of Open Source implementations. We delineate a set of requirements that Single Sign-On solutions should satisfy and then evaluate four different fully functional Open Source

Figure 1. User log-on to multiservice domain