zapthink white paper

SOA Security: Centralize & Integrate

SOA Security at SAIC

ZapThink, LLC • 108 Woodlawn Road • Baltimore, MD 21210 • info@zapthink.com • www.zapthink.com

SOA Security: Centralize & Integrate

SOA Security at SAIC

August 2007

Analyst: Tony Baer

Abstract

SOA adds a new dimension to information technology (IT) security challenges. Usage is dynamic and conditional. At design time, Service providers may not know how users may eventually consume the Services. Making trust explicit, therefore, is a key requirement for SOA, while establishing a dual-level of coarse and fine-grained entitlements is critical for efficiently supporting the security needs of large groups of Services from diverse application sources.

SAIC, a systems integrator with over 37 years of serving public and private sector clients with some of the world's most demanding security requirements, is applying its expertise and investing heavily in SOA. As a result of their extensive research involving multiple technologies and vendors covering client application authentication, XML Security Appliances, and application server platforms across a variety of SOA scenarios, SAIC has developed a general architecture for SOA Security which provides centralized coarse-grained authorization and access control, while implementing fine-grained authorization at the service level.

Recently applying that experience to a pioneering installation serving a multinational oil and gas company, SAIC has implemented a scalable SOA solution and SOA security architecture for B2B collaboration that interoperates across a diverse internal environment with multiple standards for enforcing security.

I. Evolution of IT Security Challenges

SOA relies on the concept of managing trust across business process domains or organizational boundaries.

Service Oriented Architecture (SOA) requires a rethinking of traditional IT security strategy. Working in concert with existing protections, SOA dictates a layered approach that can support federated identity. In place of exchanging user identities, SOA relies on the concept of managing *trust* across business process domains or organizational boundaries, involving wider groups of stakeholders inside and outside the organization. Managing trust, and with it, *entitlement* to the capabilities of Services, requires a far more granular strategy for authenticating the user, granting authorization, and providing access that depends, not only on the user's location or organizational affiliation, but also on the policies that apply to the particular Service. Security has long been a hallmark of enterprise IT systems. It is essential to ensure only the right people or organizational entities have read or write access to specific classes of data—and that only certain classes of users are authorized to execute specific processes that impact or use the data.

Life in IT has grown more complicated from the days when users accessed systems through dumb terminals to use static, self-contained applications. The complexity of IT architectures increased as legacy systems evolved to perform B2B transactions across corporate boundaries. The result is a geometric increase in centers of control and exponential increase in points of exposure. Conventional IT systems linked data to specific applications, user classes, and well-defined use cases. Security typically involved building strong perimeter defenses, coupled with user authentication, passwords, and in some cases, certificate authority infrastructures tied specific users to application or database instances.

SOA changed all that. Its loosely coupled nature severed the tight connection between user, application, and data source. Under such a scenario, designers can no longer predict every possible use case in advance. SOA can also promote reuse, sharing, and aggregating of data and processes that may extend beyond traditional groups of known users—and known uses. Increasingly, SOA is enabling processes to dynamically interact across organizational boundaries.

SOA is becoming a pillar of IT strategy because of its potential to help organizations more effectively utilize existing information assets, and leverage the processes that are the essence of their competitive edge. It can promote business agility because it can bridge traditional application and database silos by taking advantage of standards for abstracting and exposing information and process assets for use, and reuse. Furthermore, SOA is an architectural approach that can enable your organization to dynamically engage with partners and customers.

SOA introduces new forms of IT security risk. Enterprises are embracing SOA because the potential benefits of improving agility, competitiveness, and IT alignment with the business make the challenge worthwhile. Enabling technologies, standards, and best practices are emerging to make SOA security very manageable.

II. SOA Adds New Dimension to Security

The dynamic, loosely coupled nature of SOA has, in effect, added a new dimension atop the traditional challenges of managing IT security. From a security standpoint, traditional IT systems provided well-bounded environments where business analysts could identify the user base and could anticipate and design for specific usage patterns based on business requirements and use case development.

The first dimension of security for traditional IT applications usually relied upon explicit user logins and passwords. Even as Web applications opened internal systems to new classes of external users, user names and passwords typically remained the predominant form of access control for both extranets and Internet applications, where the major difference is that, with new classes of external users, access control systems typically had to refine and expand the number of access levels governing user privileges.

The second dimension of security for traditional IT systems was at the perimeter. The importance of perimeter controls grew with the advent of the Web, which magnified threat from intruders, while introducing malware as a new source of threat. Recently, as use of wireless connectivity and increased use of VPNs have multiplied the potential points of entry for intruders, enterprises are evolving firewall-based perimeter defenses to more layered strategies.

As IT architectures evolved from host to distributed client/server, and then to the web, one factor remained constant: Regulation of access could rely on *implicit* trust because the context of the interaction was explicit: IT could plan for the class of user and the type of usage in advance. That fact remained true even as distributed network-based topologies emerged, where users could access data and systems within other domains or server instances, inside the firewall. At this point, tokens began emerging that replaced disclosure of user identity with tickets that authenticated the user. Yet, these early tokens were quite rigid, restricted to authorizing a specific user, from specific client, accessing a specific application, for a pre-defined use case.

Services abstract users from the applications underlying the Service abstraction. Consequently, while trust was implicit for traditional IT applications, for SOA, it must be made explicit.

SOA adds a third dimension to support dynamic and conditional usage where the creator of a Service may not know the user base or the exact ways to consume a Service at design time. By their nature, Services abstract users from the applications underlying the Service abstraction. For instance, an end user might request a specific Service directly, or request it indirectly via an intermediary that is authorized to request that Service. In some cases, the request may trigger the orchestration of multiple Services, from different sources that might have differing criteria for clearing authorizations.

Consequently, while trust was implicit for traditional IT applications, for SOA, it must be made explicit. For instance, when intermediaries are involved, the Service provider must depend on the intermediary to vouch for the original requestor. To avoid reinventing the wheel when defining access privileges for each new Service, a standard mechanism for communicating trust becomes essential for SOA.

To address the unique security requirements of SOA, SAIC's architecture implements a centralized Security and Identity layer. This layer uses Web Service standards that enable clients and Services to rely on the intermediary as a "trust broker." By using a trust broker, a Secure Token Service (STS) can abstract the necessary configurations. Besides centralizing token and identity management, this central trust Service enables enterprises to centralize the point of interaction with other organizations.

This trust management architecture is particularly useful for situations where an organization requires federation across disparate security domains. Federation

between security domains likely causes identity collisions, such as when two systems each have different users named John Smith. Mitigation against these collisions via extended classification, mapping, or other any other method is better handled at a central location to maintain management controls such as versioning and key storage.

The Importance of Authorization and Entitlements

ZapThink considers security as the first roadblock to SOA adoption. A key to the puzzle is resolving the issues of authorizations and entitlements.

ZapThink considers security as the first roadblock to SOA adoption, because without a way to maintain the security context of users across the Service abstraction, no organization will be able to compose arbitrary Services, and thereby realize one of the main benefits of their SOA implementations. A key to the puzzle is resolving the issues of *authorizations* and *entitlements. Authorization* is the act of determining whether a user (or system, process, or Service) is or is not allowed to perform some operation or view some data. In turn, *Entitlements* are corporate, industry, and contractual rules that determine access privileges to resources for specific individuals or groups of individuals.

Authorization is typically involve coarse and fine-grained levels of entitlements. Coarse-grained entitlements involve high-level access control decisions that apply to an entire application, Web site, or Service, yet are also typically devoid of application or Service-specific context. Because the rules—or policies—are broad-based, it is normally more efficient to implement them centrally. An example of a coarse-grained entitlement is determining whether a specific trading partner may gain access to an extranet.

At the next level down is fine-grained entitlement that provides more detailed control decisions, such as access to objects or functions within applications, parts of Web pages, elements in XML documents, or records in databases. For SOA, it's important to implement such entitlements at individual Service level because of their high degree of specificity. An example would be a rule that restricts access to supplier price lists to procurement staff.

Managing entitlements are critical to the functioning of any IT application; for SOA, the need is especially acute because users and providers are abstracted from each other—and from the applications that underlie the Services. For instance, because Web Services can be highly extensible, some cases may involve a requestor acting through one or more intermediaries. Through intermediaries, the requestor may call for Services that may in turn compose one or more sources.

The result is a multi-hop interaction which can occur over varying periods during which infrastructure operating conditions or business policies could change. For instance, the loosely coupled nature of SOA means that a Service might remain the same, while the underlying applications might change. Furthermore, because Service consumption may not always be predictable, providers of a Service may not know who the consumers of the Service are, if users orchestrate the Service dynamically with other Services at run time. Consequently, a centralized or federated ID and access management approach becomes essential for consistent policy enforcement covering the granting of authorizations and acceptance of trusts for SOA.

SAIC's SOA Security architecture implements coarse-grained policy enforcement in the security and identity layer through the use of XML gateway appliances. Gateways proved to be a very flexible solution since they are capable of both performing the duties of the Central Trust Service and policy enforcement. In addition, the gateways provide implementation flexibility due to depth of their capabilities. They gateways could handle as much, or as little of the security enforcement workload as necessary, picking up where a localized implementation

leaves off. It could support fully centralized, decentralized, or hybrid approaches by providing a common building block approach, and offloading compute-intensive burdens such as parsing XML, or handling encryption and decryption. Acting as the centralized Coarse-Grained policy and trust hub, the gateway effectively mediated differences between local security implementations.

III. SAIC's SOA Security

SAIC is a large research and engineering company with more than 44,000 employees in over 150 cities worldwide. SAIC provides products and services to government and commercial customers worldwide in the areas of defense, intelligence, logistics and product support, homeland security, space and life sciences, science and technology and global commercial services. SAIC and its subsidiaries are highly ranked in both the government and commercial arenas. Having served the public and private sector for over 37 years, SAIC has deep experience serving organizations with stringent security requirements including current homeland security as well as performing intelligence Services for two of the world's largest financial institutions. These Services provide a view of threats that extend beyond current perimeter defenses enabling companies to respond to intrusions beyond the reach of traditional IT security measures.

SAIC is developing architectures which incorporate multiple technologies and vendors to cover issues ranging from client application authentication and XML security appliances to application server platforms.

As a recognized leader in the areas of IT services and IT security, SAIC is now focusing its years of experience on SOA. Investing heavily in SOA research and development (R&D), SAIC is developing architectures which incorporate multiple technologies and vendors to cover issues ranging from client application authentication and XML security appliances to application server platforms. R&D use cases have covered everything from simple point to point Web Service calls to complex, multi-domain compound Service calls. As a result of these R&D efforts and through numerous client implementations, the company has developed a deep understanding of the technologies, processes and issues involved with implementing SOA, and SOA security strategies.

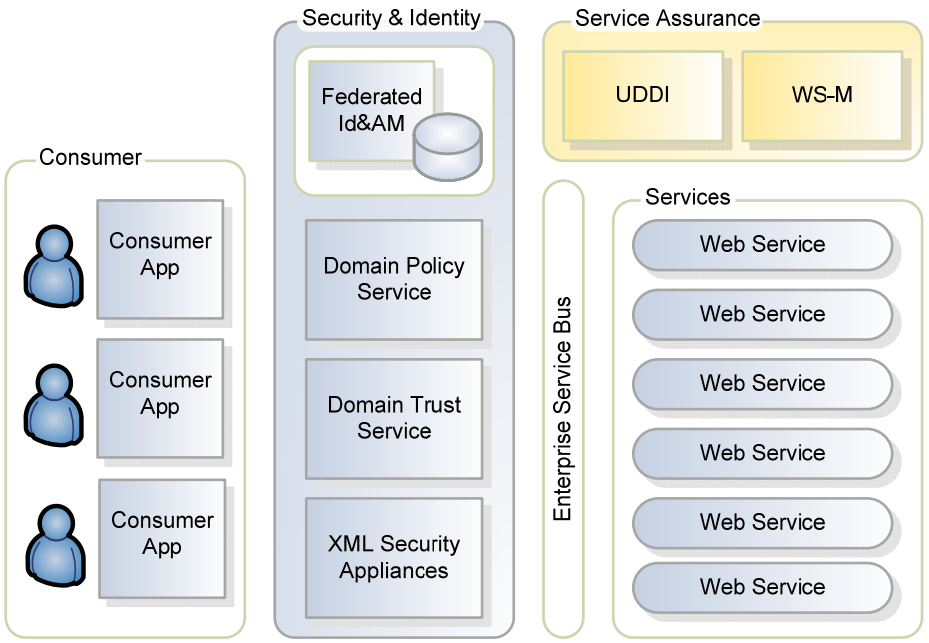
As a vendor-neutral system integrator, SAIC is applying this expertise in helping clients:

- Develop and implement SOA security strategy
- Evaluate the maturity of Web Services standards, and determine which standards to implement
- Evaluate vendor SOA security products

As an example, SAIC is currently working with a global oil and gas company that was looking to SOA to improve integration with trading partners. As a large, diversified global organization, the client had an extremely diverse IT environment across multiple business units. In one organization, it had to contend with BEA, SAP, and Microsoft .NET platforms and applications. The organization's existing IT security infrastructure was similarly varied, including a mix of legacy tokens-based systems such as Kerberos and X.509, plus multiple basic authorization systems relying on user name and password. In many cases, access and authorization were application-dependent. Compounding matters, Web Services standards support throughout the company's emerging SOA environment was highly inconsistent. Different platforms supported different versions of the standards. For instance, one appserver vendor hadn't documented its recent upgrade of WS-Trust support, while another vendor didn't support the standard at all.

In response, SAIC implemented a SOA Security architecture previously developed through its R&D efforts, as shown in the figure below. That architecture, designed to provide a federated, dual-level authorization solution for exchanging trust and granting authorization in highly heterogeneous environments was a perfect fit for the client's SOA needs.

SAIC's SOA Security Architecture



Source: SAIC

SAIC's SOA Security Architecture

Key to SAIC's architecture was a conclusion that it's possible to centralize security and implement mechanisms which allow for the integration of entitlements and identity attributes into the message flow.

Key to SAIC's architecture was a general conclusion drawn from their R&D efforts: it's possible to centralize security and implement mechanisms which allow for the integration of entitlements and identity attributes into the message flow. In other words, developers of both clients and Services can be free from the current burden of needing to "bake in" SOA specific security mechanisms into each client application or Web Service they're developing.

Key design benefits of SAIC's SOA Security architecture:

- Support of standards, including WS-Trust, WS-Security, Web Services, SAML
- Secure Token Service to centrally issue, validate and manage security tokens
- Centralized Coarse-Grained authorization and access control
- Fine-Grained authorization at the Service level using a standardized mechanism to ease development
- Standardized mechanism utilizing out of band message level identity attributes to enable Fine-Grained authorization
- Utilization of XML appliances for providing standards-based integration points for legacy systems that do not implement current standards

Within the architecture, SAIC leveraged recent developments in the area of XML security gateways to implement a central trust Service and a centralized point where they could consistently enforce coarse-grained policies governing access to external partners—a key benefit for organizations contending with SOX and similar compliance burdens. They layered centralized trust Services and policy Services atop existing authorization, authentication, and access control processes which they enforced at the final access points—enabling the client to get the best of both worlds: consistent enforcement at the perimeter, while preserving existing investments and security practices at the business unit.

Making the Case for An Independent Security Partner

There are significant benefits to using an "honest broker" when specifying and implementing SOA security. Heterogeneous IT environments are common in most organizations; few are dominated by single platforms or applications. For instance, even most SAP customers have significant installed bases of third party applications, and many also continue to maintain large mainframe systems. Furthermore, any organization that intends to increase collaboration with external business partners must assume that those entities will operate different applications and platforms.

There is also the challenge of managing diversity in SOA. While most vendors support core web Services standards, vendors typically update support to current versions of these standards on varying timetables. Additionally, key Web Services security standards such as WS-Security, WS-Trust, SAML, and WS-Federation are evolving. Vendors are updating support for these standards at different rates, and in some cases, selectively.

An independent partner can provide an unbiased assessment regarding the readiness of vendor support of critical Web Services security standards, compatibility with the IT environment, and the degree of interoperability that different SOA security offerings provide. Furthermore, testing compliance with Web Services Security standards, and support of the organization's security policies, is essential when building the security infrastructure for SOA. Specifying, testing, and implementing SOA security requires a knowledgeable partner familiar with different commercial implementations. Independent systems integrators are well positioned to deliver successful results.

IV. The ZapThink Take

There is little question that SOA throws some new curves when managing IT security. The prime differentiator is that of context: with conventional IT applications, designers know the interactions and classes of users well in advance. Because the context is known, trust is implicit. SOA changes the equation because the context for consuming the Service may not be known until runtime. Furthermore, because SOA allows for the aggregation of requests and Services, in many cases, the Service provider may not enjoy a full picture of what entities are consuming the Service, and how. Consequently, communicating trust is essential when the Service provider does not always understand the full context of the Service interaction. There is also little question that extending IT security practices to SOA requires specialized knowledge on existing authentication, authorization, and access control processes, and how those processes must be extended to cover the demands of SOA.

Having delivered systems integration Services to demanding private sector clients and all branches of the federal government for over 35 years, SAIC has baked

Having delivered systems integration Services to demanding private sector clients and all branches of the federal government for 35+ years, SAIC has baked information security into its culture.

information security into its culture. Its experience ranges from extensive background conducting security audits for federal agencies to building e-commerce capabilities governing electric power grid capacity management and monitoring cyber threats to global financial institutions.

SAIC is now applying that same rigor to design and validation of SOA security architecture, beginning with an internal research program that is charting the threats in SOA environments and putting its research to practice as it develops and implements SOA security strategy for diversified global entities that are managing Services—not only across multiple internal domains—but complex networks of B2B partnerships as well, SAIC's value proposition leverages years of cybersecurity experience with independence that provides an unbiased view on commercial support of Web Services security standards. Given that commercial support of critical standards for managing federated trust, such as SAML 2.0, is still a work in progress, having an unbiased voice can provide the edge in ensuring successful implementation.

Contact information: SAIC August 2007

For more information, please contact:

Atif Aleemi, AVP, SOA R&D
+1 (703) 625 9134

Chris Mann, AVP, Enterprise Info. Mgmt. R&D
+1 (248) 767 8442

SOA_Security@saic.com

Copyright, Trademark Notice, and Statement of Opinion

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 November 2000 and is headquartered in Baltimore, Maryland.

ZAPTHINK CONTACT:
ZapThink, LLC
108 Woodlawn Road
Baltimore, MD 21210
Phone: +1 (781) 207 0203
Fax: +1 (815) 301 3171
info@zapthink.com

ZapThink, LLC • 108 Woodlawn Road • Baltimore, MD 21210 • info@zapthink.com • www.zapthink.com