

White Paper:

XML Threats and Web Services Vulnerabilities: Understanding Risk and Protection



Table of Contents

Overview	1
A Complete Framework	1
Prevention.....	1
Protection	1
Screening.....	1
SecureSpan™ for Threat Protection	2
The SecureSpan™ Gateway	2
The SecureSpan™ Manager	2
The SecureSpan™ Bridge	2
Message-Level Prevention, Protection, and Screening with SecureSpan™	2
Parameter Tampering	3
Recursive Payloads	3
Oversized Payloads.....	3
Coercive Parsing	4
Schema Poisoning	4
WSDL Scanning.....	4
Routing Detour	4
External Entity Attacks	5
SQL or XQuery Injection.....	5
Replay Attacks	5
XML Morphing	5
Summary.....	5
About Layer 7 Technologies	6
Contact Layer 7 Technologies	6
Legal Information.....	6

Overview

XML-based Web services are becoming a more pervasive foundation technology for integrating applications and exchanging data in service-oriented architectures. Like all new technologies, however, XML-based Web services also present a range of new risks.

New security challenges arise from XML data structures. Granular application calls, input data, or executable attachments can be maliciously constructed to damage or expose a receiving application. XML-based Web services compound the number of vulnerabilities by providing access to application APIs and target applications. The distributed, peer-to-peer nature of Web services also introduces bi-lateral threats and vulnerabilities that can be passed through multiple application hops.

This White Paper reviews various XML or Web services-specific threats that have been identified as potential exploits, examines how to address these threats, and discusses a complete threat protection solution: Layer 7 Technologies' SecureSpan™ portfolio.

A Complete Framework

A complete threat-protection framework needs to address three key functions: Prevention, Protection, and Screening.

Prevention

A protection framework must ensure the secure flow of messages by blocking potential message-level exploits like the insertion of attacks into the message stream. Message signing, sequence numbers, and the use of PKI (public key infrastructure) between clients and services helps ensure message integrity and provides specific protection against man-in-the-middle and replay attacks.

Protection

Software or infrastructure must be able to protect itself and downstream systems against attacks that are designed to render it inoperable. Well-known Web space attacks such as DDoS, payload poisoning, and external commands are as much a threat in XML and Web services deployments. A well-designed processing architecture combined with specific safeguards can help protect against attacks.

Screening

Message-level screening should encompass all traditional firewall functions as well as allow the system administrator to allow or deny specific messages or actions. These functions include comprehensive schema validation, integrity enforcement, encryption/decryption, message content queries, identity verification, and other allow or deny criteria. The ability to delegate or offload specific payload processing to other best-in-class systems — such as a virus scan engine — allows security managers to tailor the scope of the screening as required.

SecureSpan™ for Threat Protection

Layer 7's SecureSpan™ product line provides a turnkey, reusable, and standards-based method for overcoming XML and Web services-specific threats and vulnerabilities. The system secures XML and Web services-based integrations using three components: the SecureSpan™ Gateway XML firewall, the SecureSpan™ Manager to ensure policy compliance, and the SecureSpan™ Bridge for enabling partner connectivity. Each product solves a portion of the challenge; together they combine to provide a comprehensive framework for threat prevention, protection, and screening.

The SecureSpan™ Gateway

The SecureSpan™ Gateway is a hardware accelerated XML firewall that defends access to Web services exposed to business partners and external departments. Delivered as a high-performance rack-mount appliance, blade or remotely configurable software, the SecureSpan Gateway is deployed in a DMZ or data center in front of shared Web services. The Gateway provides integration and security architects administrative control on how Web service get exposed to and accessed by external applications. These includes controls for defining policy around transport, data translation, identity, credentialing mechanisms, PKI, access preferences, XML threats, data validation, communication integrity, privacy management, SLA, audit and so forth.

The SecureSpan™ Manager

The SecureSpan™ Manager is a SOA Policy Compliance Manager for controlling and validating Web services policies in B2B and cross-enterprise environments. Through an intuitive user interface, administrators connect to shared services, establish trust and identity sources with existing infrastructure, and use these sources to define identity specific policies through a declarative policy language of security and SLA assertions. After policies are defined and provisioned they can be validated and audited across an integration to ensure transaction compliance to business and regulatory rules.

The SecureSpan™ Bridge

The SecureSpan™ Bridge is an XML VPN client for enabling fast and flexible partner connectivity in XML and Web services environments. Deployed as software or hardware in partner environments the SecureSpan Bridge provides a code-free mechanism for managing PKI, Single Sign-on, Federation and Security Change Management in cross-domain Web services integrations.

Message-Level Prevention, Protection, and Screening with SecureSpan™

The first step in protecting critical Web services resources is to ensure that all incoming messages are screened for potential threats to the downstream service or the protection infrastructure itself. Some of these threats may be the result of poorly designed or

implemented client-side code, while others may be malicious. In either case, administrators need the flexibility to identify and react to non-conformant messages or operations while allowing secure access by trusted parties. This requires dedicated, purpose-built technology designed to process XML and Web services protocols as thoroughly and efficiently as possible.

The following list reviews various XML and Web services threats and discusses how SecureSpan™ addresses these threats on a message-by-message basis.

Parameter Tampering

Parameters are used to send client-specific information to a Web service so that a certain remote operation can be executed. Instructions on how to use parameters are described in a WSDL (Web Services Description Language) document. Potentially, an attacker could manipulate the parameter options to retrieve unauthorized information.

SecureSpan™ uses strict schema validation and XPath queries to verify parameter content and ensure that parameters are used for legitimate purposes only. Additionally, the SecureSpan™ Manager's WSDL wizard can be used to expose only a specific subset of the WSDL code, further restricting potential exploits.

Recursive Payloads

XML can nest elements within a document to address complex relationships such as a purchase order that includes shipping and billing addresses and quantities. Attackers can attempt to break an XML parser by creating a file with thousands of nested elements.

SecureSpan™ can apply both schema validation and nesting depth limits that will deny these types of attacks. If elements are unreasonably nested, then the SecureSpan™ Gateway FastPath XML Stream Processor will stop parsing when the predefined nesting threshold is crossed and reject the message.

Oversized Payloads

Since XML is relatively verbose, potentially large files are always a consideration in a protection infrastructure. Programmers can limit a document's size, but there are a number of reasons why a file may be hundreds of megabytes or gigabytes. Large file sizes, however, could also mean that an attacker is attempting to manipulate the parser to execute a denial-of-service attack.

Layer 7's FastPath XML Stream Processing technology ensures that all message parsing is driven explicitly by defined policy expectations rather than by the arbitrary content of message payloads. Therefore, a denial-of-service attack will not impact the SecureSpan™ Gateway parser itself. If downstream applications are particularly sensitive to message size, then size thresholds can also be enforced at the Gateway.

Coercive Parsing

A coercive parsing attack attempts to exploit the “bolt-on” interfaces used to link legacy systems with XML components in an existing infrastructure. The attack tries to overwhelm a system's processing capabilities or install malicious mobile code.

SecureSpan™ protects back-end systems and limits Web service access by enforcing strict policy compliance. Attackers will not have the appropriate credentials, and will be denied access to the protected Web service. Schema validation and size restriction checks can also be used to ensure that messages comply to expected parameters and do not overwhelm any “bolt-on” components.

Schema Poisoning

XML schemas model an XML document's grammar and template structure. Parsers use schemas to properly interpret Web service messages. Since schemas describe necessary pre-processing instructions, they are vulnerable to tampering if not stored securely. An attacker may attempt to compromise the schema file itself and replace it with a similar but modified one at a different location.

SecureSpan™ does not load schemas from unauthorized locations. All schema locations are configured by the SecureSpan™ Gateway administrator independent of the sender. Administrators can also choose to load the schema files once and persist the schemas locally in the Gateway, blunting the impact of any changes to the source file.

WSDL Scanning

WSDL is a mechanism for Web services to dynamically describe the parameters used when connecting to commands that accept input from external sources. WSDL files are often built automatically using tools designed to expose and describe all information available in a command. An attacker might cycle through the various command and string combinations to discover unintentionally related or unpublished application program interfaces.

SecureSpan™ selectively proxies all internal WSDLs, shielding access to the original WSDLs on application servers. The SecureSpan™ Gateway will deny direct access to all WSDLs even when an attacker guesses a related unpublished WSDL. The SecureSpan™ Manager's WSDL tool can also expose only a specific subset of an exposed WSDL, further restricting potential exploits.

Routing Detour

The Web Services-Routing specification helps direct XML traffic through an environment by allowing a way station in an XML path to assign routing instructions to a document. The way stations can be compromised, allowing attackers to insert bogus instructions to re-route a confidential file. The attackers can then strip out the malicious instructions before forwarding the document to its destination.

SecureSpan™ is typically deployed in front of any way stations and therefore protects against direct access. The enforcement of message-level security through XML signing and encryption

ensures the integrity of routing-specific fields and the payload itself, preventing and identifying any tampering.

External Entity Attacks

XML can build documents dynamically by pointing to a URI (Uniform Resource Identifier) where the actual data exists. These external entities may not be trustworthy, as an attacker could replace the data being retrieved with malicious data.

By default, SecureSpan™ does not resolve external entities. The SecureSpan™ Gateway can be configured through the XPath policy assertion to block all messages containing references to external entities.

SQL or XQuery Injection

By executing multiple commands in an input file, SQL or XQuery injection could be used by an attacker to execute multiple commands in an input field, allowing access to native stored procedures or unvalidated commands.

The SecureSpan™ schema validation process verifies that the basic structure of the message conforms to defined expectations. The Manager's pre-defined threat filter can also be applied to detect and reject specific commands — such as SQL Selects — on a service-by-service basis.

Replay Attacks

In a replay attack, attackers issue repetitive SOAP (Simple Object Access Protocol) messages in an attempt to overload a Web service or XML parser.

SecureSpan™ can enforce message rate limits on a per-service or per-originating address basis. These settings automatically reject obviously spurious messages from either intentional attacks or misbehaving client applications.

XML Morphing

XML can be legitimately transformed for any number of reasons, but malicious morphing can transform an XML document and its contents into something completely different than its source intended. This can be exploited by an attacker to cause unexpected or inappropriate behavior of previously legitimate messages.

SecureSpan™ does not apply embedded transformations from external entities without administrator permission. Schema validation can also be used to ensure the rejection of any messages whose format does not match expectations.

Summary

In many ways, XML and Web services-specific threats are no different from existing forms of threats and attacks. The unique challenge is ensuring that any enterprise threat protection strategy addresses XML-specific threats before wide-spread deployment of XML or Web services.

Layer 7's FastPath XML Stream Processing is designed to screen out XML threats in real-time before they consume valuable internal resources. Thus, the three-component system helps to reduce the impact of many attacks while ensuring a high-availability Web services deployment.

While intelligent application design and basic network security measures are still very important, the SecureSpan™ product line provides a highly effective framework to protect XML and Web services-based applications.

About Layer 7 Technologies

Layer 7 Technologies (www.layer7tech.com) helps enterprises realize secure, cost-effective business integration using XML and Web services. The Layer 7 SecureSpan portfolio is designed to govern and accelerate Web service integrations spanning security and identity domains, without expensive and inflexible programming. The benefit to business includes faster time-to-market, lowered integration costs and security consistency across federated departments and partners.

Contact Layer 7 Technologies

Layer 7 Technologies welcomes your questions, comments, and general feedback.

Email:

info@layer7tech.com

Web Site:

www.layer7tech.com

Phone:

1-800-681-9377

Legal Information

Copyright © 2005 by Layer 7 Technologies, Inc. (www.layer7tech.com). Contents confidential. All rights reserved. SecureSpan™ is a registered trademark of Layer 7 Technologies, Inc. All other mentioned trade names and/or trademarks are the property of their respective owners.