zapthink
zapnote

Doc. ID: ZTZN-1182
Released: October 20, 2005

ZAPTHINK ZAPNOTE™

LAYER 7 TECHNOLOGIES
SOLVING PORTAL CHALLENGES WITH CROSS-DOMAIN SOA SECURITY

Analyst: Jason Bloomberg

Abstract

Companies are implementing Service-Oriented Architecture because it abstracts disparate, heterogeneous IT resources, enabling them to reuse business Services that users can access through a variety of methods, such as corporate portals. However, there are several barriers to widespread SOA adoption, including the fact that most companies isolate their security, identity, and policy information in disparate, inconsistent identity stores, or *identity silos*.

This identity problem centers on managing authentication and authorization between the user and the underlying Web Services. Companies must tackle the problem of identity silos to make progress with their SOA initiatives. Layer 7 Technologies offers a suite of SOA security and policy management products that resolve the identity silo problem by federating identity information, providing a critical part of a secure SOA infrastructure.

Portals and Security Context Challenges in a Service-Oriented Architecture

Corporate portals have become established fixtures at many companies as the primary user interface to diverse enterprise applications. While portals have achieved widespread success in meeting the goals of information visibility, access to applications, and aggregated reporting, companies have faced two critical limitations on the application of portals to critical IT problems: the ability to integrate application functionality across heterogeneous systems in a flexible manner, and the ability to provide a consistent, enforceable, and mangeable security infrastructure across disparate identity systems distributed throughout the organization.

To address these issues, Service-Oriented Architecture (SOA) has become the primary approach for dealing with the difficult issues of heterogeneity in the enterprise. By providing a unified architecture for delivering information and functionality consistently across both Web interfaces and Web Services, SOA promises significant IT benefits including flexibility and reuse of IT assets. SOA exposes back-end systems and legacy applications as Service assets that Service consumers can access and compose into higher-level business processes. As a result, companies are looking for ways for their portal initiatives to leverage the benefits that SOA offers. Portals serve as one of the primary applications that can serve as Service consumers.

However, in order to realize the SOA vision of loosely coupled, composite Services that abstract heterogeneous environments, organizations must first tackle the significant issues of managing security, policy and transactional preferences consistently between disparate applications. Bridging browser-centric portals and Web Services, however, creates security and XML processing challenges. There must be a way of translating user credentials for authenticating against a Web portal into a Web Services request. Web services must then perform independent authentication and authorization decisions based on the content of various XML messages. Portals that support different rights and capabilities will then have to deal with diverse transport protocols, as well as data normalization and personalization issues.

The underlying problem with providing such unified security in an SOA is one of *context*. Business Services that abstract heterogeneous application functionality present a significant challenge to the identification of the user of that functionality and what rights, privileges, and responsibilities they have across the various back-end systems. However, when the user is separated from the Service because applications appear in separate *security domains*, that context is lost. The challenge with securing heterogeneous interfaces is therefore to maintain this context, even when the user is many steps removed from a Service.

Since SOA provides a layer of abstraction, it is important to maintain the security context, including the rules and policies that apply to that user, as well as information about the business process or transaction the user is currently participating in across this layer of abstraction. A single Web Service might expose functionality from several systems and applications, and in some cases, those applications may change over time. Therefore, it's

important to maintain the security context across the entire IT infrastructure to ensure the appropriate security.

To get a handle on this problem of SOA security, it makes sense to start with how the infrastructure represents users – in other words, with *identity*. Because a Service network can potentially touch all the users and applications in an enterprise – as well as users and applications at other companies – the enterprise must be able to manage the identities of those users, as well as the security policies that apply to those users, separate from the applications that interact with those identities. However, making sure that users follow policies across distributed, loosely-coupled Services that span security and identity domains requires companies to adopt new ways of defining, managing, and enforcing policies. In addition, companies require a mechanism for controlling and auditing how they deploy and enforce policies across security boundaries in order to assure compliance with corporate policies and/or regulatory requirements. At the root of the SOA security challenge, therefore, is how an application in one security domain determines the access rights for those identities that originate in a different security domain.

Breaking down Application and Identity Silos

One of the reasons that security remains a challenge is because today's businesses have implemented a variety of specialized applications that they typically purchased or developed in isolation at different points in time. The result of this incremental IT decisionmaking is a set of *application silos* consisting of isolated, monolithic applications, disparate interfaces, and different data schemas. Many integration approaches have sought to resolve the application silo problem with limited success. SOA now represents a new approach to breaking down these silos, enabling the sharing of reusable application components across any number of diverse applications or platforms, leveraging the power and flexibility of standards-based Web Services.

Web Services, however, still leave the problem of *identity silos*. Identity silos contain different sets of user identities and security technology that represent users and groups of users in different, inconsistent ways. Such silos are significant hurdles to the successful integration of applications residing in different security domains, even when a company is adopting SOA.

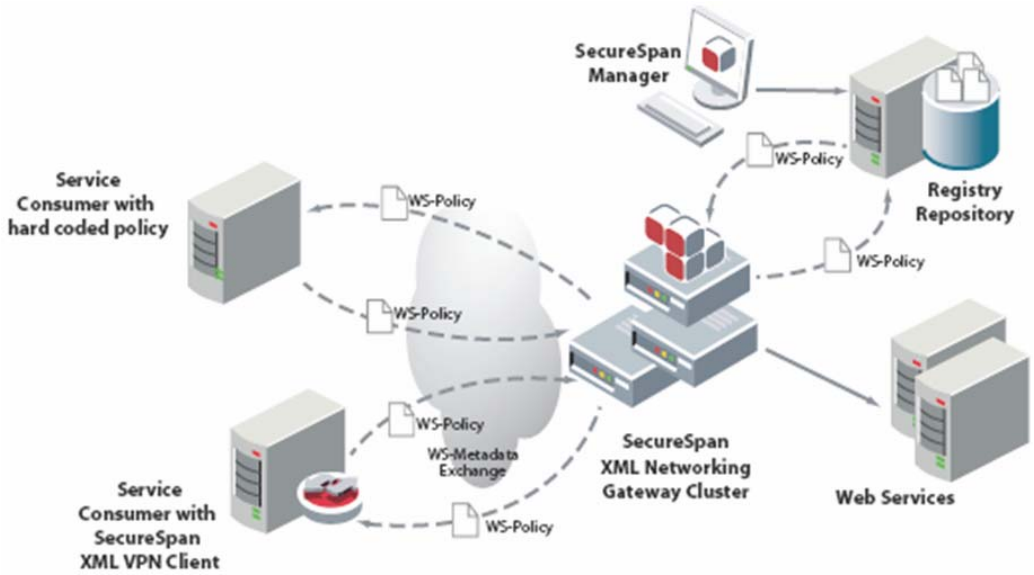
Identities created locally rarely have relevance outside of their local security domain. As a result, identity silos within an enterprise or between partners complicate the process of authenticating and authorizing users. If a legitimate user, application, or Web Service authenticates against an identity provider in one identity silo, their identity or any evidence of their authentication may have no relevance when that user requests access to another application or Web Service in another identity silo.

Breaking down such identity silos in an SOA implementation requires a policy control and audit framework that can span security and identity domains. It also requires an ability to centrally define policies for how to access, provision, and enforce Web Services, as well as the ability to publish that policy to any consuming application trusted to access the Web Service. This last step requires a mechanism for establishing *trust* between the provider and consumer of each Service by validating external identities in a consistent manner. Provisioning identities in this heterogeneous environment of trust requires that both ends of any interaction can provide proof that they have properly negotiated and implemented policies on both sides of each interaction. Therefore, providing such proof is essential to establishing trust between security domains and breaking down the corresponding identity silos.

Layer 7 Technologies: Enabling Portals with SOA

Vancouver-based Layer 7 Technologies provides an environment for governing SOA policy across loosely-coupled Services that addresses these issues of context and identity across security domains. Their *SecureSpan* product suite includes the *SecureSpan XML Firewall*, *SecureSpan XML VPN*, and *SecureSpan Manager.* These products enable the establishment of PKI-based trust relationships between portals and Service providers, provide policy authoring and validation, and automatically provision policy across all Service endpoints. Administrators define policies inside the SecureSpan Manager product and then publish them for runtime enforcement to the SecureSpan XML Firewall for the portal to execute, or to a UDDI registry for centralized storage. The figure below illustrates how these products work together to build a secure environment for SOA.

The Layer 7 Technologies SecureSpan Product Suite



Source: Layer 7 Technologies

SecureSpan resolves the identity silo problem by abstracting the individual identity mechanisms in each security domain, so that a user's identity at the portal interface maintains its context across the domains. Regardless of the authentication and authorization mechanism, SecureSpan translates each authorization into a SAML token that applications and Services can understand. When users access multiple back-end applications through a portal, Identity and Access Management (IAM) products exist for providing one-time login or single sign-on (SSO) capability to the systems. The user only needs to login one time on the portal to bootstrap the SSO process. The SecureSpan XML Firewall and SecureSpan XML VPN can then extend this SSO sessioning model to remote applications interacting with Web Services.

The SecureSpan XML Firewall integrates with several Web SSO products and allows for the reuse of Web session tokens for Web Services interactions. The SecureSpan XML VPN can then perform a similar role to a portal by forwarding client credentials, retrieving and caching cookies or session tokens, embedding these tokens in SOAP messages, and performing URI-based redirects to the appropriate Service. The end result is seamless SSO across multiple back-end Web services without complex client-side programming. The SecureSpan XML VPN automatically handles SSO operations on behalf of one or more Web Services client applications, leveraging the same SSO infrastructure that a company has already acquired and implemented for the Web, saving both implementation time and expense.

The ZapThink Take

There are two fundamentally different approaches for dealing with identity silos: *centralization* and *federation.* A company can attempt to centralize their various identity stores into a single, authoritative system that tracks all users, groups, and policies across the organization. Centralization is the most straightforward approach since it is easy to implement in a single product, but it doesn't scale well across distributed enterprises, it is difficult to sell to siloed IT management, and it isn't appropriate for most business-to-business scenarios.

The alternative to centralization is *federation*, where separate identity stores remain, but the company introduces an infrastructure that allows these repositories to interact. Federation offers better scalability than centralized approaches, and can often overcome political and cross-organizational issues where centralization cannot. However, federated approaches are far more complex and difficult than centralized approaches, since they require sophisticated integration and coordination techniques. Layer 7 Technologies has focused on this challenge, and has built significant capabilities in its suite for addressing the federated policy and security challenges.

Many organizations find that the lack of a federated identity infrastructure hobbles their corporate portals. In the absence of effective federation, portal applications must interact with disparate back-end systems, either by supporting multiple identities for multiple systems, or making do with access to that portion of enterprise functionality that supports a centralized identity store. However, identity federation alone doesn't resolve all the issues facing today's portals – for that, companies also need SOA. Layer 7 Technologies' SecureSpan product suite therefore does critical double duty, resolving the issues of identity silos while also enabling secure SOA.

Product Features

SecureSpan Product Suite

Overview:

Layer 7 Technologies' SecureSpan product suite secures and governs XML and Web Services interactions spanning departments, business units, and partners. Providing XML firewall capabilities, adaptive policy enforcement, and client-side security coordination, SecureSpan ensures secure and flexible Web Services deployments across security and identity domains.

Features:

The SecureSpan product suite comprises three interoperable products that protect applications exposed as Web Services, connect applications across security and identity domains, and validate policy compliance end-to-end across transactions.

- The *SecureSpan XML Firewall* is an XML firewall and Web Services gateway that protects and controls the access to shared Web Services and their exposure to applications in external identity and security domains. It enforces access, privacy, integrity, threat, content, availability, audit, transformation, routing and service virtualization functions for communications entering and leaving a Web Services deployment.

- The *SecureSpan XML VPN* speeds and secures Web Services integrations spanning identity and security domains. It provides architects the ability to connect Web Services with clients in outside departments and partners without manually coding PKI, SSO, identity federation, security, non-repudiation and quality of service policies.
- The *SecureSpan Manager* allows administrators to centrally define, provision, verify and audit fine-grained security and connectivity policies for cross-domain Web Services and XML integrations. It allows graphical scripting of complex policies and context-based rules, enabling end-to-end policy management and compliance.

Value Proposition:

- With SecureSpan, customers realize lowered integration costs, increased security reliability, faster time to production, and the ability to future-proof their Web Services and SOA initiatives.

Profile: Layer 7 Technologies October 2005

Funding:
GrowthWorks Venture Capital, BDC Venture Capital
President and CEO:
Lonny McLean
Product:
SecureSpan Product Suite
Address:
P.O. Box 10095
1501-700 West Georgia St.
Vancouver, BC
V7Y 1B6
URL:
http://www.layer7tech.com
Phone:
800-681-9377
Contact:
info@layer7tech.com

Related Research

- *High Performance and Appliance Approaches for XML* Report (ZTR-DI102)
- *Service Orientation Market Trends* Foundation Report (ZTR-WS110)
- *Reactivity* ZapNote (ZTZN-1180)
- *Conformative Systems* ZapNote (ZTZN-1171)

- *DataPower* ZapNote (ZTZN-1159)
- *Forum Systems* ZapNote (ZTZN-1170)
- *Sarvega* ZapNote (ZTZN-1165)

About ZapThink, LLC

ZapThink is an IT advisory and analysis firm that provides trusted advice and critical insight into the architectural and organizational changes brought about by the movement to XML, Web Services, and Service Orientation. We provide our three target audiences 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 helps its customers in three ways: by helping companies understand IT products and services in the context of Service-Oriented Architecture (SOA) and the vision of Service Orientation, by providing guidance into emerging best practices for Web Services and SOA adoption, and by bringing together all our audiences into a network that provides business value and expertise to each member of the network.

ZapThink provides market intelligence to IT vendors and professional services firms that offer XML and Web Services-based products and services in order to help them understand their competitive landscape, plan their product roadmaps, and communicate their value proposition to their customers within the context of Service Orientation.

ZapThink provides guidance and expertise to professional services firms to help them grow and innovate their services as well as promote their capabilities to end-users and vendors looking to grow their businesses.

ZapThink also provides implementation intelligence to IT users who are seeking guidance and clarity into the best practices for planning and implementing SOA, including how to assemble the available products and services into a coherent plan.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOA by vendors, end-users, and the press. Respected for their candid, insightful opinions, 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 and government organizations, as well as many emerging businesses. Its analysts have worked at such firms as IDC, marchFIRST, and ChannelWave, and have sat on the working group committees for standards bodies such as RosettaNet, UDDI, and ebXML.

Call, email, or visit the ZapThink Web site to learn more about how ZapThink can help you to better understand how SOA will 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