Chapter 11
Threat Modeling:
Securing Web 2.0 Based Rich Service Consumers

Nishtha Srivastava
Infosys Technologies Ltd, India

Sumeet Gupta
Infosys Technologies Ltd, India

Mayank Mathur
Infosys Technologies Ltd, India

ABSTRACT
This research work proposes a threat modeling approach for Web 2.0 applications. The authors’ approach is based on applying informal method of threat modeling for Web 2.0 applications. Traditional enterprises are skeptical in adopting Web 2.0 applications for internal and commercial use in public-facing situations, with customers and partners. One of the prime concerns for this is lack of security over public networks. Threat modeling is a technique for complete analysis and review of security aspects of application. The authors will show why existing threat modeling approaches cannot be applied to Web 2.0 applications, and how their new approach is a simple way of applying threat modeling to Web 2.0 applications.

INTRODUCTION
One of the major trends in the IT industry today is the adoption of Service Oriented Architecture (SOA) in building applications leading to a flexible and standardized architecture for better collaboration and sharing of data among various applications. The evolution of Web 2.0 technologies such as blogs, wikis, podcasts, RSS, etc. has emerged as a key facilitator for creating rich service consumer ecosystems to augment the benefits of SOA including interoperability, reuse and standardization. This has expanded the reach of SOA with rich interactive controls and adoption of Web 2.0 tools and services to access content for any user at any time through any channel.
**What is Web 2.0?**

Web 2.0 is a term coined by Tim O’Reilly describing changing trends for using World Wide Web (www) as a platform to facilitate information collaboration. These concepts have led to the development and evolution of web-based communities such as social-networking and video sharing sites, content generation tools and services such as wikis, blogs, podcasts, content tagging and aggregation. Other key concepts that have emerged include web syndication like RSS and Mashup applications, which combine content from more than one source for an integrated experience. Although the term Web 2.0 suggests a new version of the web, it does not refer any update to technical specifications, but to changes in the way software developers and end-users utilize the web.

Web 2.0 is basically a new way to use existing Internet technologies— such as XML and JavaScript—to enable participation, interaction, and collaboration among users, content providers, and businesses, rather than just the traditional viewing of static web pages, said Hewlett-Packard security evangelist Michael Sutton. (Lawton, n.d.)

**Evolution of Web 2.0 Based Technologies and Systems**

Application development has evolved over the years from purely desktop application to purely web application to what is now an application nurturing the best of the both i.e. RIAs. The result of this has blurred the line between purely desktop and exclusively web applications. Historically, the web had been a largely unidirectional, designed as a medium for print content. Web was adopted as means of content sharing and small-scale data exchange via e-mail, corporate sites, and so forth. But it was not architected as a responsive writable means to leverage as a platform and a common working place. Although client-server computing idea of separating user interfaces (UI) from business logic and data persistence was good, the UIs tight coupling restricted choice of server-side technology. To overcome these shortcomings there was a requirement to effectively utilize web as a Content Management Workplace. It was required to capture, deliver, customize, and manage web content across an enterprise/division and so evolved Web 2.0 technologies.

This evolution led to the development of functionally rich and responsive applications using web as a platform rather than the typically static pages of traditional web technologies. These applications run on some complex set of technologies such as Asynchronous JavaScript and XML (AJAX), Flash, JavaScript Object Notation (JSON), Simple Object Access Protocol (SOAP), Representational State Transfer (REST). These technologies along with cross-domain information access contributed in empowering the client. This allowed end-users to add, generate and share content onto web in real time. This facilitated co-creation of ideas by information sharing and collaborative development which led to the development and evolution of web-based communities and hosted services, such as social-networking sites, video sharing sites, wikis and blogs.

**Web 2.0 and Business and Need for Security**

Web 2.0 has led to creation of new business processes, communities and business models which have added substantial benefits for traditional business. While most of Web 2.0 technologies are evolutionary, it’s the convergence of these technologies - along with fundamental shifts in the nature of business – which facilitated to its growth. Web 2.0 tools are better suited for content collaboration, sharing, publishing, and management of enterprise data. Wikis have already been useful in group content generation and as a lightweight project management tool.

However enterprises are skeptical in adopting Web 2.0 applications for internal and commercial
Related Content

Teaching Systemic Risk: An In-Class Simulation for Diverse Audiences
[www.igi-global.com/article/teaching-systemic-risk/145365?camid=4v1a](www.igi-global.com/article/teaching-systemic-risk/145365?camid=4v1a)

Algorithms for Detection and Classification of Abnormality in Mammograms: An Overview
[www.igi-global.com/chapter/algorithms-for-detection-and-classification-of-abnormality-in-mammograms/203391?camid=4v1a](www.igi-global.com/chapter/algorithms-for-detection-and-classification-of-abnormality-in-mammograms/203391?camid=4v1a)

Socio-Economic and Psychological Risks of Unemployed Youth in Developing Countries: Evidence From Hawassa City, Ethiopia

Offline/Online Security in Mobile Ad Hoc Networks
[www.igi-global.com/chapter/offline-online-security-mobile-hoc/76517?camid=4v1a](www.igi-global.com/chapter/offline-online-security-mobile-hoc/76517?camid=4v1a)