As I mentioned in a previous columns, there’s a new set of draft documents from the Computer Security Resource Center (CSRC) of the US National Institute of Standards and Technology (NIST) <http://csrc.nist.gov/publications/drafts.html>.

SP 800-95, “Guide to Secure Web Services” <http://csrc.nist.gov/publications/drafts/Draft-SP800-95.pdf> “provides detailed information on standards for Web services security. This document explains the security features of Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), the Universal Description, Discovery and Integration (UDDI) protocol, and related open standards in the area of Web services. It also provides specific recommendations to ensure the security of Web services-based applications.”

The 140-page document was written by Anoop Singhal and Theodore Winograd. It has the following structure:

1. Introduction
2. Background to Web Services and Their Relationship to Security
3. Web Service Security Functions and Related Technologies
4. Human User’s Entry Point into the SOA: Web Portals
5. Secure Web Service-Enabling of Legacy Applications
6. Secure Implementation Tools and Technologies

The authors point out that designers and managers of Web servers face particularly difficult security problems: “Many of the features that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections, and relative autonomy (lack of human intervention) are at odds with traditional security models and controls.” [Page ES-1] Problems include protecting confidentiality and data integrity and the constant threat to availability caused by the universal access inherent in the World Wide Web. They argue that simple “Perimeter-based network security technologies (e.g., firewalls, intrusion detection) are inadequate to protect SOAs [Service Oriented Architectures]” because “SOAs are dynamic, and can seldom be fully constrained to the physical boundaries of a single network.” In addition, “SOAP [Simple Object Access Protocol] … is transmitted over HTTP [Hyper Text Transfer Protocol], which is allowed to flow without restriction through most firewalls. Moreover, TLS [Transport Layer Security], which is used to authenticate and encrypt Web-based messages, is unsuitable for protecting SOAP messages because it is designed to operate between two endpoints. TLS cannot accommodate Web services' inherent ability to forward messages to multiple other Web services simultaneously.”

Highlights of the recommendations include

1. Replicate data and services to improve availability.
2. Use logging of transactions to improve accountability.
3. Use Secure software design and development techniques to prevent vulnerabilities.
4. Use performance analysis and simulation techniques for end to end quality of service and quality of protection.
5. Digitally sign UDDI [Universal Description, Discovery and Integration] entries to verify the author of registered entries.

Appendix A consists of four scenarios in 13 pages that illustrate the principles and recommendations presented in the body of the Guide:

1. Financial Institution Developing a Web Service
2. Healthcare Emergency Responders Orchestration of Web Services on Different Platforms
3. Web Services Enabling of Legacy Civil Agency System

Appendix B is a summary of common attacks against Web servers (15 pages). Appendix C is a one-page summary of the ebXML standard (Electronic Business using eXtensible Markup Language). Appendix D is a good glossary of useful terms for discussions of Web security (nine pages) and Appendix E lists three pages of appropriate acronyms. Finally, Appendices F and G provide a total of 10 pages of pointers to useful print and online resources for improving Web security.

If readers have comments for improvement of the documents, they can submit them to <mailto:800-95comments@nist.gov?Subject=Comments%20SP800-101> by October 30, 2006.”

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:meabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.