zapthink
zapnote

Doc. ID: ZTZN-1152
Released: May 25, 2004

ZAPTHINK ZAPNOTE™

TEROS
SECURING WEB SERVICE DATA AND INTERFACES

Analyst: Ronald Schmelzer

Abstract

As systems become more distributed and abstracted through Web Services-based SOAs and other means, it becomes increasingly difficult for a company to gain adequate knowledge of their vulnerabilities and the level to which their systems are exposed. In addition, companies must safeguard the data that is transmitted between systems. In the case of Web Services, this data is known as the "payload" that is transmitted within and between organizations.

Teros leverages a history of providing deep content inspection for traditional Web applications that is apropos for solving Web Services payload and interface security challenges. The Teros Web Services Security Gateway applies application learning to implement enhanced security controls on application inputs.

Securing Both the Data and Interfaces to Web Services

Traditionally, when companies think about securing their software assets, they tend to think about securing access to the programmatic interfaces and making sure that unauthorized parties aren't able to snoop on interactions between systems. Certainly, there are substantial solutions in this space, ranging from technologies such as SSL that secure Web-based traffic to Enterprise Identity Management (EIM) systems that aim to provide strong sources of identity tied to authoritative policy management systems on the network. And on the whole, these systems provide significant value to the enterprise.

However, there remains a significant challenge in making sure that the data that is transmitted by an application and the interfaces themselves are secured. What is to stop a malicious intruder from gaining access to a system through legitimate means and sending dangerous or unauthorized data to the interface? As systems become more distributed and abstracted through Web Services-based SOAs and other means, it becomes increasingly difficult for a company to gain adequate knowledge of their vulnerabilities and the level to which their systems are exposed.

In addition, companies must safeguard the data that is transmitted between systems. In the case of Web Services, this data is known as the "payload" that is transmitted within and between organizations. This payload information might be insurance claims, electronic patient records, or simply acknowledgements of transactions received. Whatever the size, companies must safeguard these payloads from illegitimate transactions and improper usage. Finally, all this security activity must happen in a way that doesn't slow down the overall performance of the network. Thus remains the challenge of deep content inspection at network speed.

Teros: Securing the Service Payload

Teros provides a solution that terminates HTTP and HTTPS traffic and parses both inbound Web requests as well as Web server responses to enforce correct application behavior. Their solution "learns" correct behavior by tracking the state of each user session and deeply inspecting all input data submitted to applications. With this knowledge, the Teros gateway performs data type inferencing and recommends constraints on application inputs to automatically block unauthorized and unexpected data, such as SQL commands and buffer overflow exploits.

Teros has applied the above capabilities now to Web Services payloads and interfaces. Rather than focusing on making sure that Web Service requests simply conform to key specifications, the Teros solution is designed to defeat attacks and security compromises at the XML document and element level. They use historical information from Web Services requests, as well as WSDL file definitions, to control input data types for each Web Services operation. For example, Teros can ensure that a Web Services operation only receives input data types conforming to phone numbers, thus blocking unauthorized inputs such as SQL commands.

In addition to controlling inputs to Web Services applications, the Teros gateway also provides specific attack defenses to block exploits such as SQL injection, buffer overflows and denial of service (DoS) attacks. The Teros solution also stops identity theft by blocking the disclosure of sensitive corporate and customer information (e.g. credit card and social security numbers) in application responses. A common management console is leveraged to define and enforce consistent security across all applications.

As a result of the above capabilities, the Teros application gateway delivers well-tested and proven attack protection for both Web (HTML) and Web Services (XML) in a single security appliance.

Teros Products

Teros	Availability: Now

Overview:

The Teros Web Services Gateway is a hardened security appliance that is deployed directly in the data path of Web Services application traffic and blocks attacks that are not detected by network-based firewalls and intrusion detection systems. The Teros Gateway enforces a positive security model that only permits correct application behavior, without relying on attack signatures. It provides defenses for vulnerabilities that may exist within custom applications, as well as the known weaknesses in commercially developed software.

Details:

- *Teros Web Services Security Gateway* -- Delivers proven defenses against application-layer exploits, such as buffer overflow attacks, SQL injection attempts, denial of service (DoS) attacks and more. The Teros Web Services Security Gateway defends Web Services applications against attack and provides deep content security for confidential data objects.

Key Differentiators:

- *Security that focuses on the payload and interface data* – Rather than focusing just on authentication and access control, Teros Web Services Gateway focuses on the payload and interface data exposed and exchanged by Web Services assets. The Teros solution automatically learns WSDL (Web Services Description Language) message types and formats. It then presents recommendations to the security manager for tightening constraints on inputs to Web Services applications.

- *Deep content inspection at wire speed* – The Teros Web Services Security Gateway is a hardware network device that can operate on Web Services payloads and interfaces without imposing additional latency or processing bottlenecks.

Value Proposition:

Key Teros benefits include:

- Advanced security capabilities through inspection of not just Web Services authorization and destination, but also of the payload and interface data.
- Low cost of security definition maintainability through sharing of Web, Web Service rules definitions.

The ZapThink Take

As companies seek to widely deploy Web Services throughout and outside their corporations, they will necessarily need to address the critical security issues raised by standards-based access to ubiquitous computing resources. While there are many solutions on the market focusing on securing access to Web Services resources, there are few that grapple with the challenge of managing the data that is exchanged between "trusted" parties. The Teros solution is unique on the market with this focus, and ZapThink believes that companies that

seek a complete solution to their Web Services security concerns must at some point implement security measures that address the payload and interfaces themselves and not just access to those interfaces.

Profile: Teros May 2004

Date Founded: 2000 (Formerly named Stratum8)
Funding:
Privately-Held, Venture-backed: Institutional Venture Partners, BA Venture Partners, New Enterprise Associates , CMEA Ventures, Chevron Ventures
Employees: 50
CEO: Bob Walters
Products:
- *Teros Web Services Security Gateway*

Address:
3965 Freedom Circle, 9th Floor
Santa Clara, CA 95054
URL: http://www.teros.com
Main Phone: 408-850-0800
Contact:
Greg Smith
gsmith@teros.com
(408) 850-0844

Related Research

- *XML and Web Services Security* Foundation report (ZTR-WS104)
- *Service Orientation Market Trends* Foundation Report (ZTR-WS110)

About ZapThink, LLC

ZapThink is an IT market intelligence firm that provides trusted advice and critical insight into XML, Web Services, and Service Orientation. We provide our target audience of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

ZapThink's role is to help companies understand these IT products and services in the context of SOAs and the vision of Service Orientation. ZapThink provides *market intelligence* to IT vendors who offer XML and Web Services-based products to help them understand their competitive landscape and how to communicate their value proposition to their customers within the context of Service Orientation, and lay out their product roadmaps for the coming wave of Service Orientation. ZapThink also provides *implementation intelligence* to IT users who are seeking guidance and clarity into how to assemble the available products and services into a coherent roadmap to Service Orientation. Finally, ZapThink provides *demand intelligence* to IT vendors and service providers who must understand the needs of IT users as they follow the roadmap to Service Orientation.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOAs by vendors, end-users, and the press. They are in great demand as speakers, and have presented at conferences and industry events around the world. They are among the most quoted industry analysts in the IT industry.

ZapThink was founded in October 2000 and is headquartered in Waltham, Massachusetts. Its customers include Global 1000 firms, public sector organizations around the world, and many emerging businesses. ZapThink Analysts have years of experience in IT as well as research and analysis. Its analysts have previously been with such firms as IDC and ChannelWave, and have sat on the working group committees for standards bodies such as RosettaNet, UDDI, CPExchange, ebXML, EIDX, and CompTIA.

Call, email, or visit the ZapThink Web site to learn more about how ZapThink can help you to better understand how XML and Web Services impact your business or organization.

ZAPTHINK CONTACT:

ZapThink, LLC
11 Willow Street, Suite 200
Waltham, MA 02453
Phone: +1 (781) 207 0203
Fax: +1 (786) 524 3186
info@zapthink.com
www.zapthink.com