Chapter 21

Improving the Information Security of Collaborative Web Portals via Fine-Grained Role-Based Access Control

S. Demurjian
University of Connecticut, USA

H. Ren
University of Connecticut, USA

S. Berhe
University of Connecticut, USA

M. Devineni
Serebrum Cooperation, USA

Sushil Vegad
Serebrum Cooperation, USA

K. Polineni
Serebrum Cooperation, USA

ABSTRACT

Collaborative portals are emerging as a viable technology to allow groups of individuals to easily author, create, update, and share content via easy-to-use Web-based interfaces, for example, MediaWiki, Microsoft’s Sharepoint, and so forth. From a security perspective, these products are often limited and coarse grained in their authorization and authentication. For example, in a Wiki, the security model is often at two ends of the spectrum: anonymous users with no authorization and limited access via read-only browsing vs. registered users with full-range of access and limited oversight in content creation and modification. However, in practice, such full and unfettered access may not be appropriate for all users and for all applications, particularly as the collaborative technology moves into commercial usage (where copyright and intellectual property are vital) or sensitive domains such as healthcare (which have stringent HIPAA requirements). In this chapter, we report on our research and development effort of a role-based access control for collaborative Web portals that encompasses and realizes security at the application level, the document level (authoring and viewing), and the look-and-feel of the portal itself.
INTRODUCTION

Over the past decade, the World Wide Web (WWW) has come to the forefront as a viable means to allow individuals and organizations to collaborate. Consequently, web portals have emerged as a means to facilitate these interactions, ranging from information repositories to full-fledged authoring and document content collaboration. For instance, WebMD (www.webmd.com) and Wikipedia (www.wikipedia.org) are utilized by unregistered users to browse content via easy-to-use web-based interfaces. For registered users, these web portals provide a means to author, create, modify, and track documents of all types within a consistent framework or infrastructure. A registered user of Wikipedia has the ability to create new document content and modify existing content. Open source products such as Mediawiki (http://www.mediawiki.org) or a commercial solution such as Microsoft’s Sharepoint (http://www.microsoft.com/sharepoint/default.mspx) allows any individual with sufficient expertise to generate their own web portal to meet specific purposes and needs.

However, from a security perspective, these products are often very limited in the level of protection that is offered to information content that is created and uploaded using these various portals. For example, a registered Wikipedia user could create and upload intentionally erroneous content (e.g., a document that says that the world is flat). Some of these web sites depend on the community of users themselves to monitor document content; as the volume of content at these sites grows, it becomes problematic to attempt to maintain information in this fashion. Due to the lack of security and control, many corporate and governmental users are hesitant to utilize such technologies for content creation and collaboration, restricting their usage to an information repository; these same users have serious confidentiality, copyright, and intellectual property concerns as well. For example, an emerging usage of collaborative portals is in patient and physician collaboration on day-to-day health care (https://www.relayhealth.com/rh/default.aspx) where confidentiality is governed in the United States by the Health Insurance Portability and Accountability Act (HIPAA, http://www.hhs.gov/ocr/hipaa/). Utilizing existing collaborative portals in health care are likely to violate HIPPA, given the coarse level of access and limited accountability to content creation and modification; the security of patient/physician interactions simply could not be assured.

For commercial viability, collaborative portals must have more rigorous security capabilities than the coarse-grained authorization and authentication (user names and passwords) that are typically offered by Wikis/web portals. As a web application, a collaborative portal must prevent inherent vulnerabilities. As characterized by the Open Web Application Security Project (OWASP), the top ten web application vulnerabilities have been identified to assist developers, designers, and organizations in protecting their web applications from intrusion and malicious access (http://www.owasp.org/index.php/Top_10_2007). These vulnerabilities include: SQL injection flaws where SQL code typed into say a name or address data field alters a command to the database possibly resulting in the release of information; insecure communications as reflected by the lack of usage of https (secure http) for all interactions that have sensitive data; inadequate cryptography algorithms and credentials that do not adequately protect data stored in a database; and so on. In addition to this targeted discussion, there is a comprehensive primer of WWW security issues that classifies security concerns according to: client side via a web browser, server side in the web and application servers themselves, CGI scripts and their potential security holes, protection of confidential documents from access and misuse, and denial of service attacks (http://www.w3.org/Security/Faq/). Collaborative portals, by their nature, are intended to promote a high degree of interaction, and provide administrative users with a high degree of access (via privileges); as a result, all of