Web Services Security: Techniques and Challenges

(Extended Abstract)

Anoop Singhal

Computer Security Division
National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899, USA
anoop.singhal@nist.gov

Abstract. Web services-based computing is currently an important driver for the software industry. While several standards bodies (such as W3C and OASIS) are laying the foundation for Web services security, several research problems must be solved to make secure Web services a reality. This talk will present techniques for Web services security and some of the challenges and recommendations for secure web services. This paper is based on our experience in developing the National Institute of Standards and Technology (NIST) Special Publication SP 800-95, "Guide to Secure Web Services". Some of the challenges for secure web services are

1. End to End Quality of Service and Protection
2. Availability of Service
3. Protection from Command Injection Attacks
4. Identity Management

To adequately support the needs of Web services-based applications, effective risk management and appropriate deployment of alternate countermeasures are essential. Defense-in-depth through security engineering, secure software development, and architecture risk analysis can provide the robustness and reliability required by these applications.

Reference

1. Singhal, A., Winograd, T., Scarfone, K.: NIST Special Publication 800-95, Guide to Secure Web Services (August 2007), http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

V. Atluri (Ed.): DAS 2008, LNCS 5094, pp. 158, 2008.