Chapter 7

Web 2.0 Technologies for Business Solutions: A Security Perspective

Shah Jahan Miah
Griffith University, Australia

ABSTRACT

Web 2.0 is a new way of using existing Web resources interactively, and has attracted growing interest from the Web community, and more recently from businesses. However, there are emerging issues associated with security with the use of Web 2.0. This chapter provides an overview of Web 2.0 and outlines the security issues with Mashups and other applications within the Web 2.0 environment.

INTRODUCTION

Web 2.0 is a new way of using existing Web resources interactively. This is achieved by using a programming technique called AJAX, which stands for Asynchronous JavaScript and XML. This technique helps make Web pages more interactive and enables collaboration from participants. It may also provide ways for hackers to hit a Web server and to exploit sites in attacks on visitors.

Recently, Web 2.0 technologies have been used for many business solutions, in terms of user enabled Web-services, and it has attracted growing interest from the Web community. For example, Digital library services (Curran, Murray, & Chris-
tian, 2007; Pearce, 2006) can be viewed as a platform where Web 2.0 technologies have been used to enhance user participation. In addition, the growing number of social networking features in websites, such as myspace, facebook and blogger, has potentially become a useful tool for business in terms of market research and increased exposure of products on the market. In the past, business applications driven by users were not able to be developed easily using traditional requirement and build approaches, especially for Web based service development.

Business processes are rapidly changing, due to the potential for improved virtual operations, and Web developers have started using Web 2.0 technologies for Web based user interface design, service composition design, as well as social or community based features design, to create more interactive business applications. As conventional technologies for Web services suffer from weaknesses, such as dynamicity, scalability, and flexibility, the view of emerging technologies offers an innovation to businesses and online communities. However, the security concerns of such technologies are an emergent problem for business users. This chapter describes key aspects of the security issues of the Web 2.0 technologies.

Web 2.0 technologies, especially Mashups, help develop Web-based applications by gathering content from several online sources. The basic principle of the technologies is to reuse existing content or services developed by other parties. The end result of such services can provide enhanced support for business and end-users, and the use of Mashup technologies can provide Web browsers with an important role at the user side. For example, Hakkola (2008) describes Web browsers as not just a tool for accessing static HTML based content, but when combined with Web 2.0 and Mashups, a useful tool for accessing content more dynamically and frequently. The classic browsers still have rigid security options when interacting with Mashups based applications, due to its dynamic nature. Wang, Fan, Howell and Jackson (2007) suggest that the Mashups applications have either no trust between the third parties, or there is full trust between them. According to Ashley (2007), this leads to a dilemma of having to consider both security and functionality for end-user browsers. This is because the browsers at the end user level have default security features that do not address the dynamic nature of Mashups, when interacting with third parties’ applications. Wang, Fan, Howell and Jackson suggest that the Mashups applications do not define trust levels between the third parties. This suggests a new security strategy is required for Mashup users.

The structure of this chapter is as follows. The first section of the chapter discusses the background of Web 2.0 technologies, with respect to business solutions. Secondly, we discuss applications developed using Web 2.0 technologies. The third section discusses the security concerns of the technologies in the context of online businesses. The final section summarizes the entire chapter by demonstrating the key boundaries of the discussion.
Enforcing Privacy on the Semantic Web
[www.igi-global.com/chapter/enforcing-privacy-semantic-web/23372?camid=4v1a](www.igi-global.com/chapter/enforcing-privacy-semantic-web/23372?camid=4v1a)

Identifying and Analyzing the Latent Cyber Threats in Developing Economies
[www.igi-global.com/chapter/identifying-and-analyzing-the-latent-cyber-threats-in-developing-economies/173128?camid=4v1a](www.igi-global.com/chapter/identifying-and-analyzing-the-latent-cyber-threats-in-developing-economies/173128?camid=4v1a)