August 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURE WEB SERVICES

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Web services technologies help organizations use their computer systems and networks more efficiently and serve their customers more effectively. Web services provide a flexible way for organizations to connect applications and services so that they can communicate with each other and support each other over networks. This connectivity allows for better communication with customers, improved sharing of resources and data, and more efficient links of organizational processes across different systems and operating environments. In applying Web services, organizations can utilize different computer systems without changing their existing technologies and software design approaches, and without making major modifications to their legacy applications and databases.

Web services are implemented by means of a service-oriented architecture (SOA) that allows for interoperability, connectivity, and resource sharing. The SOA, which is based on open standards, is a collection of software services that can communicate with each other by passing data or by coordinating internal or external computer activities. This allows for the development of applications that use services and that are available as services for other applications to use. Examples of Web service applications are a financial institution's business-to-business service that allows transactions to be sent by third parties such as customers and business partners, and a healthcare provider's application that binds the healthcare provider networks with a hospital's Web services.

The many features that make Web services appealing also present security challenges to the implementation of the Web services approach. The improved accessibility of data, dynamic application-to-application connections, and reduced need for human intervention in providing Web services are capabilities that are not easily protected using traditional security models and controls.

Guide to Secure Web Services

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued NIST Special Publication (SP) 800-95, *Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology*, written by Anoop Singhal of NIST, Theodore Winograd of Booz Allen Hamilton, and Karen Scarfone of NIST. This publication helps organizations understand Web services and the challenges of integrating information security practices into SOA design and development to assure secure Web services.

The guide explains current and emerging standards that have been developed for Web services and provides background information on the most common security threats to SOAs. The information presented can be applied to many different hardware platforms, operating systems, and applications. Other topics discussed in the guide include Web portals, the human user's entry point into the SOA based on Web services; the challenges associated with making legacy applications secure; and secure implementation tools and technologies.

Important supplemental information is included in the appendices to the guide: a discussion of attacks that have been initiated against Web services and SOAs; an overview of Electronic Business eXtensible Markup Language (ebXML), a

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since September 2006:

- *Forensic Techniques: Helping Organizations Improve Their Responses to Information Security Incidents, September 2006*
- *Log Management: Using Computer and Network Records to Improve Information Security, October 2006*
- *Guide to Securing Computers Using Windows XP Home Edition, November 2006*
- *Maintaining Effective Information Technology (IT) Security Through Test, Training, and Exercise Programs, December 2006*
- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*
- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*
- *Border Gateway Protocol Security, July 2007*

Web services protocol suite developed by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT); a glossary of terms related to Web services; an acronym list; and a list of in-print resources and online tools and resources that will help the reader understand Web services and SOAs, security concepts and methodologies, and the general relationship between them.

The secure Web services guide is available from NIST's Web page: http://csrc.nist.gov/publications/nistpubs/index.html.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Security Issues

Standards are essential to the successful use of service-oriented computing. The SOA can be implemented using open standards and standard protocols such as SOAP, an eXtensible Markup Language (XML)-based protocol for exchanging structured information in a decentralized, distributed environment.

Voluntary standards organizations have been addressing the need for standards that form the foundation for Web services, and for standards and techniques that protect Web services. These organizations include the World Wide Web Consortium (W3C), the Organization for the Advancement of Structured Information Standards (OASIS), the Internet Engineering Task Force (IETF), and the Liberty Alliance.

Many of the standards and techniques that have been developed complement or extend one another, but there are many problems to be solved, such as service description, automatic service discovery, and quality of service (QoS) methods. The standards developed for Web service security do not provide all of the techniques that are needed to develop robust, secure, and reliable Web services.

Organizations should apply risk management procedures, use secure software development techniques, test their systems, and select effective security controls to provide robustness and reliability. Organizations should be concerned about providing protection for:

+ Confidentiality and integrity of data that is transmitted via Web services protocols in service-to-service transactions, including data that traverses intermediary services;

+ Functional integrity of the Web services requiring the establishment of trust between services on a transaction-by-transaction basis; and

+ Availability of systems when denial of service attacks exploit vulnerabilities unique to Web service technologies and target core services, such as the discovery service, on which other services rely.

Frequently used perimeter-based network security technologies, such as firewalls, do not provide adequate protection for SOAs, which are dynamic and can seldom be fully constrained to the physical boundaries of a single network. In addition, SOAP is transmitted over HyperText Transfer Protocol (HTTP), which is allowed without restriction through most firewalls.

Transport Layer Security (TLS), which is used to authenticate and encrypt Web-based messages, is inadequate for protecting SOAP messages because TLS is designed to operate between two endpoints. Also, TLS does not provide protection for messages which are forwarded to other Web services when these messages are not forwarded simultaneously by Web services applications.

In the Web service processing model, SOAP messages and XML documents must be secured as they are forwarded along potentially long and complex chains of consumer, provider, and intermediary services. However, Web services processing makes those services subject to unique attacks, as well as to variations on familiar attacks targeting Web servers.

Security Techniques for Web Services

Ensuring the security of Web services involves augmenting traditional security mechanisms with security frameworks based on use of authentication, authorization, confidentiality, and integrity mechanisms. NIST SP 800-95 describes how to implement those security mechanisms in Web services and how to make Web services and portal applications robust against expected attacks. Available specifications that address specific security issues include:

+ Confidentiality of Web service messages. XML Encryption, a specification that is available from the World Wide Web Consortium (W3C), provides a mechanism to encrypt XML documents.

+ Integrity of Web service messages. XML Signature, a specification produced jointly by the W3C and the Internet Engineering Task Force (IETF), allows for selectively signing XML data.

+ Web service authentication and authorization. XML Signature, Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), as proposed by the Organization for the Advancement of Structured Information Standards (OASIS) group, provide mechanisms for authentication and authorization in a Web services environment.

+ Message integrity and confidentiality. Web Services (WS)-Security, a specification produced by OASIS, defines a set of SOAP header extensions for end-to-end SOAP messaging security and allows communicating partners to exchange signed encrypted messages in a Web services environment.

+ Authentication. Security for Universal Description, Discovery and Integration (UDDI), developed by OASIS, enables Web services to be easily located and subsequently invoked. Security for UDDI

enables publishers, inquirers, and subscribers to authenticate themselves and authorize the information published in the directory.

See Appendix G of NIST SP 800-95 for references to these and other open standards that have been developed for secure Web services.

Challenges

While current standards deal with many security issues, there are still many issues to be addressed: repudiation of transactions; secure issuance of credentials; exploitation of covert channels; compromised services; spread of malware, such as viruses and Trojan horses, via SOAP messages; denial of service attacks; and incorrect service implementations. The following provides additional information on some of these challenges.

Discovery. In Web services discovery, participants identify and compose Web Services Description Language (WSDL)-specific services based on definitions in a UDDI registry. Discovery involves matching a set of functional and other criteria with a set of resource descriptions. The goal is to find appropriate Web service-related resources. Because of the potentially large number of service candidates in the registry, performance rankings for algorithms used to search, match, and compose services can vary from case to case.

As the set of available Web services expands, advanced tools will be needed to help identify services that match a customer's functional and security requirements. It is important for service providers to describe their service capabilities and for service requesters to describe their requirements in an unambiguous and semantic way. Techniques that take advantage of Semantic Web technologies can improve discovery capabilities. An existing standard for Ontology Web Language for Services (OWL-S) is an example, but more work needs to be done to integrate such technologies into Web service registries. In OWL-S, the service requester can describe the service requirements using terms from a semantic model. Reasoning techniques are then used to find the semantic similarity between the service description and the request to find a set of matching services automatically. Both UDDI and OWL-S can be used to specify the security properties of a Web service, but this security support is not available for the discovery process. However, W3C's Semantic Annotations for WSDL is a step in the direction of merging Web services discovery technology with semantic Web technology. Even with semantic Web services discovery, true automation will require that the requester be able to determine explicitly the security requirements of the provider in addition to its functionality.

End-to-End Quality of Service and Protection. Most Web services deployed do not provide guarantees for Quality of Service (QoS) or Quality of Protection (QoP) under the scenario of attacks. QoS is important in defining the expected level of performance a particular Web service will have. By prioritizing traffic, overall performance of the system can be improved. Standards have been developed for WS-Reliability and WS-ReliableMessaging to provide some level of QoS. Both standards support guaranteed message delivery and message ordering. Other QoS parameters, such as rate of failure or average latency, are usually dealt with by lower-layer protocols. For Web services to truly support QoS, existing QoS support must be extended so that the packets corresponding to individual Web service messages can be routed accordingly to achieve predictable performance.

Overlap between OASIS and W3C Standards. Similar and overlapping Web services security standards that are being developed by different standards bodies are a source of confusion to system developers. These standards are often updated, resulting in interoperability problems and a need for more formal specification and testing of standards.

Methodologies for Web Services Security. The main emphasis of Web services security today is on basic infrastructure (e.g., protocols and languages). As technology matures and Web services become widely adopted, there will be a need for methodologies and recommended practices for security to help developers identify assets to be protected, analyze possible attacks, and decide protection levels and trade-offs.

Availability and Protection from Denial of Service Attacks. Availability enables a Web services application to detect a denial of service (DoS) attack, to continue operation as long as possible, and then to gracefully recover and resume operations after the attack. Techniques are needed to replicate data and services and ensure continuity of operations in the event of a fault. Also needed are management and monitoring solutions to provide service performance and availability monitoring to meet certain service-level objectives.

NIST's Recommendations for Secure Web Services

NIST recommends the following actions to protect Web services. Organizations should consider these actions as part of their risk management processes to balance the economic and operational costs of protective measures and achieve gains in mission capability by protecting systems and data.

- **Replicate Data and Services to Improve Availability.** Since Web services are susceptible to DoS attacks, it is important to replicate data and applications in a robust manner. Replication and redundancy can ensure access to critical data in the event of a fault. This protective measure will also enable the system to react in a coordinated way in dealing with disruptions.

- **Use Logging of Transactions to Improve Non-Repudiation and Accountability.** Non-repudiation and accountability require logging mechanisms involved in the entire Web service transaction. As of mid-2007, there were few implemented logging standards that can be used across an entire SOA. In particular, the level of logging provided by various UDDI registries, identity providers, and individual Web services varies greatly. Where the provided information is not sufficient to maintain accountability and non-repudiation, it may be necessary to introduce additional

software or services into the SOA to support these security requirements.

■ **Use Threat Modeling and Secure Software Design Techniques to Protect from Attacks.** Secure software design techniques facilitate the design and implementation of Web services software without defects that can be exploited. Threat modeling and risk analysis techniques should be used to protect the Web services application from attacks. Used effectively, threat modeling can find security strengths and weaknesses, discover vulnerabilities, and provide feedback into the security life cycle of the application. Software security testing should include security-oriented code reviews and penetration testing. When threat modeling and secure software design techniques are used, Web services can be implemented to withstand a variety of attacks.

■ **Use Performance Analysis and Simulation Techniques for End-to-End Quality of Service and Quality of Protection.** Queuing networks and simulation techniques are important tools in designing, developing, and managing complex information systems. Similar techniques can be used for quality-assured and highly available Web services. In addition to the QoS of a single service, end-to-end QoS is critical for most composite services. For example, enterprise systems with several business partners must complete business processes in a timely manner to meet real-time market conditions. The dynamic and compositional nature of Web services makes end-to-end QoS management a major challenge for service-oriented distributed systems.

■ **Digitally Sign UDDI Entries to Verify the Author of Registered Entries.** UDDI registries openly provide details about the purpose of a Web service as well as how to access it. Web services use UDDI registries to discover and dynamically bind to Web services at run time. Should an attacker compromise a UDDI entry, it would be possible for requesters to bind to a malicious provider. Therefore, it is important to digitally sign UDDI entries so as to verify the publisher of these entries.

■ **Enhance Existing Security Mechanisms and Infrastructure.** Web services rely on many existing Internet protocols and often coexist with other network applications on an organization's network. Many Web service security standards, tools, and techniques require that traditional security mechanisms, such as firewalls, intrusion detection systems (IDSs), and secured operating systems, are in effect before implementation or deployment of Web services applications.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. Publications dealing with some of the issues discussed in NIST SP 800-95 include:

NIST SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government*, provides guidance to federal agencies on how to select cryptographic controls.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance to organizations in identifying the risks to their missions as a result of using information technology, in assessing the risks, and in taking steps to reduce the risks to an acceptable level.

NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, discusses PKI functions and their applications, and the implementation of PKI techniques by federal agencies.

NIST SP 800-44, *Guidelines on Securing Public Web Servers*, helps organizations develop, configure, and maintain secure Web servers.

NIST SP 800-92, *Guide to Computer Security Log Management*, provides advice on developing, implementing, and maintaining effective log management practices throughout an organization.

These publications and other security-related publications are available from NIST's Web site: http://csrc.nist.gov/publications/nistpubs/index.html.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.