Chapter 4
Security Issues in Web Services

Priyanka Dixit
Rajiv Gahndi Prouodyogiki Vishwavidyalaya University, India

ABSTRACT

This chapter describes how security is an important aspect in today's digital world. Every day technology grows with new advancements in various areas, especially in the development of web-based applications. All most all of the web applications are on the internet, hence there is a large probability of attacks on those applications and threads. This makes security necessary while developing any web application. Lots of techniques have been developed for mitigating and defending against threats to the web based applications over the internet. This chapter overviews the important region of web application security, by sequencing the current strategies into a major picture to further the future research and advancement. Firstly, this chapter explains the major problem and obstacles that makes efforts unsuccessful for developing secure web applications. Next, this chapter distinguishes three basic security properties that a web application should possess: validation, integrity, accuracy and portray the comparing vulnerabilities that damage these properties alongside the assault vectors that contain these vulnerabilities.

INTRODUCTION

In the distributed environment the World Wide Web is the source that delivers static pages called as web application (Li & Xue, 2011). It is most prominent technology in the world for providing web services, information, and data access over the internet (Li & Xue, 2011). The technological improvements in data frameworks are necessary for the automation of various applications in different business and commercial areas. Information becomes turned into a basic asset in various associations, organizations along these, efficient access to information, distribution of information, and extract data from the information, and making exploitation of the data has turned to a dire necessity. Therefore, there has been needed security from the numerous attackers, which not just modification of data but misusing and destroying data from various sources scattered over the internet (Thuraisingham, 2003; Shrivastava, Sharma, & Bawankan, 2012).

Web applications and services are self-described or modular that can be published, access from anywhere on the internet. These applications can be written in any programming language and run on

DOI: 10.4018/978-1-5225-4100-4.ch004

any platform over the internet. A web service serves three of the basic responsibility in the web service framework these are Service requester, service broker, service provider. The service provider can be any business model, organization, the enterprise that is capable of providing services. The service requester can be any organizations that have the need for the service and service broker that acts as the intermediate between the service provider and requester (Kuyoro Shade et al., 2012).

The Web services are most attractive and important area for the research to the scientist and researchers. It is an important technology for the development and advancement of the distributed environment. Besides all of these merits of web services, there are some major challenges too that makes the deployment of web services over the internet is the critical one. The most challenging area for the web services is security and privacy. The secure service deployment is difficult today and the major issue for the distributed and heterogeneous applications. There are the following e-commerce models due to which the services provided to the customer business or vice versa like B2C and B2B but security is the important issue for providing secure web service.

All the web applications and services are run on the WWW so there is need of strong security architecture for protecting and make them securely running over the internet. This chapter presents the basic terminologies of security and privacy measures for Web Services also defines the security threads that makes difficult to provide secure web services over the internet.

FUNDAMENTAL PRINCIPLES OF SECURITY

Some of the fundamentals of security for the end to end services and application security in the distributed applications over the internet. Here describe the basic security principles that are necessary for the security architecture of web services and applications.

1. **Authentication:** This security term is basically verified the end users, registered system entities, and other components that are claiming. The authentication is the process by which authenticity of the user is checked on the internet it may any credentials, which may explain the following attributes like the identity of the person, role, group etc that can be integrated with the authentication principle.
2. **Authorization:** Is the term of security that granting any permission for accessing of resources, providing the access control, through which only authenticated users may access the resources, services via internet it acts like prevention against threats and unauthorized access. Access controls ensure that only the authorized users can access, control and modify the resource and no unauthorized access can be happened by this principle.
3. **Cryptography:** It provides security mechanisms and techniques that useful for protection of data from alteration and misuse. There are Encryption algorithms are used at the sender side which provides data confidentiality by encrypting the original data or message into some unreadable form that cannot be read by the third party and reverse algorithm at the receiver end, which contained decryption key that helps to decrypt the encrypted data. There are other algorithms like RSA, Diffie Hellman algorithms etc are used for secure key generation that responsible for the confidential information sharing and other terminology digital signature that ensures integrity and non-repudiation so that the data should be valid that send by the authentic person it is not been altered or modified during transmission over the medium.