Chapter 13

Architecture for Improving Security in Web Environment

Varaprasad Rao M
Anurag Group of Institutions, India

Ambati Venkata Krishna Prasad
K.L. University, India

ABSTRACT

Web security threats have undergone much sophistication compared to their initial introduction and they are becoming more & more evolved every day. The evolution might be in terms of new ways of attack or bringing in resistance to using simulated OS or VM environments. Web service architecture is a set of standard protocols to communicate secure web services. Which include policy, security, trust, secure conversation, reliable messaging and automatic transactions. Security is one of the major issues which reduces the growth of computing and complications with data privacy and data protection continue to plague the market. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. The architecture of web poses such a threat to the security of the existing technologies when deployed in a web-based environment. In this chapter, the different security risks presented and specific to the different security issues that has emanated due to the nature of the service delivery models.

INTRODUCTION

Security is one of the major issues which reduces the growth of computing and complications with data privacy and data protection continue to plague the market. This chapter begins with a service and extends services to any application in Web environment. Now a days, every application is running on Web or Mobile is based on only service oriented. A comparative study on object orientation and service orientation is presented. Further, a new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. The architecture of web poses such a threat to the security of the existing technologies when deployed in a web-based environment. This chapter organized the concepts of the key security requirements; the difference between threats, attacks,
Architecture for Improving Security in Web Environment

vulnerabilities, and countermeasures; the key distinctions for web service architectures; the WSS Framework; the key principles and patterns for building secure services; the deployment of a new model and comparison with existing model.

BACKGROUND

Service

Patterns & Practices from Microsoft mentioned that a service is a public interface that provides access to a unit of functionality. Services literally provide some programmatic ‘service’ to the caller who consumes them. Services are loosely coupled and can be combined from within a client or from within other services to provide more complex functionality. Services are distributable and can be accessed from a remote machine as well as from the local machine on which they are running.

R. Chinnici, M. Gudgin, J-J. Moreau, J. Schlimmer, S. Weerawarana, (2003) and J. Cowan, R. Tobin, (2001) mentioned that services are message-oriented, meaning that service interfaces are defined by a Web Services Description Language (WSDL) file and operations are called using XML-based message schemas that are passed over a transport. Services support a heterogeneous environment by focusing interoperability at the message/interface definition. If components can understand the message and interface definition, they can use the service regardless of their base technology.

Common Services Scenarios

In MSDN; the services are flexible by nature and can be used in a wide variety of scenarios and combinations. The following are key scenarios that we will return to many times over the course of this guide:

- **Service Exposed Over the Internet**: This scenario describes a service that is consumed by Web applications or smart client applications over the Internet. Authentication and authorization decisions have to be made based upon Internet trust boundaries and credentials options. For example, username authentication is more likely in the Internet scenario than the intranet scenario. This scenario includes business-to-business as well as consumer-focused services. For example, a Web site that allows scheduling of your family’s doctor visits could be included in this scenario.

- **Service Exposed Over an Intranet**: This scenario describes a service that is consumed by Web applications or smart client applications over an intranet. Authentication and authorization decisions have to be made based upon intranet trust boundaries and credentials options. For example, an Active Directory user store is more likely in the intranet scenario than in the Internet scenario. An enterprise Web-mail application could be included in this scenario.

M. Gudgin, M. Hadley, N. Mendelsohn, J-J. Moreau, H. Nielsen (2003) stated that now a days, every application is running on Web or Mobile is based on only service oriented. A comparative study on object orientation and service orientation is presented as follows.