

Security In the New World of SOA & Mobile Devices

May 24, 2005

Scott Boehmer

General Manager, Mobile Business Solutions
Sprint Business Solutions

Scott.A.Boehmer@mail.sprint.com

Agenda

- Legislative impacts on Web Services
- Web Services Security Concerns
- SAML & WS-Security interaction to address the security challenges
- Impacts of SAML and WS-Security on Mobility
- View to the Future
- Summary



Security Legislation Requires Businesses to Follow Strict Security Practice Guidelines

- CIOs are feeling security pains and the government has responded by creating standards and legislation requirements to address these security pain points.

- Homeland Security
- The Patriot Act
- Sarbanes-Oxley
- Gramm-Leach-Bliley (GLB)
- HIPAA California Law SB 1386
- California Assembly Bill 1950
- Payment Card Industry (PCI) Data Security Standard
- Government Information Security Reform Act (GISRA)
- Computer Security Enhancement Act of 2001



Legislation Driving Web Services Security

- Notifying people that their information has been stolen is no longer enough. New laws are requiring reasonable steps be taken to secure information.

- California Assembly Bill No. 1950
 - Requires anyone who licenses personal information about a California resident to implement & maintain reasonable security procedures & practices
- Payment Card Industry (PCI) Data Security Standard
 - Created commonly accepted set of industry tools and measurements resulting in a single validation process that will satisfy all the credit card associations
 - This standard applies to all Members, merchants, and service providers that store, process or transmit cardholder data. Subject categories include:
 - » Build and Maintain a Secure Network
 - » Protect Cardholder Data
 - » Maintain a Vulnerability Management Program
 - » Implement Strong Access Control Measures
 - » Regularly Monitor and Test Networks
 - » Maintain an Information Security Policy

SOAs, Web Services, and the Benefits

- **Service-Oriented Architecture (SOA)** is a collection of self-contained services that communicate with each other. The services are interoperate with each other, but are not dependent on the context or state of each other. This distributed systems architecture provides flexible & loose coupling of resources.

- **Web Services** describes a way of integrating a group of loosely related Web-based applications using XML & other standards including SOAP, WSDL, UDDI, & XSD. Allows for different applications from different sources communicating with each other across a common standard, which results in less custom code development.

- Benefits of Web Services:

- **Integration:** Many organizations still have their applications operating in "silos". Web Services breaks down those "silos" & allows applications to share data & functions between each other.
- **Access:** Web Services provides access through different interfaces. In a much simpler manner a Web service can provide access to multiple clients & formats.
- **Flexibility:** Web Services supports "machine-to-machine communications", allowing a Web service to ask another Web service for something. Web Services can even be aggregations of multiple Web Services, resulting in some complex combinations.

Who Should Enhance Their Security?

- As a general rule if you are using simple Web services internally (behind the firewall) that do not involve confidential corporate data your existing security may be adequate

- You should consider enhancing your security to handle Web Services security challenges if you:

- **Begin creating complex Web services**
 - **Are accessing confidential corporate or personal data**
 - **Are extending access beyond the enterprise firewall**
- Many companies begin exploring Web services on simple applications that do not contain valuable corporate or personal data, as your use of Web services matures, so should the use of enhanced security features.



Ease of Integration Introduces Security Problems

- With Web Services any kind of data can be transported, including executables & expandable external references through your traditional firewall security utilizing open ports 80 (HTTP) and 443 (HTTPS).
- **Trust:** Web Services allow direct connectivity to data, not typically available from untrusted networks. As data is passed from one application to the next, the trust needs to be passed along as well.
- **End-to-end is different than point-to-point:** With Web Services messages may pass through several intermediaries and several possible hubs. Consequently, securing the transport channel, as many traditional security methods use, may not be sufficient. Security must be transient and persist from origin to reception.
- To address these challenges new security technologies are required, which is why today we would like to discuss SAML (Security Assertion Markup Language) and WS-Security.

SAML & WS-Security Compliment Each Other

<p>What is SAML? Security Assertion Markup Language (SAML) is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects.</p> <p><i>The Security Language</i></p>	<p>What is WS-Security? WS-Security describes how to attach signature & encryption headers to SOAP messages & how to attach security tokens to messages. Support multiple security token formats, trust domains, signature formats, and encryption technologies.</p> <p><i>The Messaging Language</i></p>
<p>Why use SAML? The SAML standard provides the means by which authentication & authorization assertions can be exchanged between communicating parties.</p>	<p>Why use WS-Security? WS-Security addresses how to maintain a secure context over a multi-point message path. Complex solutions need end-to-end security baked in. The identity, integrity, & security of message & caller need to be preserved while message crosses domains, encryption keys & hops.</p>

Impacts of SAML & WS-Security on Mobility

- Forces businesses to streamline their processes
- Suppliers can use same language to describe offerings
- Simple & reliable way to blend existing systems with new applications & services
- Innovative technology that enables low-cost, platform-neutral systems integration to realize the SOA vision
- Reduces the maintenance burden because each application does not need a copy of external data



- End users will enjoy using applications, services, and devices that are linked together using Web services
- Web services give users ability to act on information any time, any place, & from any smart device
- You can request & get information in real time, & transform it to your particular format. This allows for delivery of individualized software & services

View to the Future

- Industry experts project Web services as **one of the fastest growing Enterprise Integration (EI)** technologies over the coming years
- The **final SAML V2.0 OASIS Standard specification set** as of 15-Mar-2005
- Fourteen organizations joined together and **demonstrated interoperability of the WS-Security OASIS Standard** at the Gartner Application Integration & Web Services Summit in Los Angeles on 20-April-2005



"Mobile is one of the most exciting new areas for applications. We want to make sure these applications are rich and that they fit in with other devices." In addition, "Web services are getting to be so key in this space and we want the Web services calls to be the same on all devices."

- Bill Gates (March, 2004)