

WebServices

.NET J2EE XML JOURNAL

WSJ2.COM

**International Web Services
Conference & Expo**



INSIDE: CONFERENCE BROCHURE



**March 18-20, 2003
Boston, MA
Hynes Convention Center**

**REGISTER BY
MARCH 14
SAVE
\$300**



RETAILERS PLEASE DISPLAY
UNTIL APRIL 30, 2003

\$6.99US \$7.99CAN



**SYS-CON
MEDIA**

PAGE
14

A New World of Web Services Security

Using open B2B process integration platforms as a testing ground

FOCUS ON WEB SERVICES SECURITY

Insecurities

The need to choose



Sean Rhody
3

A Strategy for Securing Web Services

A developer's approach to dealing with security standards in a state of flux

Mark Sechrist

7

We Know Web Services Need Security, But What Type?

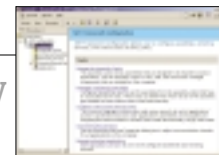
Exciting but not "dangerous" technologies

Mark O'Neill

18

The Basics of Code Access Security

Minimal coding that offers a huge return



Thom Robbins

28

The Security Challenge

A look at a typical case scenario



Marc Chanliau

32

Security Walk before you run - but don't stand still

James Phillips

58

Product Review: Quadrasis/Xtradyne SOAP Content Inspector

Providing comprehensive solutions for Web services security

Joe Mitchko

12

Mobile Web Services: Extending Web Services to the Real World

Using SOAP to access a J2EE-enabled mobile device & Ashwin Rao

Ash Parikh

22

IBM

www.ibm.com/websphere/portalplay

INTERNATIONAL ADVISORY BOARD

Andrew Astor, David Chappell, Graham Glass, Tyler Jewell,
Paul Lipton, Anne Thomas Manes, Norbert Mikula,
Frank Moss, George Paolini, Simon Phipps

TECHNICAL ADVISORY BOARD

Steve Benfield, Bernhard Borges, JP Morgenthal, Andy Roberts,
Ajit Sagar, Michael A. Sick, Simeon Simeonov

EDITORIAL

EDITOR-IN-CHIEF

Sean Rhody sean@sys-con.com

EDITORIAL DIRECTOR

Jeremy Geelan jeremy@sys-con.com

INDUSTRY EDITOR

Norbert Mikula norbert@sys-con.com

PRODUCT REVIEW EDITOR

Joe Mitchko joe@sys-con.com

.NET EDITOR

Dave Rader davidr@fusiontech.com

TECHNICAL EDITORS

David Chappell chappell@sonicsoftware.com

Anne Thomas Manes anne@manes.net

EXECUTIVE EDITOR

Gail Schultz gail@sys-con.com

EDITOR

Nancy Valentine nancy@sys-con.com

ASSOCIATE EDITORS

Jamie Matusow jamie@sys-con.com

Jean Cassidy jean@sys-con.com

ASSISTANT EDITOR

Jennifer Stille jennifer@sys-con.com

PRODUCTION

PRODUCTION CONSULTANT

Jim Morgan jim@sys-con.com

LEAD DESIGNER

Richard Silverberg richards@sys-con.com

ART DIRECTOR

Alex Bolero alex@sys-con.com

ASSOCIATE ART DIRECTOR

Louis Cuffari louis@sys-con.com

ASSISTANT ART DIRECTOR

Tami Beatty tami@sys-con.com

CONTRIBUTORS TO THIS ISSUE

Marc Chanilau, Joe Mitchko, Mark O'Neill, Ashish Parikh,
Jim Phillips, Gilbert Pitz, Ashwin Rao, Sean Rhody,
Thom Robbins, Mark Seistr

EDITORIAL OFFICES

SYS-CON MEDIA

135 CHESTNUT RIDGE ROAD, MONTVALE, NJ 07645

TELEPHONE: 201 802-3000 FAX: 201 782-9637

WEB SERVICES JOURNAL (ISSN# 1535-6906)

Is published monthly (12 times a year)

By SYS-CON Publications, Inc.

Periodicals postage pending

Montvale, NJ 07645 and additional mailing offices

POSTMASTER: Send address changes to:

WEB SERVICES JOURNAL, SYS-CON Publications, Inc.

135 Chestnut Ridge Road, Montvale, NJ 07645

©COPYRIGHT

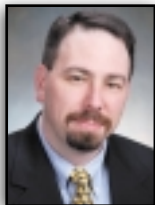
Copyright © 2003 by SYS-CON Publications, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy or any information storage and retrieval system without written permission. For promotional reprints, contact reprint coordinator. SYS-CON Publications, Inc., reserves the right to revise, republish, and authorize its readers to use the articles submitted for publication.

All brand and product names used on these pages are trade names, service marks, or trademarks of their respective companies. SYS-CON Publications, Inc., is not affiliated with the companies or products covered in Web Services Journal.

Insecurities

Written by
Sean Rhody



Author Bio:

Sean Rhody is the editor-in-chief of Web Services Journal. He is a respected industry expert and a consultant with a leading Internet service company.

SEAN@SYS-CON.COM

When I was younger, I found out the hard way that I was allergic to certain medications – I got three shots and went into shock. It left me deeply afraid of needles. To this day, doctors need to give me something to bite on when they give me a shot. Dentists, well, let's just say they need to count their fingers.

But we're not going to talk about my insecurities. Instead, we're going to look at a topic that is on most Web services developers' minds. Security is the most vital topic in the Web services space today, so much so that two competing standards have been proposed and are in the process of being implemented by various vendors.

Security Assertion Markup Language (SAML) is a token-passing system that uses XML to describe security assertions and permissions. It was developed recently and turned over to OASIS, which ratified it as an open standard.

OASIS has also produced the Web Services Security (WSS) standard as an alternative approach to SAML. WSS uses XML, but the format of information and the intent of the specification differ somewhat from SAML. Neither specification is a complete analog of the other – there are differences that make neither a complete subset of the other.

What's really important is that Web services products begin supporting one or both of these standards. The ability to secure Web services is one of the key factors that will drive them from the world of trial implementations into a deep deployment model.

Security means different things to different people. Some are concerned with encryption of data over the wire, so that no outside party can snoop on communications between two computers. Some are concerned with the ability to restrict functionality based on user identity, which perforce requires the ability to validate identity, and then to restrict access based on it in some fashion. Still others are concerned about securing Web services using standard tools for the security definition, such as LDAP.

Whatever the issue, one concept is vitally important – the mechanism for Web services security should not be a new, proprietary mechanism. For security of Web services, the protocols and mechanisms need to fit into the overall security architecture of the company hosting the service. The last thing any company needs is a new security paradigm – companies spend enough time and money defining their policies now, without Web services requiring a different tack.

The good news is that the standards pretty much take this into account. The bad news is that products that implement the basic Web services protocols (SOAP, XML, WSDL, UDDI) do not in general provide any type of security (in the form of SAML or WSS) implementation, and typically have no plans to do so. So it looks like Web services will fragment to a certain extent into a group of core service providers and a group of niche players who will focus on topics like security, management, and monitoring. Which isn't the worst of all worlds, but it certainly is a disappointment to those who want the added value of being able to go to a single vendor for all the tools (and of not having two vendors do the finger-pointing game when something fails to work as planned).

Certainly the major players are involved in the specification development, but it's companies like Netegrity who are actually implementing the standards and developing products to secure Web services transactions.

This issue is devoted to a variety of topics around security. We'll try to introduce some of the issues that you'll encounter as you try to deploy Web services, and look to experts from various security-focused organizations, including Netegrity and HP.

In the meantime, I've got to reschedule my dentist appointment. Seems my dentist is getting insecure about giving me shots. ☹

Mind Reef

www.mindreef.com

Mind Reef

www.mindreef.com

A Strategy for Securing Web Services

A developer's approach to dealing with security standards in a state of flux



Security is not a new concern for companies that want to protect key information and systems from unauthorized access. Protection from such attacks has traditionally been achieved by placing those systems in a tightly controlled intranet accessed through a hardware firewall, possibly over secure TCP/IP connections. However, as more information and functionality are made available over the Web and distributed computing begins to cross corporate Internet boundaries, these mechanisms are no longer adequate. In addition, new concerns arise as a result of distributed computing and transacting business over the Web.

AUTHOR BIO:



Mark Secrist is a senior consultant for the HP Developer Resource Organization with more than 10 years of experience involving distributed object technologies and building n-tier, Web-based applications. He currently consults with enterprise customers on J2EE and Web services development.

MARK_SECRIST@HP.COM

With respect to Web services security, there are five primary areas to consider. *Authentication* is the act of assuring an entity is who it says it is by providing some form of proof. *Authorization* is the process of determining what an authenticated user is entitled to do. *Confidentiality* is a means of guaranteeing that only the intended recipient can view the information being exchanged. *Integrity* is a means of ensuring that information arrives at its intended destination unaltered. Finally, *nonrepudiation* is the ability to trace or log the fact that a document was sent and received so that a recipient can't later claim they never received it or that a sender can't deny they sent the document.

It's important to realize that there are many different ways to apply security to a Web services application. This includes leveraging the existing transport and infrastructure capabilities, as well as modification of the SOAP message itself. Each technique has certain advantages and disadvantages. For example, the use of HTTPS for transmitting SOAP messages between client

and server provides encryption (confidentiality) of the SOAP message with very little programmatic work required by the developer. However, the disadvantage is the performance degradation encountered in encrypting every message that is exchanged, as well as the lack of flexibility in defining what service is permitted to decrypt the message. In the same way, leveraging infrastructure services for authenti-

cation and authorization may mean less work for the programmer but runs the risk of vendor or platform lock-in. On the other hand, applying security to the message itself both provides the greatest flexibility for defining specifically what aspects of security are used and enables a higher degree of interoperability among services operating in a heterogeneous collection of platforms and programming languages.

	XML-Signature	XML Encryption	XKMS	SAML	WS-Security
Authentication					
Authorization					
Confidentiality					
Integrity					
Nonrepudiation					

TABLE 1 | Security standards and the issues they address

Parasoft

www.parasoft.com/ws2

Security Standards for Web Services

Because Web services is fundamentally built on XML for describing and invoking services, it isn't surprising that XML would also play a large role as the medium for communicating security information. There are a number of XML-based standards that are emerging to address the various aspects of security, such as XML-Signature, XML Encryption, Web Services Security (WSS), and SAML. Some of these standards aren't explicitly limited to Web services in their application, but make sense simply because they are XML-based. No one standard completely addresses all of the issues associated with security, although some will address more than one issue. Table 1 will help you relate some of the standards to the security issues they address.

A Web service solution will often combine these technologies to achieve the desired level of security. However, it is important to realize that not all aspects of security will be required for a particular solution. There is almost always a price to pay, whether it is performance, complexity of development and maintenance, or the cost of the solution. As a result, a key guiding principle in applying security is to secure only what must be secured. Think carefully about what aspects of security will be required based on the nature of the service and the environment in which the interaction will take place.

The Strategy

By now, you will have grasped the fact that adding security to Web services can be complex, not only because of the variety of choices available, but also because many of the standards are still evolving. While it's tempting to let this be a barrier to developing Web services or implementing any security, it is important to realize there are strategies that can be used to help reduce complexity and help isolate developers from many of the changes taking place. Here is just one way in which this can be accomplished. Many Web services engines or SOAP servers support the idea of message handlers (sometimes called interceptors). This is the ability to intercept the SOAP message and pass it through a series of processing steps prior to actually delivering the message to the service implementation code. Usually this is an optional step that can

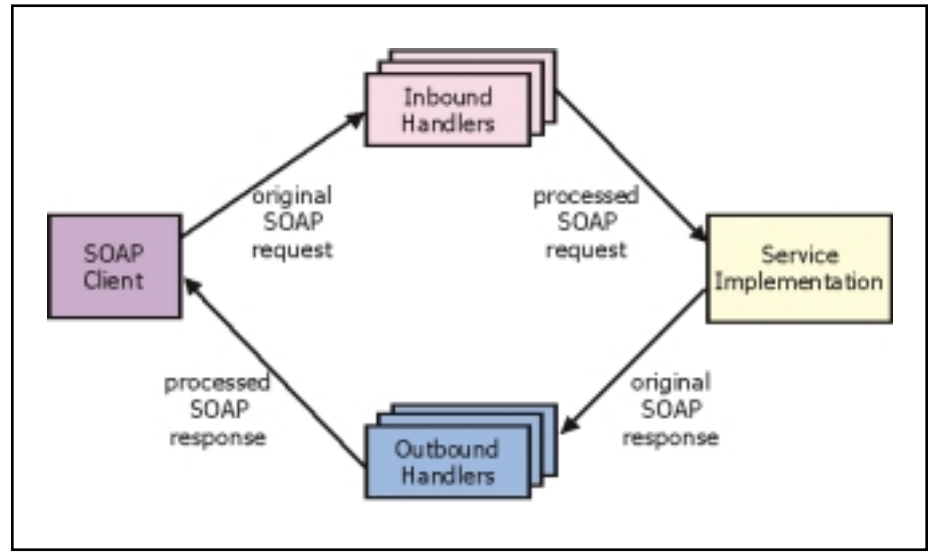


FIGURE 1 | Generic handler architecture

be configured and applied to either individual services or to all services deployed on the server.

As an example, suppose that the credit card number element has been encrypted by the sender and a particular service is the intended recipient. An encryption handler could be written to intercept the message, extract the document in the body of the message, decrypt the credit card number, and reinsert the document back into the SOAP body before passing it on to the implementation. There are several benefits to this approach. First, the actual implementation is not encumbered by the task of having to decrypt the element, providing a degree of isolation of tasks. Second, the message handler can be used to wrap potentially unstable APIs or custom functionality in a way that allows later change to the security elements without directly affecting the actual service or client functionality. Figure 1 illustrates the generic handler architecture.

Figure 1 describes in generic terms how the handler mechanism works. Typically, some number of request handlers and response handlers (described in the figure as inbound and outbound handlers) can be registered with the SOAP engine. In addition to defining what handlers will be used, an order of invocation can also be defined. The developer can create a handler for inserting and extracting a specific type of security element, such as XML Encryption or XML-Signatures. Most platforms allow the ability to define and register handlers for the SOAP

server. Some platforms, such as Apache Axis, also allow for the ability to define client-side handlers for processing the SOAP request prior to transmitting the request to the service and following receipt of the response from the service.

Now that we've talked about handlers in the generic sense, let's look at a specific example of using client- and server-side handlers to digitally sign and validate a SOAP message with Apache Axis. Consider a situation where a client will be submitting a list of parts for which it wishes a supplier (Acme Supplier) to provide a quote on price and availability. In order for Acme Supplier to be willing to provide a quote, it needs to validate that the request indeed originated from the claimed client. This is done by having the client digitally sign the SOAP message and the Acme Supplier service verify the signature before passing the request on to the actual service implementation. In order to enable this capability, we will create a `ClientRequest SigningHandler` class to sign the document and a `ServerRequest SigningHandler` class to intercept the request and validate the signature. Figure 2 shows the Axis-specific architecture for the example we've just outlined.

Apache Axis provides an abstract basic handler (`org.apache.axis.BasicHandler`) that can be used to get started. In this case it is only required to implement the `invoke()` method to define the specific behavior you want to provide. In this case, the implementation for the `ClientRequest SigningHandler` might look something like Listing 1. The

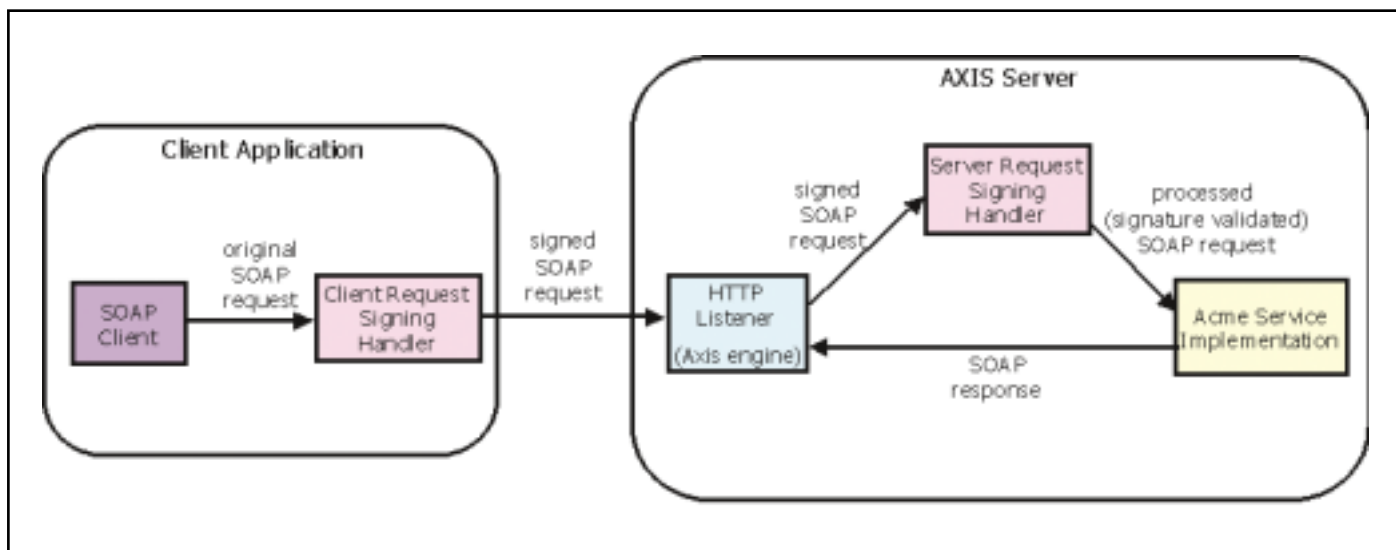


FIGURE 2 | Axis-specific architecture

details of actually signing the document have been left out here to illustrate just the approach. For a more complete example, please see the entire source code (the source code may be found on the Web at www.sys-con.com/webservices/sourcecode.cfm). In order for the client to actually make use of this handler, it must first create and register the handler (see Listing 2).

Finally, Listing 3 is an example implementation of the ServerRequestSigningHandler that will extract and validate the signature before allowing the request to be passed to the implementation.

In order for the Axis server to be aware of and pass the request to the server side request handler, it must be registered as well. This can be done programmatically, but a better way is to include this with the registration of the service itself in the Axis Web Service Deployment Descriptor (WS DD). Listing 4 is an example of the WSDD file that would register the service and a single handler for processing the digital signature.

From this example, you can see that using message handlers is one way to implement

security in a Web services architecture with minimal impact to the service and client implementation itself. This approach can be used to isolate the developer from changes that may occur in the security standards and APIs. In addition, it enables a high degree of flexibility in implementing the various aspects of security.

Conclusion

In this article, I've shown an example of using the message handler technique to hide implementation specifics for digitally signing and validating a SOAP message. This technique can also be used to provide XML encryption capabilities, adding WSS elements to a SOAP header, adding SAML assertions and validating them, and so forth. With this technique, it is possible to use multiple handlers to add various security capabilities. For example, one pair of handlers could be used to encrypt and decrypt certain elements of a document while another pair could be used to sign and validate the document.

While many of the security standards

are still emerging and stabilizing, it is important to begin thinking about how to secure your Web services. The first step is to be aware of the different aspects of security and the various standards that can be used to secure Web services. The second step is to know the state of these standards so as to not choose technologies that introduce great risk into the solution. The third step is to define a strategy and an architecture for implementing security in a way that provides the greatest amount of isolation from the changes that will most certainly continue to take place throughout this year.

References

- Hirsch, Frederick. *Getting Started with XML Security*. (<http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html>)
- Eastlake, Donald E., III; Niles, Kitty (2002). *Secure XML, The New Syntax for Signatures and Encryption* (Addison-Wesley).
- *Apache Axis SOAP Toolkit*: <http://xml.apache.org/axis> ©

Listing 1: ClientRequestSigningHandler

```

public class ClientRequestSigningHandler extends
BasicHandler {
    static {
        // Initialize the xml-security library
        org.apache.xml.security.Init.init();
    }

    public void invoke(MessageContext msgContext) throws

```

```

AxisFault {
    try {
        msgContext.getService();
        Message requestMessage =
msgContext.getRequestMessage();
        SOAPEnvelope unsignedEnvelope =
requestMessage.getSOAPEnvelope();
        SOAPEnvelope signedEnvelope =
signTheEnvelope(msgContext,unsignedEnvelope);
        requestMessage = new Message(signedEnvelope);
    }
}

```

```
msgContext.setCurrentMessage(requestMessage);
    } catch (Exception e) {
        e.printStackTrace();
        throw
AxisFault.makeFault(e);
    }
}
```

Listing 2: SupplierServiceClient

```
String endpointURL = "http://localhost:8080/axis/services/AcmeSupplier";
// Set up the call to the service
Service service = new Service();
Call call = (Call)
service.createCall();
call.setTargetEndpointAddress(new
URL(endpointURL));
SOAPBodyElement[] reqSOAPBodyElements
= new SOAPBodyElement[1];
// Fill out the SOAP body here

// Create and set the client request
handler
ClientRequestSigningHandler
clientReqHandler =
        new
ClientRequestSigningHandler();
clientReqHandler.setOption("key-
store", "acmekeystore.jks");
call.setClientHandlers(clientReqHandler, null);
// Invoke the service
Vector resSOAPBodyElements =
        (Vector)
call.invoke(reqSOAPBodyElements);
```

Listing 3: ServerRequestSigningHandler

```
public class
ServerRequestSigningHandler extends
BasicHandler {
    static {

org.apache.xml.security.Init.init();
    }

    public void invoke(MessageContext
msgContext) throws AxisFault {
        try {
            Message inMsg =
msgContext.getRequestMessage();
            Message outMsg =
msgContext.getResponseMessage();

            // verify signed message
            Document doc =
inMsg.getSOAPEnvelope().getAsDocument();
            CachedXPathAPI xpathAPI =
new CachedXPathAPI();
            Element nsctx =
doc.createElement("nsctx");

nsctx.setAttribute("xmlns:ds",
Constants.SignatureSpecNS);
```

```
Element signatureElem =
        (Element)
xpathAPI.selectSingleNode(doc, "//ds:Signature", nsctx);

XMLSignature sig =
        new
XMLSignature(signatureElem, "http://acmesupplier.com");

boolean valid =

sig.checkSignatureValue(sig.getKeyInfo()
().getPublicKey());

        if (! valid) {
            System.out.println("The
signature is invalid");
            throw
AxisFault.makeFault(new
Exception("Validation Failed"));
        }
        System.out.println("Signature
validation succeeded");
    } catch (Exception e) {
        System.out.println("Exception
caught: " + e);
        throw
AxisFault.makeFault(e);
    }
}
```

Listing 4: Axis server deployment file

```
<deployment

xmlns="http://xml.apache.org/axis/wsdd/"

xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">

    <!-- Define the Signature Handler
for the request -->
    <handler name="requestHandler"
type="ServerRequestSigningHandler">
        <parameter name="filename"
value="MyService.log"/>
    </handler>

    <!-- Services from SupplierService
WSDL service -->
    <service name="AcmeSupplier"
provider="java:RPC" style="document">
        <operation name="getQuote"
qname="operNS:QuoteRequest" />
        <parameter name="allowedMethods"
value="getQuote"/>

        <requestFlow>
            <handler
type="requestHandler"/>
        </requestFlow>
    </service>
</deployment>
```

Download the code at

sys-con.com/webservices

WebServices JOURNAL

PRESIDENT AND CEO

Fuat A. Kircaali fuat@sys-con.com

COO/CFO

Mark Harabedian mark@sys-con.com

VP, BUSINESS DEVELOPMENT

Grisha Davida grisha@sys-con.com

ADVERTISING

SENIOR VP, SALES & MARKETING

Carmen Gonzalez carmen@sys-con.com

VP, SALES & MARKETING

Miles Silverman miles@sys-con.com

ADVERTISING DIRECTOR

Robyn Forma robyn@sys-con.com

ADVERTISING ACCOUNT MANAGER

Megan Ring-Mussa megan@sys-con.com

ASSOCIATE SALES MANAGERS

Carrie Gebert carrie@sys-con.com

Alisa Catalano alisa@sys-con.com

Kristin Kuhnle kristin@sys-con.com

SYS-CON EVENTS

PRESIDENT, SYS-CON EVENTS

Grisha Davida grisha@sys-con.com

CONFERENCE MANAGER

Michael Lynch mike@sys-con.com

CUSTOMER RELATIONS/JDJ STORE

CUSTOMER SERVICE REPRESENTATIVE

Margie Downs margie@sys-con.com

JDJ STORE MANAGER

Rachel McGouran rachel@sys-con.com

SYS-CON.COM

VP, INFORMATION SYSTEMS

Robert Diamond robert@sys-con.com

WEB DESIGNERS

Stephen Klimmurray stephen@sys-con.com

Christopher Croce chris@sys-con.com

ONLINE EDITOR

Lin Goetz lin@sys-con.com

ACCOUNTING

FINANCIAL ANALYST

Joan LaRose joan@sys-con.com

ACCOUNTS RECEIVABLE

Kerri Von Achen kerri@sys-con.com

ACCOUNTS PAYABLE

Betty White betty@sys-con.com

SUBSCRIPTIONS

SUBSCRIBE@SYS-CON.COM

1-888-303-5282

FOR SUBSCRIPTIONS AND REQUESTS FOR BULK ORDERS,

PLEASE SEND YOUR LETTERS TO SUBSCRIPTION DEPARTMENT

COVER PRICE: \$6.99/ISSUE

DOMESTIC: \$69.99/YR (12 ISSUES)

CANADA/MEXICO: \$89.99/YR

ALL OTHER COUNTRIES: \$99.99/YR

(U.S. BANKS OR MONEY ORDERS)



Global Knowledge

www.globalknowledge.com



Reviewed by Joseph A. Mitchko

Quadrasis/Xtradyne SOAP Content Inspector

Providing comprehensive solutions for Web service security

They carefully planned for days for the worst possible attack. Once their presence was detected, the enemy's agents, who were stealthy and highly intelligent, would surely be drawn to their defensive walls. It would only be a matter of time before the ongoing and relentless probing would begin, eventually finding some unknown and unforeseen weakness in its design. Once compromised, the walls would surely be breached and the eventual plundering and destruction would spell doom for the innocent inhabitants within. Instinctively they knew not to underestimate the dark and ever-present forces residing in the ether.

This may sound like a scene from the latest *Lord of the Rings* movie. Actually, it depicts an everyday event for Internet service providers – bringing new servers online. In many cases, it only takes a few minutes for the firewall probing to start when a new Web server is indoctrinated to the Internet.

This is the world that global Web services must exist in, and it does not paint a pretty picture. Luckily, standards are emerging to address the numerous issues regarding Web service security (WS-Security, SAML) and new products to implement them. Quadrasis SOAP Content Inspector is one such product to tackle the tough Web service security issues of today.

Overview

The Quadrasis/Xtradyne SOAP Content Inspector (SCI) provides a flexible and comprehensive set of solutions for protecting Web service resources both inside and outside the corporate firewall. It comprises three main components which, depending on in-

stallation, can reside on a single server or on separate boxes. The SCI Policy Server manages the various security policies and basically makes all decisions regarding access to resources. The SCI Proxy Server intercepts SOAP requests and, depending on decisions made by the Policy Server, passes the request to the protected Web service or denies access to the service. The final component, the SCI Administration Console, allows you to maintain user names and user groups exercise role-based access control to Web service resources, configure message encryption techniques, and set up event monitoring (see Figure 1).

Regarding user stores, you can either use a built-in database for user information or configure SCI to retrieve user information from a directory server (using LDAP). SCI is compatible with several of the leading directory service products including Netscape (iPlanet).

If your security design involves processing SAML assertions with attribute data (i.e., from an LDAP server), you'll need to install an additional product from Quadrasis. I'll have more on that later.

4A Functionality

The functionality provided by SOAP Content Inspector can be summarized in four basic functional categories – authentication, authorization, auditing, and administration. Authentication limits access to only those clients that can be certified by several mechanisms including SSL Client certificate, basic HTTP authentication, SAML assertions, or anonymous public access. Basically, you better be who you claim to be or you cannot use the Web service resource.

Authorization will restrict access to an authenticated SOAP client to only the Web service resources spelled out by the policy information stored on the Policy Server. The



About the Author:

Joe Mitchko is a technology specialist working for a leading Internet service company and is product review editor and contributing writer for Web Services Journal magazine.
JMITCHKO@RCN.COM



COMPANY INFO

Quadrasis, the security division of Hitachi Computer Products (America), Inc.
Software Solutions Division
1601 Trapelo Road
Reservoir Place, 3rd Floor
Waltham, MA 02451
Phone: (781) 890-0444
Facsimile: (781) 890-4998
Web: www.quadrasis.com
E-mail: solutions@quadrasis.com

EVALUATION DOWNLOAD

www.quadrasis.com/prod_download/register.asp

LICENSING INFORMATION

Licensing is on a CPU basis with up to 50 simultaneous connections.

http://www.quadrasis.com/prod_download/register.asp

TESTING ENVIRONMENT

OS: Windows-2000 Professional
Hardware: IBM ThinkPad T30



SCI policy can authorize access down to the SOAP RPC method level and manages access control lists for user and user groups levels.

For SCI auditing capabilities, SOAP Content Inspector can log a number of events, including connection establishment, authentication, and authorization results. You have the option of logging to a flat file or to the Windows 2000 event log service.

The last of the 4A feature list, administration, represents the GUI-based SCI Admin Console provided with SOAP Content Inspector. The console has two views, professional and expert. The professional view is where you would spend most of your time when setting up your policies and other configuration settings. It sets things up logically according to functionality. The expert view, on the other hand, is essentially one large hierarchically arranged property sheet for the system. You go there only if you need to tweak something that is not normally handled by the professional view. I found the Admin Console

fairly straightforward and easy to use. SOAP Content Inspector keeps security arrangements at a single policy level and does not include higher levels of abstraction, such as domains and realms, as found in other security policy services. This tends to make configuring and administering security policies easier to set up.

One last set of features, not really part of the 4A feature list, involves message integrity and validation. SOAP Content Inspector is able to detect ill-formed messages by validating the XML inside the SOAP message. It also has the capability of digitally signing the SOAP header and message blocks as a whole, making modification impossible without detection.

Architecture

One of the more interesting features of the SOAP Content Inspector is its flexibility in handling SAML (Security Assertion Markup Language) assertions, one of the emerging standards in Web services today. An *assertion*

essentially provides a mechanism for security information to be passed around from one party to another. A SOAP message containing a SAML assertion (or contained in the SOAP header) can provide authentication and authorization information that has been populated ahead of time by some authentication service. The assertion thereby contains proof of the message's authenticity as well as information regarding which Web service resources are authorized for access.

SCI can be set up as a proxy for the Web service, authenticate the client (user) of the message, create and append a SAML assertion to the message, and forward the message to the real Web service application. With the SAML assertion firmly attached to the SOAP message (or SOAP header), it can be forwarded to other nested Web services providing a single sign-on mechanism.

In another mode of operation called a Federated Trust, SOAP Content Inspector can be configured on both the client and service sides of the Web service, acting in a sense as a dual proxy (see Figure 2). The client will forward the SOAP message to the client-side proxy, provide the necessary authentication, and attach a SAML assertion to the message. The message is then delivered to the server-side proxy, where the SAML Assertion is processed. If authorized to use the Web service, the validated SAML assertion is retained in the SOAP message and the request is forwarded to the true Web application. The assertion processing occurs under the covers and provides a transparent and

secure means for SOAP messages to be delivered over the Internet.

Another strength of the SOAP Content Inspector is in its ability to inject attribute information (user e-mail addresses, business addresses, etc.) into SAML assertions. It is currently the only product on the market with this level of functionality. In order for SOAP Content Inspector to do this, you must install and configure EASI Security Unifier, which requires a separate product installation (and licensing) from Quadrasis. With attributes embedded in the SAML assertion, a Web service will not only be guaranteed that the client is authenticated and authorized to use the service, but will have relevant and current user information available for processing. This saves the Web service from having to make separate trips to an LDAP server and from requiring separate LDAP connect, bind, and search configuration settings.

Installation

As of this writing, SOAP Content Inspector is only available for installation on Windows 2000, so you better put on your Microsoft administrator's hat. To start off, prior to installation you'll need to download and install the Java 1.3 Runtime Environment (or greater) and several security-related libraries (JSSE, JCE). Check the installation (startup) guide for details. Although Java 1.4 comes bundled with the security class libraries, you still need to separately download and install each security package until version 1.4 is certified by Quadrasis.

Documentation

SOAP Content Inspector comes with several well-written guides to help you configure and secure your Web services. I found the Administrator's Guide to be extremely useful, taking you step-by-step through setting up the system and establishing a base set of policies.

Conclusion

Installing and configuring secure Web services is straightforward using Quadrasis SOAP Content Inspector. Its policy management is somewhat less complex to configure compared to other security management products, and can essentially run straight out of the box allowing you to get acquainted with security policies first instead of configuring external systems such as database and directory services. ©

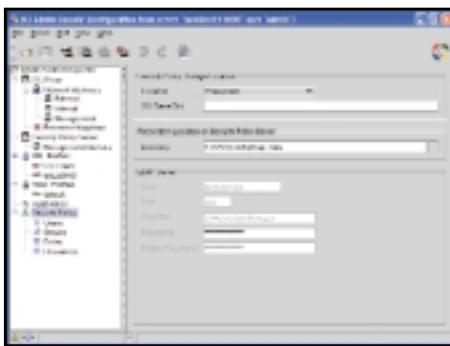


FIGURE 1 | The SCI Admin Console

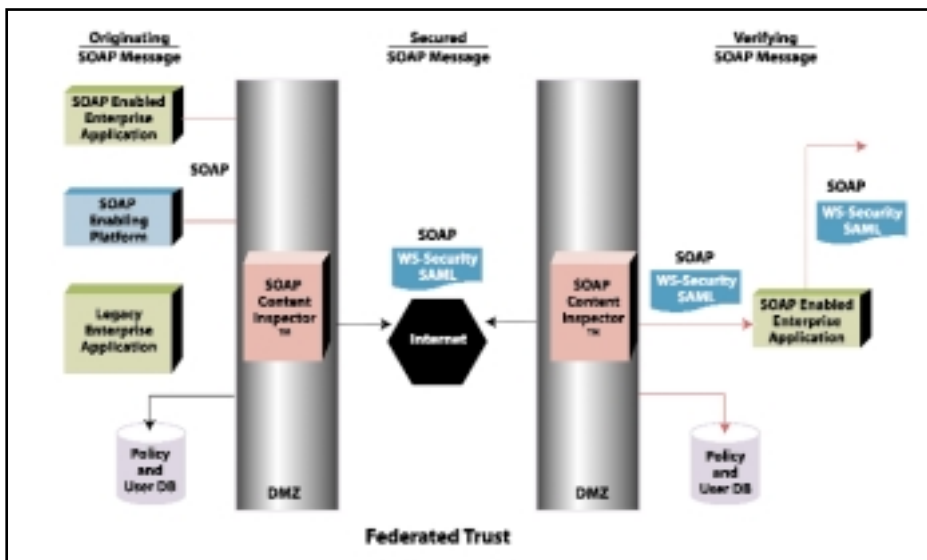


FIGURE 2 | SOAP Content Inspector used as a Federated Trust

A New World of Web Services Security

Using open B2B process integration platforms as a testing ground

Recently there have been a number of exciting developments in the area of Web services security standards (SAML, WS-Security, XACML, etc.). However, unless you are a security expert and closely involved in these standards, it is difficult to sort through the alphabet soup and understand what each standard is about. Do the standards address the same or different problems? How do they interact?

This article seeks to clear up some of this confusion by illustrating how the various security standards could be applied to address the security needs of a particular business problem, in our case an open B2B process integration platform that enables collaborative e-business and supply chain capabilities. Yet we must note that these new security standards are applicable to any distributed computing environment, from a multidivision secure intranet portal to a group of public Web sites that want to share user identity and access data.



AUTHOR BIO:

Gilbert Pilz has more than 18 years of software development experience and extensive experience in distributed systems security. As

E2open's chief security architect, he oversees the architecture and implementation of E2open's application security services as well as the user and business partner registration infrastructure that underpins these services.
GPILZ@E2OPEN.COM

Business Problem Overview

The convergence of hosted outsourcing and B2B process integration has created a new space for computing services – the open B2B process integration platform. Typical hosting solutions provide a shared infrastructure and amortize that cost across their customer base. B2B process integration typically consists of numerous point-to-point connections that provide increased transactional speed and efficiency with trading partners. An open B2B process integration platform, by comparison, provides a shared infrastructure that captures the benefits of both outsourcing and integration at a significant cost savings. Each organization has to create only one B2B connection to the shared platform. Data pushed across the platform can be transformed and securely routed to any other connected organization. As you will see, there are many areas in which the shared B2B model is exponentially less expensive to create and maintain and more efficient than a point-to-point model.

As Figure 1 illustrates, the platform must

support a mix of server-to-server and user-to-application interactions. The flexible, lightweight nature of Web services makes them ideal for an open B2B process integration platform. The consumers of the platform, the individual Trading Partners, can integrate their existing systems with the platform without the need for complicated and expensive integration engines. The ability to describe services in WSDL and register these descriptions in the central, UDDI-based directory, decreases the cost of service deployment and eases service adoption.

Throughout this article, I refer to the following business challenge, typical in a B2B integration application, to illustrate our discussion:

Trading Partner A submits a purchase order to Trading Partner B via the platform using SOAP messaging. Because some of the information within the purchase order is sensitive (part numbers, quantities, etc.) a portion of the message that carries the purchase order must be encrypted with the public key of Trading Partner B. For purposes of authentication and nonrepudiation, the entire purchase order must be signed with the private key of Trading Partner A.

Security Requirements

The key problem for such an application is security. Our platform must meet the following



high-level security requirements:

- **Message integrity and confidentiality:** Provide end-to-end message integrity and confidentiality. This applies to conversations between Trading Partners and the platform (where the platform makes up one end of the conversation) as well as conversations between Trading Partners (in which the platform acts as an intermediary).
- **Authentication:** Mutually authenticate all participants in the system (users and servers).
- **Authorization:** Restrict participants to the services and data that they are allowed to access.

- **Provisioning:** Add and remove Trading Partners and their users to and from the platform quickly and with a minimum of human involvement.

These high-level requirements in turn drive a number of lower-level requirements such as the need for an integrated directory and public-key repository.

Current Solutions

The current state of practice for addressing our high-level requirements is:

- SSL provides confidentiality (and by inference, integrity) to messages as they travel

SSL-enabled connections. SSL is also used to authenticate server entities.

- Users are authenticated via username/password combinations against a central user repository.
- Authorization is provided via some form of Web access control tool that restricts access based upon URLs, typically managed by products such as IBM Tivoli Access Manager or Netegrity SiteMinder.
- Provisioning Trading Partners and their users is currently handled via custom tools or proprietary directory-integration technologies, such as IBM Tivoli Identity Manager or Novell DirXML.

While these solutions were successful at addressing the security issues of previous business models, they fail to address the needs of a shared B2B process integration platform in a number of areas.

1. **SSL is a transport-level entity:** As such, it cannot be used to protect messages outside the context of a particular transport-level session. SSL also cannot be used to prove the identity of participants (clients or servers) outside the context of a particular transport session. Lastly, since SSL authentication is not valid beyond the life span of the connection, SSL cannot be leveraged to support nonrepudiation.
2. **Username/password authentication** It is cumbersome and fragile. Forgotten passwords are the number one source of help desk calls. Weak passwords are the primary source of security breaches.

Recent advances in Web services security overcome these problems and help us meet the four key security requirements we outlined above.

Message Integrity and Confidentiality

The first core security requirement of a shared B2B integration platform is end-to-end message integrity and confidentiality. New protocols and technologies have emerged to address this challenge.

XML-Signature and XML Encryption

Together, the XML-Signature (www.w3.org/Signature) and XML Encryption (www.w3.org/Encryption/2001) specifications – both W3C Recommendations – form the basic building blocks of Web services security.

These specifications relate to signing, veri-

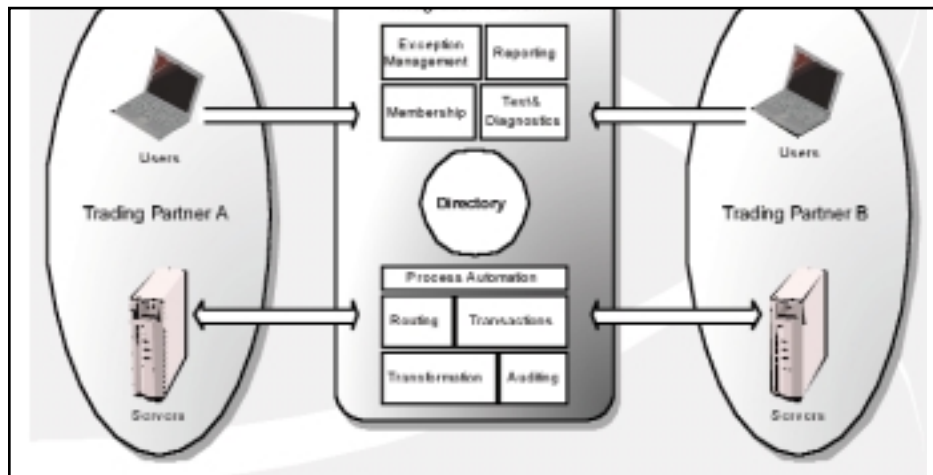


FIGURE 1 | The shared B2B process integration platform

fying, encrypting, and decrypting XML messages. Note that these standards don't define any new cipher suites or signature mechanisms. They apply existing encryption and signature algorithms to XML and capture the results of those algorithms in XML syntax. This last point is important. By working within XML, the XML signature and encryption standards make the results of their operations consumable by XML-aware components. This allows solutions built using XML to add encryption and signature support without having to significantly alter their technology base. This feature is used by the Web Services Security specification to add message integrity and confidentiality to SOAP without having to make changes to the SOAP specification.

In our example, the client side of the purchase order service would use XML Encryption to encrypt the sensitive arguments of the purchase order. The encryption is performed at the business logic level because only the business logic knows which arguments are considered sensitive. The mechanism for signing the purchase order is described below.

Web Services Security

In April of 2002, IBM, Microsoft, and VeriSign jointly published the WS-Security document (www.verisign.com/wss/wss.pdf). This document is part of a larger Web services security architecture detailed in a joint white paper from IBM and Microsoft entitled "Security in a Web Services World: A Proposed Architecture and Roadmap" (www.verisign.com/wss/architectureRoadmap.pdf). The WS-Security specification was accepted as a starting point for specifications being drafted by the OASIS Web Services Security Technical Committee (www.oasis-open.org/committees/wss/#documents).

Like the WS-Security document, the OASIS Web Services Security specifications are about message-level security. Specifically, they define how to use the XML Signature and XML Encryption specifications to add integrity and confidentiality to SOAP v1.2 messages. They also include support for message-level authentication through the various types of security tokens (X.509, Kerberos, SAML, etc.).

Returning to our example, after encrypting a portion of the purchase order document, the purchase order client code invokes the SOAP messaging engine for the purchase order service. Because the purchase order service requires that all messages submitted to the service be signed

with the private key of the sender, our SOAP messaging engine transparently invokes the WSS-compliant signing service before transmitting the message. This results in a SOAP message with WSS-defined security headers that contain the digital signature value for the SOAP body along with the X.509 certificate for Trading Partner A. When this message reaches Trading Partner B, the signature can be verified and the identity of the issuer (A) is authenticated (provided the recipient [B] trusts the entity that signed the included X.509 certificate). In addition, the individual SOAP message containing the purchase order, signature, and certificate elements could be archived to a database for purposes of nonrepudiation.

What's Missing?

Our example seems straightforward, but there are a number of unanswered questions. How does Trading Partner A know that the purchase order service requires signing the SOAP message body? How does Trading Partner A know what signature mechanisms are supported?

Trading Partner A could dynamically discover the answers via service descriptions located in a directory (such as extended WSDL entries in UDDI), or could invoke another Web service to negotiate these details. OASIS is currently considering forming a new technical committee to address some of these issues. The recently published WS-Policy (www.verisign.com/wss/WS-Policy.pdf) and WS-Trust (www.verisign.com/wss/WS-Policy.pdf) papers also address this topic.

For the foreseeable future, however, it is likely that most of these issues will be solved via configuration. This is where using a platform is crucial. Each Trading Partner needs to configure and maintain only one set of these parameters to communicate with all the other Trading Partners on the platform. Contrast this with the overhead of settling each of these issues on a per-Trading Partner basis.

Authentication

The second core security requirement of our shared B2B process integration platform is to mutually authenticate all participants in the system. This requirement breaks down into two lower-level requirements – authenticating users and authenticating servers.

Until now our discussion has centered on

the security needs of server-to-server communications. A B2B process integration platform also provides access to applications; users must be authenticated to these apps. Authenticating users against an internal LDAP store with a username/password combination is a tried-and-true method for handling this problem. But ideally we would like the Trading Partners' users to authenticate within their own security domain, then use single sign-on (SSO) to access the applications within the platform. Security Assertion Markup Language (SAML) allows us to do this.

SAML

Accepted as an OASIS committee specification in May of 2002, SAML (www.oasis-open.org/committees/security/#documents) allows our platform to configure trust relationships between itself and the Trading Partners such that the users of those Trading Partners can automatically authenticate with our platform. Once more the network effect is evident, as it is much easier for each Trading Partner to maintain a single SAML trust relationship between itself and the platform than with each individual Trading Partner.

The SAML specification defines two browser-oriented single sign-on profiles. These profiles specify how SAML can be used to provide SSO for Web browser-based applications. Nonbrowser-based applications that use SOAP (or SAML-aware server systems) can take advantage of the fact that the WSS specification supports the use of SAML Assertions as WSS "Security Tokens." This allows consumers of WSS-protected services to leverage their SAML infrastructure to provide message-level authentication for those services.

If SAML allows users to authenticate with the platform, how does the platform authenticate with the user? For this we may rely on SSL. Despite the shortcomings outlined earlier, SSL works well at authenticating servers to users.

XKMS

In my discussion of message integrity and confidentiality I made passing references to X.509 certificates. To be explicit, server entities that interact with the platform authenticate themselves using X.509 certificates. This raises a number of questions: Who issues these certificates? For how long are they valid? What are the revocation policies?

The answer to these questions, in the case of our example, lies in the capabilities of the B2B process integration platform. The plat-

form acts as an intermediate certificate authority, creating, storing, and revoking certificates as needed. The interface to all these platform services is specified by XKMS.

The XML Key Management Specification (XKMS 2.0: www.w3.org/TR/xkms2) is a W3C Working Draft. It is made up of two parts – the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS)

The X-KISS specification defines a protocol for resolving public key information contained in XML Signature and XML Encryption elements. Referring again to our example, Trading Partner B would use the X-KISS protocol to determine whether the certificate in the SOAP message it received from Trading Partner A (via the platform) was valid.

The X-KRSS specification defines a protocol that accepts registration of public key information. Once registered, the public key may be used in conjunction with other Web services including X-KISS. The use of X-KRSS greatly simplifies one of the steps in the server-to-platform provisioning process, discussed later.

Authorization

The third core security requirement for our shared B2B process integration platform is to restrict participants to the services and data that they are allowed to access. To understand how Web services security standards apply to this requirement, you must understand something about the authorization architecture of the platform. Individual components of the platform enforce authorization according to semantics particular to each component. These Policy Enforcement Points (PEPs, to use terminology defined in the “Generic AAA Architecture” - RFC 2903) use a central Policy Decision Point (PDP) to determine if a given user or server should be allowed to perform a specific action on a particular resource. The PDP’s decisions are driven by policies stored in a policy repository.

Another SAML Application

The SAML specification defines the request/response protocol used to communicate between the PEPs and the PDP (termed “Authorization Authority” by SAML) as well as the Authorization Decision Assertions that are returned by this protocol. To make its decision, the Authorization Authority frequently needs

information about the attributes of the requesting user or server, for which it uses another SAML-defined protocol to request Attribute Assertions from one or more Attribute Authorities. Consider this example:

Claude, a user of Trading Partner A, uses single sign-on to access the platform and launch the report generation application. While in the application, Claude attempts to generate a transaction report for the last 30 days.

The report generation application needs to determine if Claude is allowed to read the information necessary to generate the report. It requests an Authorization Decision Assertion from the central Authorization Authority, passing as parameters Claude’s Authentication Assertion, the name the resource needed to generate the report, and the action Claude is attempting to perform on that resource (i.e., “read”). To make this decision the Authorization Authority accesses the repository to determine the security policies applicable to the requested resource. These policies indicate that Claude’s role is a factor in this decision. To obtain information about what roles Claude is allowed to perform the Authorization Authority contacts the Attribute Authority for Trading Partner A and requests the Attribute Assertions that describe the roles assigned to Claude. With this information the Authorization Authority is capable of determining that Claude is allowed read access to the requested resource and indicates this fact in the Authorization Decision Assertion it returns to the application.

Provisioning

The fourth core security requirement is to add and remove Trading Partners and their users to and from the platform quickly and with a minimum of human involvement. Normally provisioning and deprovisioning are not thought of as security requirements but these activities are, in fact, central to the platform’s overall security fabric.

Referring back to our original example of Trading Partner A sending a (partially) encrypted and digitally signed purchase order to Trading Partner B, although XKMS/X-KRSS handles the certificate creation and registration tasks of provisioning Trading Partner A’s server, the following tasks still need to be performed before our example can be executed:


1. “Bootstrap” provisioning to allow A’s server to consume the XKMS/X-KRSS services.
2. Grant A’s server the authority to look up the certificate for B’s server using XKMS/X-KISS.
3. Subscribe A’s server to the SOAP endpoint that accepts purchase order messages.
4. Subscribe A’s server to the service that routes purchase orders to Trading Partner B.

All of these tasks need to be performed as a single atomic transaction as a result of subscribing A’s server to a particular business process.

Current practices for managing provisioning are often manually intensive, and thus expensive and error-prone. Ideally what we would like to be able to do is integrate the provisioning infrastructures of the Trading Partner’s with that of the platform. Administrators within the Trading Partners’ domains should be able to provision end users and servers for platform services as if they were provisioning them for internal services. The Trading Partners’ provisioning engine then calls a platform service to carry out this request. This sort of integration is made possible via the Service Provision Markup Language (SP ML: www.oasis-open.org/committees/provision/#documents) an OASIS working draft.

If provisioning is a security requirement, then deprovisioning is even more so. Stale accounts and access privileges that are never removed provide fertile ground for security breaches. However, integrating the customers’ provisioning and directory integration engines with the platform offers the added benefit of making sure that the Trading Partners clean up platform accounts when deprovisioning their users and servers.

Conclusion

The changing needs of the enterprise IT marketplace are driving the adoption of new infrastructure models that include the use of Web services as a common integration fabric. These new models have surpassed the capabilities of currently deployed security technologies and practices. Recent developments in Web services security standards promise to address many of these shortcomings, and open B2B process integration platforms have emerged as an early testing ground for these security challenges. 

We Know Web Services Need Security, but What Type?

Exciting but not "dangerous" technologies



It's well known that Web services need security. It's also a truism that lack of security is the barrier to the adoption of Web services. Let's dig a little deeper: What is it about Web services that provoke the security concerns? What is being done to answer the challenge? By answering these questions, this article attempts to dispel some of the confusion around Web services security.

AUTHOR BIO:



Mark O'Neill is CTO of Vordel, which produces the VordelSecure suite for Web services security. Mark is the author of *Web Services Security* (McGraw-Hill Osborne Media, 2003) and is an advisor to the XML.org industry newsletter.

MARK.ONEILL@VORDEL.COM

First, let's take a step back and focus on what security actually is. For some, security is linked to identity – a system is "secure" if the identities of all users are known and intruders are blocked. For others, security is synonymous with cryptography – for them, a "secure" document means an encrypted and/or digitally signed document. Finally, the battery of attacks on Web servers in the past few years has given rise to a third meaning of security – a system is "secure" if it is locked down against buffer-overflow attacks, denial-of-service attacks, and application-level attacks exploiting known vulnerabilities in server software.

Fortunately, the information security industry has codified these various meanings. I'll look at these in turn, beginning with access control.

3A Security: "Who's Running My Web Service?"

The Access Control theory defines the functions of "3A" security – authentication, authorization, and audit. The difference between authentication and authorization is important. Authentication is "who you are" while authorization is "what you are permitted to access." It's surprising how often a system is touted as allowing "authenticated

access," because authentication alone is rarely enough – it has to be linked to access control rules for authorization. 3A security is widely used for access to company extranets for high-value consumer services such as home banking.

3A has been successful for controlling access to Web sites. It seems obvious that it should be useful for Web services also, even for Web services that do not use HTTP. It turns out that it is indeed obvious that 3A security should be used for Web services, but implementing it isn't as easy as it might seem. The problem is that first "A", authentication. Let's look at how the *security context* differs between Web site access and Web services access.

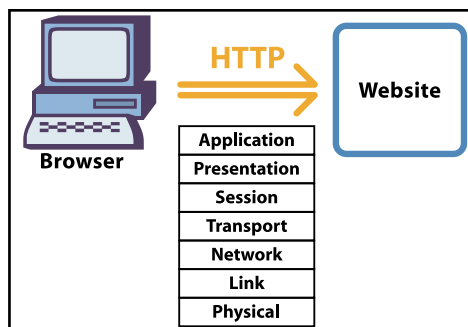


FIGURE 1 Security context for browser access to a Web site

When a Web site receives an HTTP request from a user, it has a direct connection to that user. The user's browser is at the other end of an SSL session, over which they can authenticate using a password or a client certificate. The security context is relatively simple (see Figure 1).

The well-known OSI stack applies for the connection between the user's Web browser and the Web site. Security can be applied at various levels of the stack – and TLS/SSL applies at the transport layer, as the name implies (Transport Layer Security).

Now think about how Web services enlarge the security context. Let's say that the user in Figure 1 authenticates to a Web site, and then submits a Web form that runs a Web service in order to retrieve information *on that user's behalf* (see Figure 2).

In Figure 2, things get more complicated. The OSI stack applies for both communications. However, if access to the Web service is to be based on authentication of the end user, then we have a problem, since the OSI stack only applies for each "hop" of the full transaction. Let's look at another example of multiple security contexts, this time using SOAP routing (see Figure 3).

Sitraka

(Now part of Quest Software)

www.sitraka.com/jclass/ws

Again, in Figure 3 we see that if access to the final Web service depends on the originator of the SOAP request, we have a problem. In addition, the OSI stack for each “hop” may use different communication technologies. This creates a challenge to create a “golden thread” back to the originator of the SOAP request. SOAP is independent of the underlying communication transport, and in any case it is not guaranteed that the same communication transport will be used for the entire life cycle of a SOAP message.

The challenge of implementing 3A security for Web services is being ably met by industry standards bodies including OASIS and the W3C, industry consortia such as Project Liberty, and by Microsoft. Let's look at how SAML addresses the problem we saw back in Figure 2 (see Figure 4).

In Figure 4, the scenario is contextualized into a currency trading situation. If the Web service that is executing the trade relies only on transport security, then it only has visibility of the currency dealing system (which is probably an application server). But what if the Web service must know who the trader actually is? After all, it may be the case that hundreds of traders use the same dealing system, which in turn sends SOAP requests to the trade fulfillment Web service. The answer is that the outgoing SOAP message includes a SAML *authentication assertion*. The information in this assertion indicates that the dealer was authenticated at a certain time, how they authenticated (e.g., by password), how long the authentication is valid for, and a “NameIdentifier” element to indicate the identity of the trader. The “NameIdentifier” may be an e-mail address, a username, or an X.509 common name such as “C=US, O=Acme Banking Inc, OU=Trading, CN=Joe Trader”.

SAML effectively extends 3A security along the security context all the way from the dealer to the Web service, which they ultimately use. Although SAML is not directly used for authentication, it is used to convey information about authentication events that have happened.

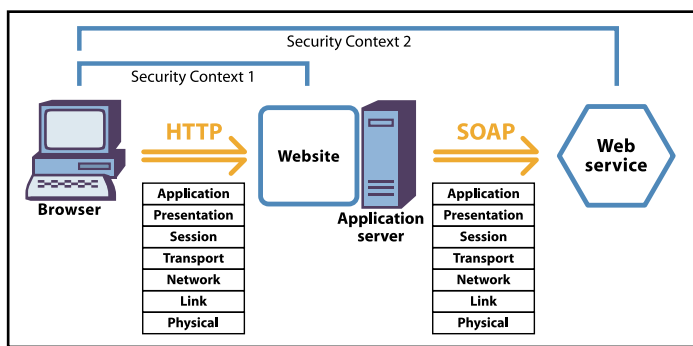


FIGURE 2 | Multiple security contexts

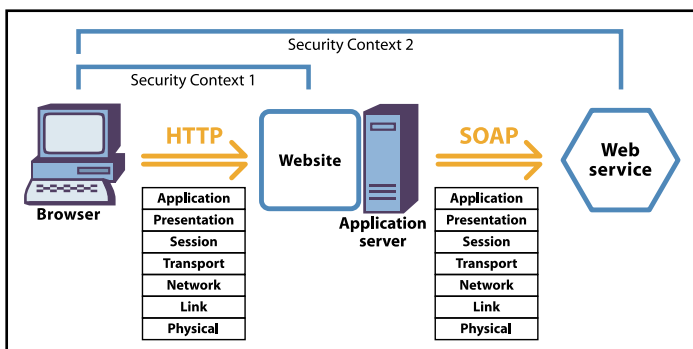


FIGURE 3 | Multiple security contexts because of SOAP routing

As we can see in Figure 4, that's very useful. As well as authentication and authorization assertions, SAML includes attribute assertions that can be used to convey information about the end user – e.g., a credit limit.

In Figure 4, notice that Step 1 is the only sign-on step – i.e., it is a Single Sign-On (SSO) scenario. Other technologies – .NET Passport and Project Liberty – that can also use SAML technology, aim to provide SSO for Web services. Liberty explicitly uses SAML and extends some of the SAML ideas, e.g., to introduce “authentication context” (information about rules governing the authentication act). It makes sense for .NET Passport to use certain portions of SAML – for example, the SAML request/response protocol (called the “SAML Protocol”), which we see in Steps 5 and 6 of Figure 4. Liberty and .NET Passport offer specifications for federated authentication services – a user can authenticate once and this authentication can be valid for multiple services. Passport and Liberty are finding uses in Web site access before Web services access, but the critical mass of Passport users (legions of Hotmail users) and of AOL Instant Messenger (AOL is a member of Project Liberty) means that in 2003, Liberty or Passport authentication should start to be used for Web services.

So far, we haven't seen any disastrous “security holes” in XML or Web services. It's true that the Web services model certainly presents challenges, due to expanding the security context beyond the simple browser-to-Web site model. However, these challenges are being addressed by the industry in specifications such as SAML.

“Confidentiality, Integrity, Nonrepudiation”: Same Old Principles, New SOAPy Environment

Look again at the SOAP routing scenario in Figure 3. Think about the high-level principles of security – confidentiality (ensuring that data in transit cannot be read), integrity (ensuring that undetectable changes cannot be applied to data), and nonrepudiation (to prove the originator sent the data). These principles existed before Web services were invented, and now must be mapped to the Web services model.

Confidentiality can be implemented at each “hop” of the transaction – but what if information sent by the originator must be hidden from the SOAP intermediary but revealed at the destination of the SOAP message? Or what if data must be protected from change by intermediaries while it is en route to the destination Web service? This is where XML-Signature and XML Encryption come into play. XML-Signature may be used to selectively sign a portion of XML data. WS-Security provides a framework for putting XML-Signature data into a SOAP message. Similarly, XML Encryption may be used to selectively encrypt a portion of a SOAP message. And again, WS-Security provides a framework for putting XML Encryption data into a SOAP message. The ability to selectively sign data is important for SOAP, since portions of the SOAP message may be volatile (e.g., routing information in the <head>), and if the entire SOAP message was digitally signed, then the signature would be almost guaranteed to break. Similarly, encrypting an entire SOAP message would be counterproductive.

XML Encryption is used to satisfy the high-level security principle of confidentiality for Web services. XML-Signature is used to satisfy the high-level security principle of integrity. When linked with a digital certificate, XML-Signature can be further used for nonrepudiation – i.e., to prove the identity of the originator of the SOAP message, and to prove the fact that they sent the message.

WS-Security describes not only how to sign and encrypt portions of

a SOAP message, but also how to sign and encrypt security tokens in SOAP messages. These security tokens include X.509 v3 digital certificates, Kerberos tickets, and username/password combinations. These security tokens allow a security context to persist within the message; later specifications such as WS-Trust and WS-Policy build on WS-Security to explain how security tokens may be obtained, or verified, using SOAP. It is convenient to think of WS-Security as a specification that takes XML security, such as XML Signature and XML Encryption; links it with preexisting security technologies, such as X.509 and Kerberos; and binds it to SOAP.

So far, we've seen how security is being applied to Web services and to SOAP in particular. The reason isn't because there is anything inherently dangerous about Web services – just that it is awkward to map 3A security, and the high-level principles of security (confidentiality, integrity, and nonrepudiation) to a distributed model.

New Threats: The Next Steps for Firewalls

Freud called dreams the “royal road to the unconscious,” believing that repressed thoughts are concealed by layers of protection while we are awake. When we are asleep, these thoughts find expression. Freud believed that a skilled psychoanalyst could use dreams to probe directly into a client's darkest secrets. The “royal road” analogy also applies to Web services, when they are implemented over HTTP. An organization may have layers of protection, but if a SOAP-over-HTTP Web service bypasses this protection, then it represents a “royal road” into the organization's IT infrastructure.

Although there is no stipulation that Web services must use HTTP, they frequently do. Existing firewalls tend to be all-or-nothing when it comes to SOAP-over-HTTP. All SOAP requests can be blocked, or all allowed through. Firewalls must be able to distinguish SOAP requests from invalid requests. A valid request and an invalid request may differ only on the basis of the SOAP method being called. Listing 1 shows a valid SOAP request to a method called “GetTime”, which takes a time zone as a parameter; Listing 2 shows a SOAP request that targets another Web service method, called “PleaseDontRunMe”.

The challenge for firewalls is how to allow the first SOAP message, targeting a valid method of a Web service, and to block the second message. It is not a case that SOAP can magically cut through firewalls – it's relatively trivial to configure a firewall to block all SOAP messages. The challenge is to *selectively* block SOAP messages. There are analogies with firewall functionality at lower layers of the OSI stack – e.g., application level gateways or stateful-inspection firewalls. Filtering on the targeted SOAP method is only the first step, however.

Filtering on the data that is provided to a Web service is more complicated because the details of each Web service are specific. Consider a Web service that takes a ZIP code as a parameter. The valid input is a five-char-

acter string. If the Web service receives 5,000 characters as input, this may indicate that an attacker is testing for vulnerability to a buffer-overflow attack. In order to block this sort of attack, a firewall must be aware of what type of data is valid for the Web service. This information is found in the WSDL for that service.

A number of vendors in the software and hardware space have launched SOAP-aware firewall products. It is important to see these in the context of “traditional” firewalls. Firewalls became popular when corporate networks were exposed to the entire world. Web services are not yet being exposed to the entire world – businesses are beginning to use XML behind the firewall, before deploying limited partner-integration projects. It can be argued that the 3A aspects of security are therefore more important than XML firewalling since it's important to control who is accessing your Web service, before examining the data they are sending.

Conclusion

This article divided Web services security into three topics: 3A security is being addressed by initiatives such as SAML, Project Liberty, and .NET Passport. The high-level principles of confidentiality, integrity, and nonrepudiation are addressed by XML-Signature and XML Encryption, which are packaged into SOAP messages using WS-Security. Finally, when SOAP is sent over HTTP, firewalls must evolve to discriminate SOAP traffic on the basis of what SOAP method is being called, and what parameters are being sent.

None of the three aspects of security mean that Web services are too “dangerous” to adopt. If proper care is used, Web services represent an exciting enabling technology that is here to stay. ☺

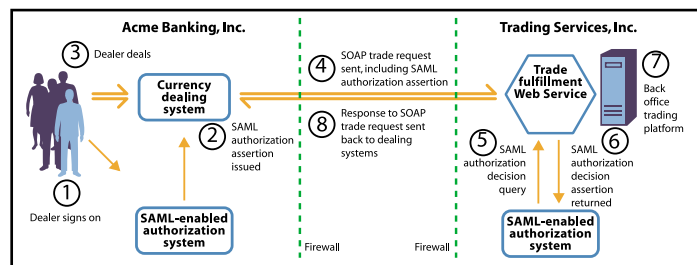


FIGURE 4 | SAML in action for Web services

WSJ ADVERTISER INDEX			
ADVERTISER	URL	PHONE	PAGE
BEA eWorld	www.bea-eworld.com		23
Global Knowledge	www.globalknowledge.com	800-COURSES	11
IBM	www.ibm.com/websphere/portalplay		2
JDJ Workshop	www.sys-con.com/education	201-802-3058	37
Linux Business & Technology	www.sys-con.com	201-802-3020	27
Mind Reef	www.mindreef.com	603-465-2204	4, 5
Parasoft	www.parasoft.com/ws2	888-305-0041	7
Pharma-IT Summit & Expo	www.pharmaitsummit.com		31
PriceWaterhouseCoopers	www.pwcglobal.com/tech-forecast_syscon		35
Sitraka (now part of Quest Software)	www.sitraka.com/class/ws	800-663-4723	19
Sitraka (now part of Quest Software)	www.sitraka.com/class/ws	800-663-4723	59
Swingtide	www.swingtide.com/testdrive		60
SYS-CON Media	www.sys-con.com/suboffer.cfm	888-303-5282	57
Web Services Edge 2003	www.sys-con.com	201-802-3069	39-56

Advertiser is fully responsible for all financial liability and terms of the contract executed by their agents or agencies who are acting on behalf of the advertiser. This index is provided as an additional service to our readers. The publisher does not assume any liability for errors or omissions.

Extending Web Services to the Real World

Using SOAP to access a J2EE-enabled mobile device

This is the first in a series of articles that will explore the realm of Web services, the challenges that lie ahead, and advancements that enable extending Web services to the real world.

Applications for real-world scenarios have significant dependencies on development time and ROI and must be robust, platform neutral, and performance sensitive. Most important, these scenarios need to be highly flexible to changes in requirements and applicability. Web ser-

vices are an effective way to balance all these aspects of real-world applications and provide a rich and extensible infrastructure for advanced topics such as J2ME interaction, portals, business on the Web, choreography, and collaboration. This article assumes that you have a basic understanding of Web services, SOAP, and the J2ME platform.

Why Web Services Make Sense for Devices

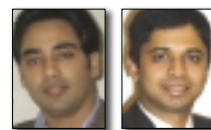
As we know, Web services can be defined as software components that are reusable,

distributed, and loosely coupled, and can encapsulate functionality and be accessed programmatically using standard Internet protocols.

The growth in e-business has led to an increased demand for instant access to real-time information and content. Users are now looking into accessing business applications not only via PCs but on mobile devices as well. Web browsers fit like a glove for over-the-wire Internet desktop computing, but were not appropriate for a wireless world that requires interactive and mobile access. Also, using browser technology on mobile devices poses challenges based on limitations in data input, client GUIs, and latency in wireless networks. And, users on-the-go find it highly cumbersome to use browse and search capabilities.

Consider a scenario in which a user would like to access real-time stock quotes. In Figure 1, the user accesses a Stock Portfolio Management Application over the wire on the back end from a Web page in a browser to look up the value of the stock.

If we extend this scenario to a user who is constantly on the move and would like to interactively access the same information in real time, we are presented with a situation in which a mobile device such as a PDA would provide such a convenience. In Figure 2, the user interactively queries a client application on a PDA that contains a list of stocks in a portfolio. The user can then select a stock



Author Bio

Ash Parikh has over 10 years of computer and IT experience, including object-oriented analysis and design, distributed architecture, middleware architecture, and software design and development. He has served in many architect-level roles with technology leaders such as Oracle Corporation, BEA Systems, Sun Microsystems, and PeopleSoft. Ash is the president of the Bay Area Chapter of the Worldwide Institute of Software Architects, an initiative close to his heart, through which he evangelizes various software architecture paradigms. He is a contributing author of *Oracle9i AS Building J2EE Applications* (Osborne Press).
ASHISHPA@HOTMAIL.COM

Ashwin Rao, the vice president of the Bay Area Chapter of the Worldwide Institute of Software Architects, has over six years of experience in software development, having begun his career writing defense industry software for real-time, embedded systems. His current focus is J2EE architecture and development and Web services. He has authored a number of articles on Web services.

ARAO@MAIL.COM



FIGURE 1 Using a Web browser to access a Stock Portfolio Management Application



FIGURE 2 Using a SOAP client application on a PDA to interact with a Stock Portfolio Management Application

Bea eWorld

www.bea-eworld.com

by clicking on a link that forwards a request to a Web service over the air using Web services technology and standard Internet protocols. The Web services accessed at the back end then interact with the Stock Portfolio Management Application.

This ability to interactively access information anytime, from anywhere, and anyhow has led to the proliferation of Web-enabled mobile clients with small form factors. More important, these clients would be ideally suited to actively participate in e-commerce transactions on the Web. This model also exposes existing legacy application services to cross-platform clients, thus enabling clients across multiple ranges of platforms to communicate with each other using an XML-based communication protocol. Such clients could perhaps be developed in different languages, OS, and hardware environments, and would be able to communicate with back-end services, once again developed in different languages, OS, and hardware environments.

Thus, the value of Web services in a mobile environment lies in the fact that they can deliver pertinent and timely information to the mobile user and provide a reliable, reconnectable infrastructure that works across platforms and architectures.

This article will use Simple Object Access Protocol (SOAP) to access a Web service.

The Architecture of J2ME Devices

The popularity of mobile devices provides a far greater opportunity to take advantage of the power of Java, with its inherent benefits such as networking and security. However, in this opportunity, there existed a quandary. The multitude of devices, with different form factors – essentially, different power consumption requirements, processing requirements, display requirements, I/O requirements – needs to be addressed by the architectural model.

Rather than adopt the least common denominator approach, the Java community developed an architecture consisting of a combination of elements that are optimized for the memory, processing power, and I/O capabilities of a related category of devices. The elements are comprised of Configurations, Profiles, and Optional Packages. This architecture is referred to as the Java 2, Micro Edition (J2ME).

A *configuration* is the lowest layer sitting on top of the device OS, and consists of a Java Virtual Machine (JVM) and a minimum set of class libraries that provides for the basic functionality of a related category of devices. Currently, two configurations have been defined based on the form factor of

mobile devices: the Connected Limited Device Configuration (CLDC) and the Connected Device Configuration (CDC).

CLDC consists of a scaled-down JVM called Kilo Virtual Machine (KVM) and is targeted at devices with slower processing power provided by 16- to 32-bit processors. CLDC is the smaller of the two configurations and is optimized for devices with low memory, in the range of 128KB to 512KB, and with a typically intermittent network connection with a small bandwidth. CDC consists of a full-fledged JVM and is targeted at devices with faster processing power with 32-bit processors. It is optimized for devices with more memory, typically 2MB, and with larger network bandwidth.

Profiles are higher-level APIs that are associated with Configurations and are layered on top of them. These APIs address the application life cycle, user interface, and device specification functionality for a related category of devices. Based on device form factors, a number of profiles, such as the Mobile Information Device Profile, (MIDP), Foundation Profile, Personal Profile and Personal Basis Profile, have been defined and are associated with the appropriate Configurations.

Layered on top of the profiles are *Optional Packages*. These packages are device specific and may be proprietary in nature. They consist of APIs that cater to specific market segment technologies, for instance SMS messaging APIs applicable to mobile phones, and also any emerging technology associated with devices.

SOAP Overview

According to the SOAP 1.1 specification, SOAP is a lightweight protocol that allows communication between objects of any kind, on any platform, and developed in any programming language. It is also a format for sending messages via the Internet, is simple and extensible, and allows you to get around firewalls. SOAP is developed as a W3C standard.

You can send an XML request to a SOAP server over HTTP and receive the response back in XML format. Since HTTP is the accepted protocol in the Internet world, and as all Web servers understand HTTP

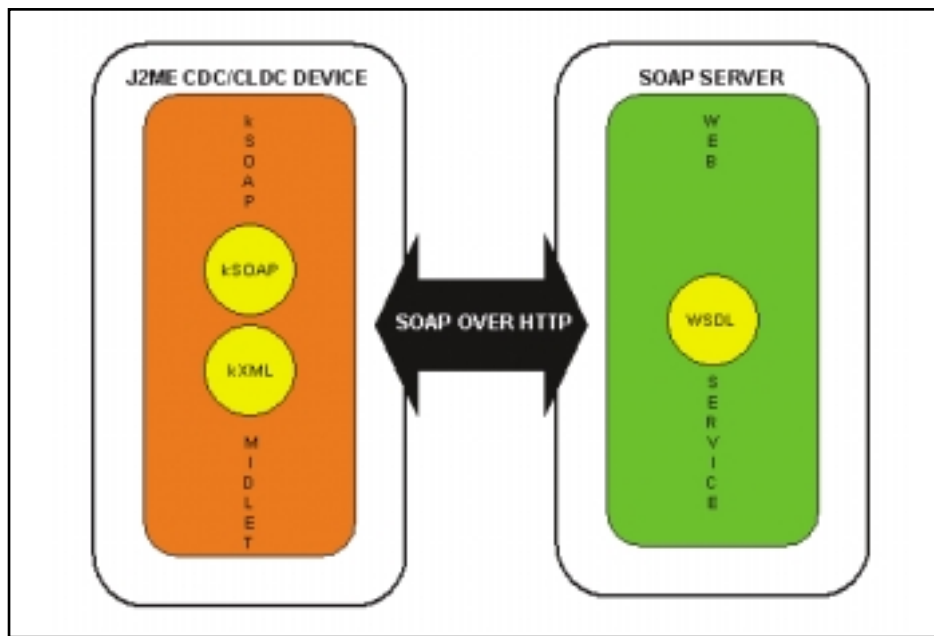


FIGURE 3 | The J2ME SOAP Stack and J2ME Web Service Interaction Architecture

requests, it is an ideal communication mode to use to enable the integration of various systems. Also, XML is emerging as the standard to exchange information over different systems. SOAP's use of XML to send and receive messages thus enables any system on any platform to read and process the messages.

Web Services Description Language (WSDL) is a standard mechanism that can define the SOAP message used to access the Web services, the protocols, and the Internet locations where these Web services can be accessed. A WSDL document describes what functionality a Web service offers, how it communicates, and where to find it. A WSDL document can be compiled to generate a SOAP client proxy that can call the Web service.

A SOAP client will initiate the process by making a SOAP request. In this process, the client will refer to the WSDL file that resides in the SOAP server to form a valid SOAP request, as shown in Figures 1 and 2. The client will then send the request to the SOAP server using HTTP.

SOAP 1.1 Implementations on the J2ME Platform

At this juncture it is important to look at a few compact, fast, and portable SOAP 1.1 implementations for J2ME. The key features of such implementations must include an XML parser, XML writing support, and a very small footprint SOAP API. Wingfoot SOAP, available at www.wingfoot.com, is a lightweight client implementation of SOAP that is specifically targeted at the J2ME CDC and CLDC platform. However, it can also be used in J2SE and J2EE environments. In this article, we will concentrate on the kXML and kSOAP open-source projects available at www.enhydra.org.

kXML provides a small-footprint XML pull parser and writer suitable for all Java platforms and J2ME CDC and CLDC, making it especially suitable for applets, Java applications, or Web services running on mobile devices like PDAs or MIDP-enabled mobile phones. It also has XML writing support, optional kDOM, and optional WAP support (WBXML/WML). kSOAP is a very small footprint SOAP API suitable for the J2ME platform and based on kXML. Figure 3 depicts the interaction between a kSOAP MIDP client applet – a MIDlet deployed on J2ME kXML and kSOAP stack – and a WSDL for the Web service available on a SOAP server infrastructure.

JSR 172: J2ME Web Services Specification

A step towards enabling developers to create and display Web services on J2ME devices has recently surfaced in the form of a Java Community Process (JCP) specification called JSR 172, designed to provide standard APIs to enable Web services for the two J2ME Optional Packages, CDC and CLDC. Content is normally delivered to the J2ME client as XML in a SOAP message, and an application on the J2ME device is used to interpret and process the message. This specification will enable service providers, device manufacturers, and content creators to realize significant ROI by rapidly and economically developing and deploying new applications, services and content to existing and new customers. This JSR extends Web services standards, including XML, SOAP, and communication with registries like UDDI to connect mobile and consumer devices. It also provides a programming model for interaction between a J2ME client and Web services.

As part of this initiative, infrastructure such as APIs for parsing structured XML data, APIs and conventions for enabling SOAP communication from J2ME, runtime APIs to support stubs generated according to the mapping, supporting XML as a transport and encoding component, and an investigation of a suitable and compact encoding mechanism for SOAP messages are being developed to enable J2ME Web services per JSR 172. (For more information on the proceedings of this JSR, please refer to <http://jcp.org/en/jsr/detail?id=172>.)

Listing 1 is the source code for the StockQuoteDemo MIDlet, a SOAP client developed using kSOAP. This MIDlet is a client application that can be installed on a J2ME device to provide access to the Stock Quote service hosted at www.xmethods.com, to retrieve and display real-time stock quotes. The link to the Web service is [www.xmethods.com/ve2/ViewListing.poj?sessionId=xHaCLLIDxdHkI-R0WtWfcNlv\(QhxieSRM\)?serviceid=](http://www.xmethods.com/ve2/ViewListing.poj?sessionId=xHaCLLIDxdHkI-R0WtWfcNlv(QhxieSRM)?serviceid=). The Endpoint URL is <http://66.28.98.121:9090/soap>. The link to the WSDL file is <http://services.xmethods.net/soap/urn:xmethods-delayed-quotes.wsdl>.

As you would do with any J2ME MIDlet, install this file in the src directory of a new J2ME Wireless Toolkit project, and then install ksoap-midp in the lib directory. (For information on downloading and using the J2ME Wireless Toolkit, please refer to <http://java.sun.com/jme>.)

After deploying the StockQuoteDemo Web Service client in the J2ME Wireless Toolkit environment, you can build and run the MIDlet by launching it from the KToolbar (see Figure 4).

A request for a stock quote is then made from the client device, after which the Web service retrieves and displays the latest market price of the stock (see Figure 5).

J2ME Web Services Development Tools Available

There are a number of free J2ME development tools available today, such as the IBM WebSphere Micro Environment; Sun ONE Studio (formerly Forte for Java); Borland JBuilder MobileSet; Sun's J2ME Wireless Toolkit, which optionally plugs into Sun ONE

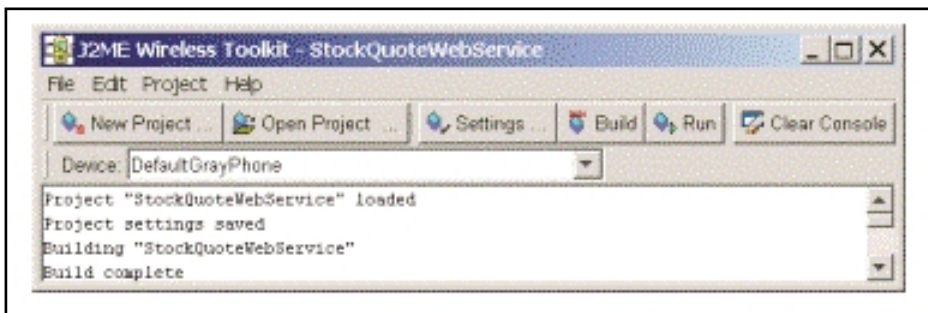


FIGURE 4 Using the KToolbar



FIGURE 5 Deployment and use of the StockQuoteDemo Web service on the J2ME Emulator

Studio and Borland IDEs; MIDP reference, MIDP for PalmOS and CLDC SDK; Motorola/Metrowerks J2ME tools for CodeWarrior; RIM BlackBerry IDE; and Zucotto WHITE-board SDK, to name a few. The J2ME Web service implementations used in conjunction with these tools could be based on the SOAP 1.1 implementations such as kSOAP or Wingfoot SOAP, discussed earlier.

Conclusion

This article showed you how a Web service is accessed from a SOAP client running on a J2ME mobile device. In the next article, we'll look at accessing a Web service through a centralized portal, using the provisioning paradigm to manage access based on a user and device profile, and usage based on billing and metering. ©

Listing 1: StckQuoteDemo MIDlet

```
import javax.microedition.midlet.*;
import javax.microedition.lcdui.*;
import java.io.*;
import javax.microedition.io.*;
import org.ksoap.*;
import org.ksoap.http.*;

public class StockQuoteDemo extends MIDlet implements
CommandListener {

    Form mainForm = new Form ("StockQuotes");

    TextField symbolField = new TextField ("Symbol", "SUNW", 5,
        TextField.ANY);

    StringItem resultItem = new StringItem ("", "");

    Command getCommand = new Command ("Get", Command.SCREEN, 1);

    public StockQuoteDemo () {
mainForm.append (symbolField);
mainForm.append (resultItem);
mainForm.addCommand (getCommand);
mainForm.setCommandListener (this);
    }

    public void startApp () {
Display.getDisplay (this).setCurrent (mainForm);
    }

    public void pauseApp () {
    }

    public void destroyApp (boolean unconditional) {
    }

    public void commandAction (Command c, Displayable d) {
try {
    // Build request string
```

```
String symbol = symbolField.getString ();
resultItem.setLabel (symbol);

    // Create a SoapObject by specifying the URN and the
method name

    // of the SOAP RPC Web Service.

    SoapObject rpc = new SoapObject
("urn:xmethods-delayed-quotes", "getQuote");

    // The addProperty method allows you to specify parameters
to for

    // the method used.

    rpc.addProperty ("symbol", symbol);

    // The HttpTransport class can be used to make the actual
call.

    // Its constructor accepts the Web Service endpoint
as well as

    // the method to be called.

    resultItem.setText (""+new HttpTransport
("http://services.xmethods.net/soap",
"urn:xmethods-delayed-quotes#getQuote").call (rpc));
}

catch (Exception e) {
    e.printStackTrace ();
    resultItem.setLabel ("Error:");
    resultItem.setText (e.toString ());
}

}

    public static void main (String [] argv) {
new StockQuoteDemo ().startApp ();
    }
}
```

Download the code at
sys-con.com/webservices

Premiering
June 2003
at
JavaOne

www.sys-con.com



Millions of Linux Users One Magazine

Linux Business and Technology

There is no escaping the penetration of Linux into the corporate world. Traditional models are being turned on their head as the open-for-everyone Linux bandwagon rolls forward.

Linux is an operating system that is traditionally held in the highest esteem by the hardcore or geek developers of the world. With its roots firmly seeded in the open-source model, Linux is very much born from the "if it's broke, then fix it yourself" attitude.

Major corporations including IBM, Oracle, Sun, and Dell have all committed significant resources and money to ensure their strategy for the future involves Linux. Linux has arrived at the boardroom.

Yet until now, no title has existed that explicitly addresses this new hunger for information from the corporate arena. *Linux Business & Technology* is aimed squarely at providing this group with the knowledge and background that will allow them to make decisions to utilize the Linux operating system.

Look for all the strategic information required to better inform the community on how powerful an alternative Linux can be. *Linux Business & Technology* will not feature low-level code snippets but will focus instead on the higher logistical level, providing advice on hardware, to software, through to the recruiting of trained personnel required to successfully deploy a Linux-based solution. Each month will see a different focus, allowing a detailed analysis of all the components that make up the greater Linux landscape.

Regular features will include:

- Advice on Linux Infrastructure*
- Detailed Software Reviews*
- Migration Advice*
- Hardware Advice*
- CEO Guest Editorials*
- Recruiting/Certification Advice*
- Latest News That Matters*
- Case Studies*

SAVE 30% OFF!

REGULAR ANNUAL COVER PRICE \$71.76

YOU PAY ONLY

\$49⁹⁹

12 ISSUES/YR

*OFFER SUBJECT TO CHANGE WITHOUT NOTICE

SUBSCRIBE TODAY!

WWW.SYS-CON.COM

OR CALL

1-888-303-5282

LINUX EDGE
conference & expo

June 3-5 LONDON
June 24-26 BERLIN
September HONG KONG
October CALIFORNIA

**SYS-CON
MEDIA**

The World's Leading IT-Technology Publisher

FOR ADVERTISING INFORMATION:

CALL 201 802.3020 OR

VISIT WWW.SYS-CON.COM

ALL BRAND AND PRODUCT NAMES USED ON THIS PAGE ARE TRADE NAMES, SERVICE MARKS, OR TRADEMARKS OF THEIR RESPECTIVE COMPANIES

The Basics of Code Access Security

Minimal coding that offers a huge return



AUTHOR BIO:



Thom Robbins is a senior technology specialist with Microsoft in New England. He focuses on .NET development and implementing XML-based solutions. Thom is a regular speaker, writer, and presenter at industry events.

TROBBINS@MICROSOFT.COM

Remember the old days when we only installed applications that were purchased from the local computer store? Actually, this was the only way to get the application media. Also, because we had mass-produced disks or tapes this provided an additional sense of security.

Of course, there were application bugs and unexpected features, but we never expected an application would intentionally destroy a desktop or server. This model doesn't work today when most software is downloaded or application code is embedded in other formats. Everything from a simple Web page to e-mails containing scripts are downloaded and run on our local machines.

The sad truth is some of this code is malicious. All companies take the necessary precautions to protect their users and critical data from the malicious code. These include firewalls, virus checkers, and common sense. Ultimately, today it seems we are always at risk. The .NET Framework provides Code Access Security (CAS) to help solve this problem and secure our systems from malicious code. In this article, I'll show the basics of how you can use CAS and the .NET Framework to protect your system.

CAS provides a centralized mechanism to assign permission levels for individual sections of code based on their origination and identity. For example, we may want to restrict Internet-downloaded controls to only accessing the user interface and specifically deny any type of access to the local file system. However, for a

small set of trusted vendors we want to provide local file system access. The problem with this example is that traditional Windows-based security doesn't provide this granular level of

support. CAS, which is part of the .NET Framework or Common Language Runtime (CLR), provides the ability to set and maintain this type of system security policy.

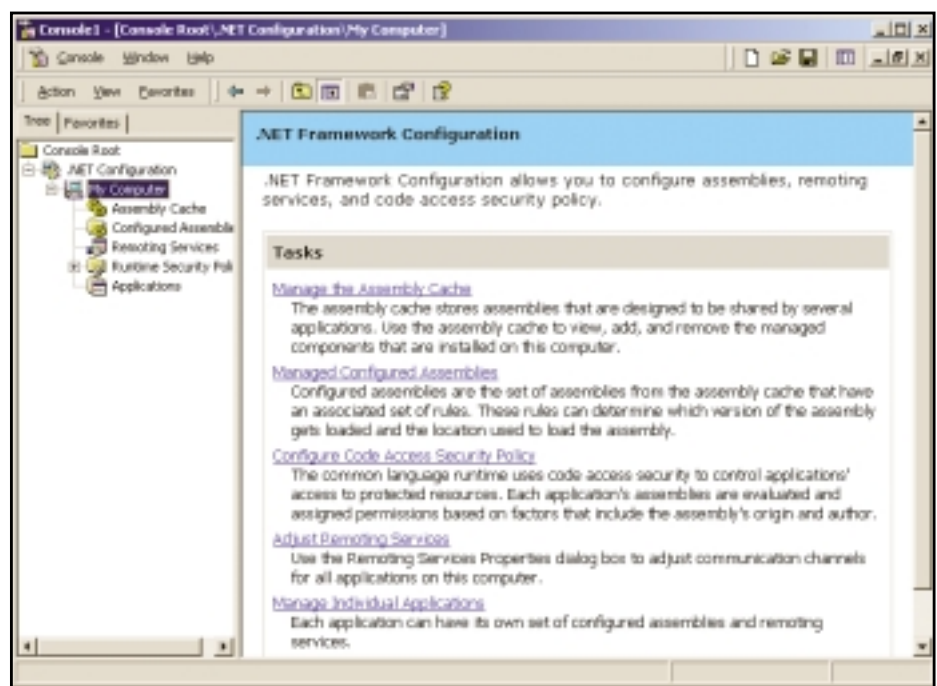


FIGURE 1

The standard MMC console is installed as part of the .NET Framework. It provides an easy-to-use way to maintain and configure security within the managed code environment.

CAS Basics

All applications that target the CLR operate in a managed environment. Among other things, this means that all code must interact with the CAS system runtime. System administrators are able to manage and uniquely specify permissions granted to each managed code assembly. Any time managed code attempts to access a protected resource (i.e., opening a file) the assigned permissions are checked. It is important to remember that the CLR walks the entire call stack when performing these checks. This prevents untrusted top-level assemblies from bypassing security checks on the lower end of the stack and gaining additional unauthorized access. The bad news is that CAS and the CLR don't have the ability to control and secure traditional unmanaged code such as COM (Component Object Model) objects. These objects deal directly with the WIN32 operating system and execute outside the control of the CLR. The good news is that CAS does offer the ability to turn unmanaged code execution on or off.

During the installation of the .NET Framework a default security policy is implemented for CAS. This policy defines the basic rules that all applications are granted by default. Actually, this is a pretty good starter set but should be thoroughly reviewed for specific concerns that companies may have. As you would expect, the policy is less restrictive for locally running applications and more restrictive for Internet-based applications. There are two ways to modify the default security framework. First is a standard MMC console (mscorefg.msc). This is the preferred method for modifying application security (see Figure 1). Second is a command-line utility called caspol.exe. This utility provides an easy to script security batch upload interface.

Assembly Requests

Essentially, Code Access Security allows each .NET assembly the ability to run with different assigned levels of privileges. Each assembly must provide specific evidence that includes its origination (Internet, intranet, or local) and optionally a public key to support its security request. CAS then evaluates these against the local security policy to determine the effective security. If at any point the assembly attempts to gain additional unauthorized permission, the CLR rejects the request and raises a security exception. One of the real benefits for end users is that they are no longer asked whether or not to trust code during

application execution. Effectively, the defined security policy and assembly evidence determine the authorization level.

Developers don't have to request permissions for their code to compile and run within the managed environment of the CLR. Ideally, it is a good practice that can make end users and system administrators better able to manage your applications. Of course, the real benefit is that by requesting permissions you are increasing the chance that your code will be allowed to execute. Additionally, if you don't identify a minimum set of permissions it becomes the developer's responsibility to gracefully handle all runtime security errors. System administrators are also able to provide a base set of permissions that meet your requested applications, requirements. Ad-

“

The general idea is that code that is downloaded, saved, and then run locally is usually inspected and reviewed...before execution ”

ministrators can use the Permission View (permview.exe) tool to examine an assembly and issue the requested permissions. If you don't provide a base permission request, administrators can't effectively determine base permissions, which can make your application difficult to administer.

Permissions are requested by applying attributes at the assembly level. These attributes vary depending on the specific permissions requested. These requests are compiled into the metadata of the assembly manifest and evaluated when code is loaded into memory for execution. Probably the most common permission request is to access unmanaged code. Listing 1 is an example of the assembly level request that uses the SecurityPermission attribute to request this access.

The SecurityPermission attribute requires

two values. The first is the SecurityAction that specifies the permission requested (Request Minimum) and a flag that indicates the requested permission (SecurityPermission Flag, UnmanagedCode).

Demand-Based Security

In addition to specifying security requests within the assembly level, you can also issue a security demand with your application. This demand specifies either declaratively or imperatively the permissions level that both direct and indirect callers must have to access your application code. Typically, direct callers are defined as members that call either static or instance methods of your application library. Indirect callers on the other hand, call either static or instance methods of another library that in turn calls yours. Within a demand request, any application that includes your code will execute only if all direct and indirect callers have the necessary security.

Demands are ideal for situations where class libraries access protected resources that you don't want to provide access to untrusted code. Demands can be placed in code using either imperative or declarative syntax. Remember that most classes in the .NET Framework already have demands associated with them. So by default you don't have to make demands associated with protected resource access. For example, the Stream Writer class automatically makes a security demand for FileIOPermission whenever it is opened. An additional demand for FileIOPermission every time you use the Stream Writer class causes an inefficient stack walk. As a general rule demands are best suited for unique resources that may require custom permissions.

Declarative demands place requests directly into your code's metadata using attributes. You can use declarative syntax to place a demand in either the class or method level of your code. If you place a declarative security check at the class level, it applies to each member of the class. However, if you place a declarative security check at the member level, it applies to only that member and overrides any permissions specified at the class level. For example, suppose you specify at the class level that PermissionA is required, and for that class's Method1 you indicate that PermissionB is required. When Method 1 is called, a security check will look only for PermissionB, but other methods of the class will still require PermissionA.

The following example places a declarative demand for a custom permission called `CustomPermission` on all callers of the `ReadData` method. The custom permission has a separately defined `CustomPermissionAttribute` that makes the demand. In this case, it takes a `SecurityAction.Demand` flag in order to specify the type of demand the attribute will perform.

```
<CustomPermissionAttribute(SecurityAction.
```

```
Demand, Unrestricted = True)>Public
Shared Function ReadData() As String
    'Read from a custom resource.
End Function
```

Imperative demands are placed in the method level of your code by creating a new instance of a permission object and calling that object's `Demand` method. The imperative syntax cannot be used to place demands at the class level. The imperative demand that you place in

your code effectively protects all the remaining code in the method in which the `Demand` method is called. The security check is performed when the `Demand` is executed; if the security check fails, a `SecurityException` is thrown and the rest of the code in that method or member is never executed unless the `SecurityException` is caught and properly handled.

The following example uses imperative syntax to place a demand on all callers for the custom permission `CustomPermission`. This code creates a new instance of the `CustomPermission` class, passing the `PermissionState.Unrestricted` flag to the constructor and then calling the `demand` method.

```
Public Shared Sub ReadData()
    Dim MyPermission As New
    CustomPermission(PermissionState.Unrestricted)
    MyPermission.Demand()
    'Read from a custom resource.
End Sub
```

Evidence-Based Security

The .NET Framework introduces a new concept for code security – evidence-based security. Evidence is the inputs to the security policy about the code. Based on the answers to these questions, the security policy can generate an appropriate set of permissions. Evidence is obtained from multiple sources that include the CLR, browser, ASP.NET, and even the operating system shell depending on the source code.

Where was the assembly obtained?

Assemblies are considered the basic building blocks of .NET Framework applications. They are the basis for deployment, version control, reuse, activation, and scoping and security authorization. Assemblies

are downloaded to the client from a Web site.

- From what URL was the assembly obtained? A security policy requires the specific address where the assembly was obtained.
- From what zone was the assembly obtained? Zones are the description of the security criteria based on the location of the code and include Internet, intranet, local machine, and others.
- What is the strong name of the assembly? The strong name is the cryptographically strong identifier provided by the author of the assembly. It doesn't provide any real authentication of the author but uniquely identifies the assembly and ensures that it hasn't been tampered with.

.NET Framework Permission Structure

The .NET Framework with Code Access Security provides a variety of permissions that you can request within your code. The following is a guide to the various permission requests available.

Permission request	Description
Minimum permissions (RequestMinimum)	Permissions your code must have in order to run.
Optional permissions (RequestOptional)	Permissions your code can use, but can run effectively without.
Refused permissions (RequestRefuse)	Permissions that you want to ensure will never be granted to your code, even if security policy allows them to be granted.
Perform any of the above requests on built-in permission sets.	Built-in permission sets, including: Nothing, Execution, FullTrust, Internet, LocalIntranet, and SkipVerification.
Perform any of the above requests on XML-encoded permission sets.	XML representation (either a string containing the XML-encoded permission set, or the location of an XML file containing the encoded permission set) of a desired permission set.

Role-Based Security

Up to this point we've discussed how Code Access Security revolves around the idea of code and not around the idea of users and roles. There is always a need to define security based on user identity. The CAS runtime also provides role-based security features that have become a standard within many enterprises, especially with the adoption of Active Directory. Within role-based security, two base levels are used: Identity and Principal.

Identity represents the user on whose behalf the code is executed. Keep in mind that this is a logical representation of the user defined by the application or developer. A principal; on the other hand, represents the actual abstraction of the user and the roles that they belong to. Classes that represent a user's identity implement the `Identity` interface. An example of a generic class providing a default implementation of this interface within the .NET Framework is `GenericIdentity`. Classes representing Principals implement the `IPrincipal` interface. An example of a generic class providing a default implementation of this interface within the .NET Framework is `GenericPrincipal`.

At runtime each thread has only one current principal object associated with it. Based on the specified security requirements, code may access and change this object as needed. Each Principal has only one identity

object. For example, Listing 2 shows a generic implementation of role-based security.

Conclusion

This article has covered quite a bit. There are a couple of things that you should remember. First, by default the security policy gives significantly more trust to code executed from the local hard drive than from other locations. The idea of executing code locally is significantly different from execut-

ing from a remote location. Downloading code, storing it to disk, and executing it has a far different set of semantics and requirements than executing code from a remote location. The general idea is that code that is downloaded, saved, and then run locally is usually inspected and reviewed, for example, with a virus scanner before execution. With CAS, the scenario is reversed. Code executed remotely provides more default security than locally executed code. It is important to un-

derstand that CAS is not a replacement for standard security precautions. It is designed to provide a new level of protection around security and maintainability of code. Also, now that you have learned the basics, start including and leveraging Code Access Security within your applications. I think you'll find that it provides a minimum of coding but yields a huge return in terms of security and manageability within your applications. ©

Listing 1: Imports System

```
Imports System.Security.Permissions
Imports System.Runtime.InteropServices
'The request is placed on the assembly level.
<assembly:
SecurityPermissionAttribute(SecurityAction.RequestMinimum,
Flags := SecurityPermissionFlag.UnmanagedCode)>

Namespace MyNamespace
    Public Class MyClass1
        Public Sub New()

        End Sub

        Public Sub MyMethod()
            'Perform interoperation with unmanaged code here.
        End Sub
    End Class
End Namespace
```

Listing 2: Generic implementation of role-based security

```
using System;
using System.Threading;
```

```
using System.Security;
using System.Security.Principal;

namespace RoleBasedSecurity
{
    class Sample
    {
        static void Main(string[] args)
        {
            String [] roles = {"Lecturer", "Student"};
            GenericIdentity i = new GenericIdentity("Thom");
            GenericPrincipal g = new GenericPrincipal(i,
                roles);
            Thread.CurrentPrincipal = g;
            if (Thread.CurrentPrincipal.Identity.Name ==
                "Thom")
                Console.WriteLine("Hello Thom");
            if (Thread.CurrentPrincipal.IsInRole("Lecturer"))
                Console.WriteLine("Hello Lecturer");
            if (Thread.CurrentPrincipal.IsInRole("Employee"))
                Console.WriteLine("Hello Employee");
        }
    }
}
```

Download the code at

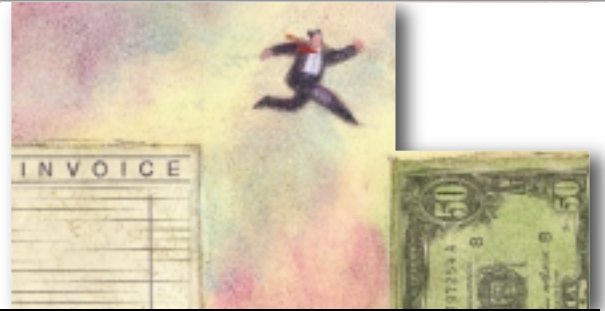
sys-con.com/webservices

Pharma-IT Summit & Expo

www.pharmaitsummit.com

The Security Challenge

A look at a typical case scenario



This article focuses on the value of Web services security. It is important to understand what Web services are and their challenges, particularly related to security. Traditionally, companies have relied on conventional, transport-level security but this approach has its limitations. The market now offers complementary XML-based solutions designed to secure documents used in Web services requests and responses. We will explore these solutions and outline "typical case scenarios" to provide a comprehensive landscape on the current offering of Web services security solutions.

AUTHOR BIO:

Marc Chanliau is a product manager for Netegrity, Inc. Chanliau has been in the software industry for over 20 years in many different capacities. Marc started the OASIS Security Services Technical Committee that culminated in the adoption of SAML as an official OASIS standard in November 2002.

MCHANLIAU@NETEGRITY.COM

Web Services Summary

Web services are loosely coupled distributed architectures that allow companies to expose business functions over the Internet. Web services are described and accessed using industry standards:

- **Extensible Markup Language (XML):** Data format
- **Simple Object Access Protocol (SOAP):** Messaging format
- **Web Services Description Language (WSDL):** Web service description
- **Universal Description, Discovery, and**

Integration (UDDI): Web service publication and discovery

Because they use standard technologies widely accepted by the industry, Web services are easy to deploy and use. They don't require expensive network architectures, and can be leveraged across applications and partners: multiple applications can take part in a Web service and a Web service can be offered to multiple partners or customers. Web services offer a less costly alternative to more proprietary business-to-business (B2B) and enterprise applica-

tion integration (EAI) solutions. They don't require specific clients, and they don't mandate proprietary communication protocols.

Web Services Challenges

For all their benefits, Web services face a few challenges. The emerging proliferation of Web services makes it necessary for enterprises to manage them. Web services management involves the ability to add or delete a Web service from the environment, administer Web services versions, monitor Web services performance, define administration points, and generate logs of all activities related to the Web services hosted by the management system.

Web services are starting to be used to carry out complex business transactions. Web services transactions are asynchronous and typically long-lived. A transaction is asynchronous when a client requesting a Web service does something else before receiving a response from the Web service provider. In transactional environments, asynchronous Web services transactions need to be coordinated, or "orchestrated."

Web services management and orchestration are predicated on Web services security, currently the main impediment to full-blown deployment of service-oriented architectures. Indeed, the first task in managing a Web service is to secure its access.

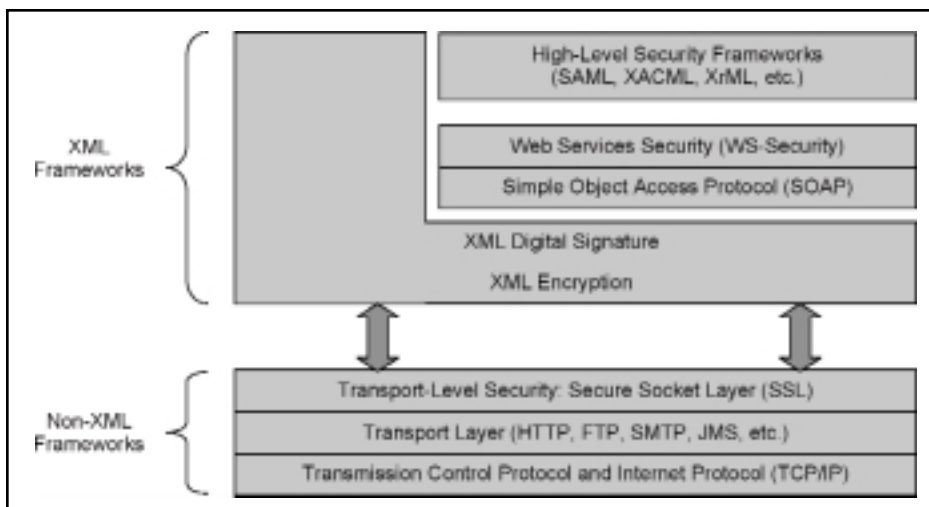


FIGURE 1 XML and Web services security stack

Web Services Security

Web services security relies on AAA (“Triple A”) insurance – authentication (“you’re in”), authorization (“once you’re in, this is what you’re allowed to do”), accounting or audit (“this is a record of what you’ve done”).

By and large, companies deploying Web services rely on traditional transport-level security for authentication, and application-specific security for authorization and accounting or audit.

Transport-Level Security

Secure Socket Layer (SSL) is the most widely used transport-level data-communication protocol. SSL provides authentication (the communication is established between two trusted parties), confidentiality (the data exchanged is encrypted), and message integrity (the data is checked for possible corruption). SSL supports transport-level security between two SSL-enabled parties. This means that when the data is not “transported” on the communication channel, it’s not encrypted; therefore, it’s not secure. This is the case when you have multiple steps in a transaction. For example, when an application invokes Web Service A for purchasing and Web Service B for shipping, you need two SSL sessions. When the documents involved in the transaction are “in transit” between the two Web services, i.e., between two SSL sessions, these documents are vulnerable to attacks. This is why transport-level security falls short, particularly in multi-step Web services.

Application-Based

Authorization and Audit

Most companies provide authorization directly into the back-end application, which creates a “silo” infrastructure. Each application’s security needs to be managed independently, thus increasing administration overhead and complex updates. Likewise, each application includes accounting and audit information that needs to be reconciled with the overall infrastructure to preserve security and consistency. Companies need to be able to validate the content of messages requesting a Web service before these messages reach the Web service, and keep track of who (or what, in the case of an application) is trying to access the Web service.

Application-Level Security

Transport-level SSL can be complemented with XML-based, application-level security,

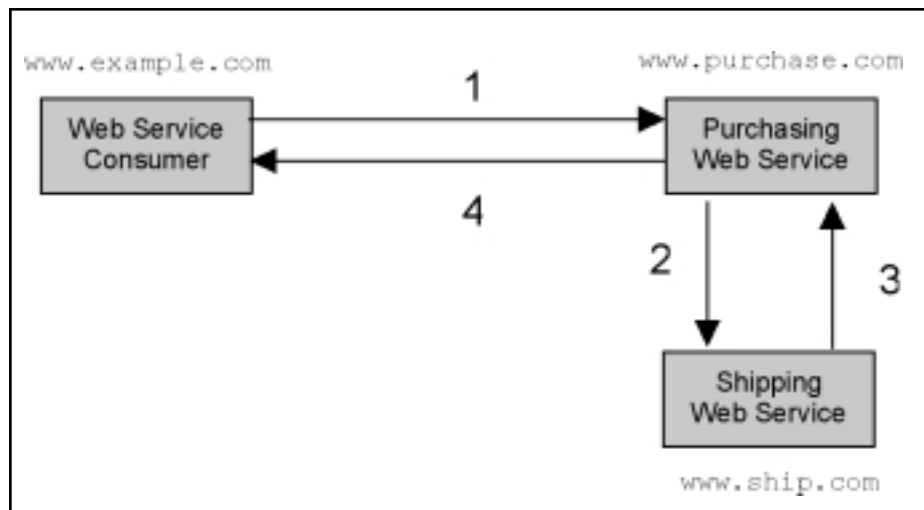


FIGURE 2 | Typical Chained Web services Scenario

including message structure; XML content confidentiality, integrity, and authenticity; and XML content access control.

Message Structure

- **Web Services Security (WS-Security):** Define security extensions to the SOAP protocol.

XML Content Confidentiality, Integrity, and Authenticity

- **XML Encryption:** Represents the encrypted content of XML data, the information that enables a recipient to decrypt it, and a mechanism for conveying encryption key information to the recipient.
- **XML-Signature:** Defines the representation of signatures on digital content and procedures for processing those signatures. XML-Signature provides detailed elements supporting data integrity, signature assurance, and nonrepudiation for Web services data.

XML Content Access Control

- **Security Assertion Markup Language (SAML):** Describes authentication, attributes, and authorization decision objects (assertions) that can be exchanged between trusted partners.
- **Extensible Access Control Markup Language (XACML):** Specifies policies to access XML documents based on objects (elements to be accessed in the XML document), subject (the user or service), action (read, write, create, delete). XACML relies on SAML for authentication.
- **Extensible Rights Markup Language (XrML):** Describes authoring rights information to be bound to an XML document.

Figure 1 shows the various layers involved in securing Web services. As I mentioned earlier, SSL is designed to encrypt a complete XML document and send it securely to a Web service provider. However, in many cases there is a need to secure only parts of a document, whether it is being sent to another party or stored before being further processed. In this case, we use XML Encryption and XML Signature.

In order to send requests to, and receive responses from, a Web service, we use the SOAP messaging framework. SOAP is augmented with a security layer defined in the WS-Security specification. WS-Security provides an envelope for the security tokens used in Web services requests and responses, such as digital certificates, Kerberos tickets, XrML, or SAML objects.

XML Encryption

XML Encryption, XML-Signature, SAML, and WS-Security all work together to ensure complete Web services security.

The XML Encryption specification describes how to represent in XML a digitally encrypted Web resource. A Web resource can be an XML document or non-XML data, such as pictures or audio files. Encryption of a document can be partial. For example, we can encrypt only a credit card number as shown in Listing 1. It defines:

- How digital content is encrypted and decrypted
- How the encryption key information is passed to a recipient
- How encrypted XML data and non-XML data is identified in order to facilitate the decryption process by the recipient

The XML Encryption specification describes how to use XML Signature with XML Encryption so that trusted parties can selectively encrypt and sign portions of documents, whether those documents are already otherwise encrypted and signed or not.

The main element in the XML Encryption schema is `<EncryptedData>`. Using this element, you can define which data in the XML document needs to be encrypted, as well as the encryption value. In the example in Listing 1, the value of the `<CreditCardNumber>` element is encrypted.

XML-Signature

The purpose of an XML signature is to associate a private key with referenced data. The key is used to ensure the provenance of the signed data. In other words, an XML signature guarantees the sender's authentication, thus assuring the recipient that the document is really coming from a trusted originator.

XML signatures apply to XML and non-XML documents. In the case of an XML document, XML signatures can apply to a part or totality of the document. They can be used with encrypted and nonencrypted documents.

Enveloped XML-signatures are embedded in the same document they apply to. Detached XML signatures apply to data that is external to the signature itself.

The XML Signature specification defines the signature syntax and data structures, as well as the signature processing rules (signature generation and validation). An XML signature is defined within the `<Signature>` element, which can be an XML document in its own right in the case of a detached signature.

Both XML-signature and XML encryption may be applied to an XML document in random order. For example, portions of a document may be encrypted by a party after the document is signed. In this case, the signature is not verifiable. The portions of the document encrypted after signing have to be decrypted before verifying the signature. The Decryption Transform for XML Signature specification enables XML signature applications to distinguish between documents encrypted before signing and documents encrypted after signing. In Listing 2, a request for a Web service is made over HTTP using a SOAP message including an XML signature.

The Security Assertion Markup Language (SAML)

SAML is an XML framework for sharing security information on the Internet through XML documents. It is designed to:

- Provide a standard way to describe existing security models
- Enable universal sharing of authentication and authorization information across enterprises
- Enable a platform-neutral solution with support for industry-standard transport protocols and messaging formats
- Keep security frameworks independent of vendor implementation and architecture

The SAML framework includes:

- **Assertions:** How you define authentication, attributes, and authorization decision information
- **A Protocol:** How you ask and get the assertions you need
- **Bindings and Profiles:** How SAML documents (assertions) ride "on" (bindings) and "in" (profiles) industry-standard transport and messaging frameworks

SAML Assertions

A SAML assertion makes statements about a subject (an individual or a service). There are three kinds of statements: authentication, attribute, and authorization decision. SAML assertions can be digitally signed (see XML-Signature above). Assertions are issued by "authorities" such as security applications or Permission Management Infrastructures (PMIs). In practice, a single authority produces and issues all three types of assertions.

All SAML assertions include the following common information:

- Issuer ID and issuance timestamp
- Assertion ID
- Subject (name and optional subject confirmation, for example a public key)
- Conditions under which an assertion is valid
- Advice on how an assertion was made

SAML Authentication statements are typically designed for Single Sign-On (SSO) use cases (see Listing 3).

SAML Attribute statements and SAML Authorization Decision statements are typically designed for distributed transactions and authorization services:

- A SAML attribute statement asserts that Subject S is associated with Attributes A, B, etc., with values a, b, etc.

- A SAML authorization decision statement is issued by an authorization authority, which decides whether to grant the request by Subject S for Action A to Resource R (e.g., a Web service), given Evidence E.

SAML Protocol

The SAML Protocol defines interaction between a SAML requester and a SAML responder (requester and responder must have a trusted relationship: they're talking about the same subject). A request is made by a SAML-aware client; a response is returned by a security service. A SAML request may include queries for authentication, attribute, and authorization decision. All types of SAML requests are met with a common SAML response, which may contain one or several assertions.

SAML Bindings

SAML bindings specify how SAML request-response message exchanges are mapped to standard messaging protocols. They define a SOAP-over-HTTP binding whereby SOAP is used to query a SAML authority and receive a response.

SAML Profiles

SAML Profiles specify how SAML assertions are inserted in, and extracted from, a message framework or protocol. They define a Web browser profile and a WS-Security profile (part of the WS-Security specification).

Web Services Security (WS-Security)

WS-Security is an XML framework that provides extensions to the SOAP envelope header used to implement message-level integrity and confidentiality in Web services. WS-Security includes security tokens that are sent as part of a SOAP message. Currently, WS-Security defines profiles for four types of security tokens:

- Kerberos tickets
- X.509 certificates
- SAML assertions
- XrML documents

WS-Security can be viewed as a security information container that can include various types of security objects. To better understand how WS-Security works, let's see how it hosts SAML information.

The WS-Security profile of SAML is based on a single interaction between a sender and a receiver.

- The sender (a Web service consumer) obtains one or more SAML assertions

PriceWaterhouseCoopers

www.pwcglobal.com/tech-forecast_syscon

and/or assertion identifiers.

- The sender adds the assertions and/or assertion identifiers to a SOAP message using WS-Security headers.
- The sender sends the SOAP message to the receiver (a Web service provider).
- The receiver processes the assertions and/or assertion identifiers present in the SOAP message.

SAML assertions and references to assertion identifiers are contained in the <wsse:Security> element, which in turn is included in the <SOAP-ENV:Header> element (see Listing 4).

Assertion identifier references and information about assertion retrieval services are included in the <wsse:SecurityTokenReference> element. One or more <saml:AssertionIDReference> elements holding the assertion identifier references may be included within the <wsse:SecurityTokenReference> element. The URI attribute of the <wsse:Reference> element specifies the location of a SAML responder implementing the SAML SOAP binding (see Listing 5).

WS-Security is the reference specification for forthcoming complementary specifications:

- **WS-SecureConversation:** Defines how security contexts are established and specify how derived keys are computed and passed.
- **WS-SecurityPolicy:** Defines the policy assertions applying to WS-Security.
- **WS-Trust:** Defines methods for issuing and exchanging security tokens, and methods to establish and access trust relationships.

Putting It All Together

This section describes a typical scenario that leverages the various security technologies described in the previous sections (see Figure 2).

1. The Web service consumer uses a local procurement application that allows him or her to fill out a purchase order in an HTML form. When he or she submits

the form, the procurement application transforms it into an XML document and inserts it in the body of a SOAP message. The procurement application also inserts the user's information in the WS-Security portion of the SOAP envelope header, either using basic authentication or a (signed) SAML assertion. Once the SOAP message is ready, the procurement application POSTs the SOAP message over HTTP or (more likely) HTTPS.

2. The Purchasing Web service receives the SOAP message from the Web service consumer and uses its security application to decrypt and process the security information included in the WS-Security element of the SOAP envelope header. If the process is successful, the user is authenticated. In addition, the Purchasing Web service security application can analyze the information in the body of the SOAP document to determine the total amount of the purchase order with XPath. XPath expressions are used to find the elements containing price data and add them up to obtain the total amount of the purchase order. The Purchasing Web service security application can then compare the total amount of the purchase order with the entitlements of the Web service consumer. If the total amount of the purchase order is less than the entitlement assigned to the Web service consumer, authorization to process the purchase order by the Web service is granted. When the Purchasing Web Service has finished processing the order, it sends a request for shipment to the Shipping Web service (in effect, the Purchasing Web service becomes a Web service consumer). The request is wrapped up in a SOAP message, which also includes security information in

the SOAP envelope header and possible additional attachments in the SOAP envelope body, such as a legal document.

3. When the Shipping Web service has successfully processed the shipment order, it sends a SOAP message to the Purchasing Web service.
4. The Purchasing Web service in turn sends a SOAP message back to the original Web service consumer, informing the user that the purchase order has been processed successfully and is being shipped. Or, the Shipping Web service can inform the original requester directly (using a SOAP message).

References

- *XML 1.0 Second Edition Recommendation:* www.w3.org/XML/
- *SOAP specification v1.1:* www.w3.org/TR/SOAP
- *Working draft of the Web services security core specification:* www.oasis-open.org/committees/wss/documents/WSS-Core-08-1212-merged.pdf
- *XML Signature Recommendation:* www.w3.org/DSig/Overview.html
- *XML Encryption Recommendation:* www.w3.org/Encryption/2001
- *Decryption Transform for XML Signature Recommendation:* www.w3.org/TR/xmlenc-decrypt
- *Security Assertion Markup Language (SAML) specification:* www.oasis-open.org/committees/security
- *Extensible Access Control Markup Language specification:* www.oasis-open.org/committees/xacml
- *Extensible Rights Markup Language home page:* <http://xml.coverpages.org/xmlr.html>
- *The XML Path (or XPath) specification defines a language designed to locate XML objects (elements, etc.) in an XML document:* www.w3.org/TR/xpath ©

Listing 1: Simple XML Encryption

```
<?xml version="1.0"?>
<PaymentInfo xmlns="http://www.example.com/payment">
  <CreditCard>
    <Name>Marc Chanliau</Name>
    <CreditCardNumber>
      <EncryptedData xmlns="http://www..." Type="http://www...">
        <CipherData>
          <CipherValue>A23B45C56</CipherValue>
        </CipherData>
      </EncryptedData>
    </CreditCardNumber>
  </CreditCard>
</PaymentInfo>
```

```
</EncryptedData>
</CreditCardNumber>
<ExpireDate>06/03</ExpireDate>
</CreditCard>
</PaymentInfo>
```

Listing 2: Embedded XML Signature

```
POST/RatingService HTTP/1.1
Host: www.example.com
Content-Type: text/xml; charset="utf-8"
```

SaturdaySessions

Alan Williamson
JDJ Editor-in-Chief

We understand the pressures of work and how difficult it can be to get time off. That is why we have designed this workshop to be held in one day and, as a special bonus, on the weekend, so no days off from work. **Your boss will be happy!**

JDJ Workshop with Alan Williamson

M	T	W	T	F	S	S
---	---	---	---	---	---	---

Coming to you...

April:
NEW YORK
WASHINGTON, DC

May:
BOSTON
TORONTO

June:
ATLANTA
RALEIGH

Performance > Efficiency > Reliability

This one-day intensive workshop is designed for developers who wish to increase the efficiency and reliability of their code development.

- 1) The day will begin by looking at the various hints and tips you can utilize at the code level to improve the quality and reduce the number of bugs you have to contend with.
- 2) The next part will look at Apache's Ant and how you can use this freely available tool for your own development, irrespective of your IDE.
- 3) Last, and most important, as the old saying goes: "You can never do enough testing." This session will look at JUnit and show you how to start building test harnesses for your code so you can begin your testing strategy.

>Performance

Java is a powerful language. While it offers a rich array of tools, the fundamentals mustn't be overlooked. Improving your code at the core layer will result in great improvements in efficiency and produce (hopefully) less bugs. We'll look at the do's and don'ts of programming and learn many hints and tips that will accelerate your Java coding.

>Efficiency with Ant

Apache's Ant is a powerful scripting tool that enables developers to define and execute routine software development tasks using the simplicity and extensibility of XML. Ant provides a comprehensive mechanism for managing software development projects, including compilation, deployment, testing, and execution. In addition, it is compatible with any IDE or operating system.

> Reliability with JUnit

A critical measure of the success of software is whether or not it executes properly. Equally important, however, is whether that software does what it was intended to do. JUnit is an open-source testing framework that provides a simple way for developers to define how their software should work. JUnit then provides test runners that process your intentions and verify that your code performs as intended. The result is software that not only works, but works in the correct way.

What you will receive...

- ✓ INTENSIVE ONE-DAY SESSION
- ✓ DETAILED COURSE NOTES AND EXCLUSIVE ONLINE RESOURCES
- ✓ JDJ CD ARCHIVE



To Register

www.sys-con.com/education

Call 201 802-3058

SPONSORED BY

JAVA DEVELOPER'S JOURNAL

PRODUCED BY
SYS-CON EVENTS

PRESENTED BY
i-TECHNOLOGY EDUCATION

```

Content-Length: 2841
SOAPAction: "getCreditRating"

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAPENV="http://...">
  <SOAP-ENV:Header>
    <SOAP-SEC:Signature SOAP-SEC:mustUnderstand="1"
      xmlns:SOAP-SEC="http://...">
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <!-- The signedInfo element allows us to sign any
                portion of
                a document, in this case, we sign the body -->
          <CanonicalizationMethod Algorithm="http://www..." />
          <SignatureMethod Algorithm="http://www..." />
          <Reference URI="#Body">
            <DigestMethod Algorithm="http://www..." />
            <DigestValue>
              o+jtqlieRtF6DrUbX8O9M/CmySg=...
            </DigestValue>
          </Reference>
        </SignedInfo>
        <!-- Following is the result of running the algorithm
              over
              the document. If changes are made to the
              document,
              the SignatureValue is changed. The security
              application
              verifies the SignatureValue, extracts the X509
              certificate and uses it to authenticate the
              user -->
        <SignatureValue>
          oa+ttbsvSFieRD2oNC5iRu2eIoqWpD6PVYIKqc...
        </SignatureValue>
        <KeyInfo>
          <KeyValue>
            <!-- Following is the public key that matches the
                  private
                  key that actually signs the document -->
            <RSAKeyValue>
              <Modulus>
                5TT/oolzTiP++Ls6GLQUM8xoFFrAlZQ...
              </Modulus>
              <Exponent>EQ==</Exponent>
            </RSAKeyValue>
          </KeyValue>
          <!-- Following is the certificate -->
          <X509Data>
            <X509Certificate>
              MIIBWDCCAxggAwIBAgI...
            </X509Certificate>
          </X509Data>
        </KeyInfo>
      </Signature>
    </SOAP-SEC:Signature>
  </SOAP-ENV:Header>

```

```

<SOAP-ENV:Body ID="Body"
  <!-- Here we can have any business payload such as a
        purchase
        order. This is the part we signed in this example -->
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Listing 3: Simple SAML Authentication Assertion

```

<saml:Assertion
  AssertionID="10.255.1.3.1034108172377"
  IssueInstant="2002-10-08T20:16:12.377Z"
  Issuer="TransactionMinderSAMLIssuer"
  MajorVersion="1" MinorVersion="0"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
  <saml:Conditions
    NotBefore="2002-10-08T20:16:12.307Z"
    NotOnOrAfter="2002-10-08T22:16:12.307Z"/>
  <saml:AuthenticationStatement
    AuthenticationInstant="2002-10-08T20:16:12.307Z"
    AuthenticationMethod="urn:oasis:names:tc:SAML...">
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.0..."
        NameQualifier="Domain Name">
        Marc Chanliau
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>http://www.../>
        <saml:SubjectConfirmationData>
          R1VD8fkkvrlrh
        </saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
    </saml:Subject>
    </saml:AuthenticationStatement>
  </saml:Assertion>

```

Listing 4: SAML Assertion in WS-Security

```

<SOAP-ENV:Envelope>
  <SOAP-ENV:Header>
    <wsse:Security>
      <saml:Assertion>...</saml:Assertion>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>...</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Listing 5: Referring SAML information in WS-Security

```

<wsse:SecurityTokenReference>
  <saml:AssertionIDReference>
    XVB12#$21abc...
  </AssertionIDReference>
  <wsse:Reference URI="http://www.example.com/SAMLservice"/>
</wsse:SecurityTokenReference>

```

Download the code at
sys-con.com/webservices

THE LARGEST WEB SERVICES, JAVA, XML AND .NET CONFERENCE AND EXPO IN THE WORLD!

Boston
2003

London
2003

Berlin
2003

Hong Kong
2003



Register by
March 14th
SAVE
UP TO **\$200**

3rd Annual

EAST

Web Services Edge Conference & Exposition

FINAL PROGRAM



Connecting the Enterprise with
Web Services, Java, XML, & .NET



March 18-20, 2003
Hynes Convention Center
Boston

**CALL TODAY
TO REGISTER**
201-802-3058
OR REGISTER ONLINE AT
www.sys-con.com

Event Sponsors

Microsoft



SYBASE



DIGITAL EVOLUTION
The Business Value of Web Services

COMPUWARE



ORACLE



Rational
the e-development company™

ALTOVA

Media Sponsors

JAVA DEVELOPERS JOURNAL

JavaWorld

WebServices

LINUX WEEK

XML JOURNAL

SAMS

BASIS

Perforce

PowerBuilder

.NET JOURNAL

SD Times

asp.netPRO

WebSphere

WebLogic

wireless

CF Advisor

ColdFusion

IBM

HSP

PowerBuilder Journal

OWNED BY
sys-con
MEDIA

PRODUCED BY
sys-con
EVENTS

Special Insert: Web Services Edge East Conference & Expo

Featuring FREE Tutorials, Training Sessions, Case Studies and Exposition

REGISTRATION FORM

CONFERENCE: March 18 – 20, 2003 EXPO: March 19 – 20, 2003

John B. Hynes Veteran Memorial Convention Center • Boston, MA

THREE WAYS TO REGISTER FOR CONFERENCE

- 1) On the Web:** Credit Cards or "Bill Me" Please make checks payable to SYS-CON Events
- 2) By Fax:** Credit Cards or "Bill Me" 201-782-9651
- 3) By Mail:** 135 Chestnut Ridge Road, Montvale, New Jersey 07645, Attention: Registration

Please note: Registrations are not confirmed until payment is received.

Please complete sections 1, 2, 3 and 4

1 YOUR INFORMATION (Please Print) ☐ Mr. ☐ Ms.

First Name _____ Last Name _____

Title _____

Company _____

Street _____

Mail Stop _____

City _____

State _____ Zip _____ Country _____

Phone _____

Fax _____ E-Mail _____

2 PAYMENT METHOD: (Payment in full due with registration)

☐ Check or Money Order Enclosed (Registration confirmed upon receipt of payment)

Check # _____ Amount of Check \$ _____

Charge my ☐ Visa ☐ MasterCard ☐ American Express ☐ Discover

Name on card _____

Card # _____ Exp. Date _____

Signature _____

Billing Address (if different from mailing address) _____

3 PLEASE INDICATE YOUR CONFERENCE CHOICE

	Before 2/28/03	Before 3/14/03	On Site
<input type="checkbox"/> GP Gold Passport Good for all three days of the .NET, Web Services, XML, Java, and Vendor Tracks, including the XML Certified Developer Fast Path Tutorial, Keynotes, Panel Discussions, preferred seating for Microsoft .NET's Russ' "Tool Shed" Tutorial, and your choice of One Sun Microsystems Java® University Class	\$1,495.00	\$1,695.00	\$1,795.00
<input type="checkbox"/> 3D Three Day Conference (Does not include Sun Java™ Education)	\$1,295.00	\$1,495.00	\$1,695.00
<input type="checkbox"/> 2 Day Conference (Does not include Sun Java™ Education) (select any two days: <input type="checkbox"/> Tue. <input type="checkbox"/> Wed. <input type="checkbox"/> Thurs.)	\$1,195.00	\$1,295.00	\$1,395.00
<input type="checkbox"/> 1 Day Conference (Does not include Sun Java™ Education) (select any one day: <input type="checkbox"/> Tue. <input type="checkbox"/> Wed. <input type="checkbox"/> Thurs.)	\$495.00	\$695.00	\$895.00
<input type="checkbox"/> JU1 Sun Java™ University Class Select one: <input type="checkbox"/> Web Services Programming Using Java™ Technology and XML (Mar.18) <input type="checkbox"/> Java™ Fast Path: Programmer (Mar.19) <input type="checkbox"/> Java™ Fast Path: Architect (Mar. 20)	\$695.00	\$895.00	\$995.00
<input type="checkbox"/> JU2 Sun Java™ University Class Select two: <input type="checkbox"/> Web Services Programming Using Java™ Technology and XML (Mar.18) <input type="checkbox"/> Java™ Fast Path: Programmer (Mar.19) <input type="checkbox"/> Java™ Fast Path: Architect (Mar. 20)	\$1,295.00	\$1,495.00	\$1,595.00
<input type="checkbox"/> JU3 Sun Java™ University Class Select three: <input type="checkbox"/> Web Services Programming Using Java™ Technology and XML (Mar.18) <input type="checkbox"/> Java™ Fast Path: Programmer (Mar.19) <input type="checkbox"/> Java™ Fast Path: Architect (Mar. 20)	\$1,495.00	\$1,695.00	\$1,895.00

4

A. Your Job Title

☐ CTO, CIO, VP, Chief Architect
☐ Software Development Director/Manager/Evangelist
☐ IT Director/Manager
☐ Project Manager/Project Leader/Group Leader
☐ Software Architect/Systems Analyst
☐ Application Programmer/Evangelist
☐ Database Administrator/Programmer
☐ Software Developer/Systems Integrator/Consultant
☐ Web Programmers
☐ CEO/COO/President/Chairman/Owner/Partner
☐ VP/Director/Manager Marketing, Sales
☐ VP/Director/Manager of Product Development
☐ General Division Manager/Department Manager
☐ Other (please specify) _____

B. Business/Industry

☐ Computer Software ☐ Travel/Hospitality
☐ Computer Hardware and Electronics ☐ Government/Military/Aerospace
☐ Computer Networking & Telecommunications ☐ Health Care/Medical
☐ Internet/Web/E-commerce ☐ Insurance/Legal
☐ Consulting & Systems Integrator ☐ Education
☐ Financial Services ☐ Utilities
☐ Manufacturing ☐ Architecture/Construction/Real Estate
☐ Wholesale/Retail/Distribution ☐ Agriculture
☐ Transportation ☐ Nonprofit/Religious
☐ Other (please specify) _____

C. Total Number of Employees at Your Location and Entire Organization (check all that apply):

	Location	Company
10,000 or more	01 <input type="checkbox"/>	01 <input type="checkbox"/>
5,000 - 9,999	02 <input type="checkbox"/>	02 <input type="checkbox"/>
1,000 - 4,999	03 <input type="checkbox"/>	03 <input type="checkbox"/>
500 - 999	04 <input type="checkbox"/>	04 <input type="checkbox"/>
100-499	05 <input type="checkbox"/>	05 <input type="checkbox"/>
100 or less	06 <input type="checkbox"/>	06 <input type="checkbox"/>

D. Please indicate the value of communications and computer products and services that you recommend, buy, specify or approve over the course of one year:

☐ \$10 million or more ☐ \$10,000 - \$99,999
☐ \$1 million - \$9.9 million ☐ Less than \$10,000
☐ \$500,000 - \$999,999 ☐ Don't know
☐ \$100,000 - \$499,999

E. What is your company's gross annual revenue?

☐ \$10 billion or more ☐ \$1 million - \$9.9 million
☐ \$1 billion - \$9.9 billion ☐ Less than \$1 million
☐ \$100 million - \$999 million ☐ Don't know
☐ \$10 million - \$99.9 million

F. Do you recommend, specify, evaluate, approve or purchase wireless products or services for your organization?
01 ☐ Yes 02 ☐ No

G. Which of the following products, services, and/or technologies do you currently approve, specify or recommend the purchase of?

☐ Application Servers
☐ Web Servers
☐ Server Side Hardware
☐ Client Side Hardware
☐ Wireless Device Hardware
☐ Databases
☐ Java IDEs
☐ Class Libraries
☐ Software Testing Tools
☐ Web Testing Tools
☐ Modeling Tools
☐ Team Development Tools
☐ Installation Tools
☐ Frameworks
☐ Database Access Tools / JDBC Devices
☐ Application Integration Tools
☐ Enterprise Development Tool Suites
☐ Messaging Tools
☐ Reporting Tools
☐ Debugging Tools
☐ Virtual Machines
☐ Wireless Development Tools
☐ XML Tools
☐ Web Services Development Toolkits
☐ Professional Training Services
☐ Other [Please Specify] _____

SYS-CON Events, Inc., and SYS-CON Media make no warranties regarding content, speakers or attendance. The opinions of speakers, exhibitors and sponsors do not reflect the opinion of SYS-CON Events and SYS-CON Media and no endorsement of speakers, exhibiting companies products, or sponsors is implied.



If you require special assistance covered under the Americans with Disabilities Act, please call 201-802-3058 by March 4, 2003.

CANCELLATIONS, SUBSTITUTIONS, REFUNDS

Fax written request to SYS-CON Registration 201-782-9651. Requests for refunds received prior to February 15, 2003 will be honored, less a 10% handling charge; requests received after February 15, 2003, and before March 1,

2003, will be honored less a 20% handling charge. No requests for refunds will be honored after March 1, 2003. Requests for substitutions must be made in writing prior to March 14, 2003. No one under 18 is permitted to attend. No warranties are made regarding the content of sessions or materials. Speakers,

sessions and schedule are subject to change without prior notice.

No solicitation by anyone other than official exhibitors, sponsors or marketing partners is permitted. Such behavior is cause for expulsion without refund.

Keynotes & Highlighted Speakers



John Magee
Vice President, Oracle9i

ORACLE

John Magee is vice president, Oracle9i, at Oracle. He has more than 14 years' experience in the enterprise software industry and has held positions in product development, product management, and product marketing. In his current role,

Magee manages technical product marketing for Oracle's application server and development tools products, and is responsible for evangelizing Oracle technology initiatives around J2EE, XML, and Web services.

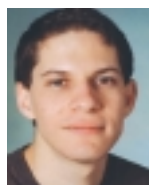


Mark Herring
Director, Java, Web Services & Tools Business

Sun Microsystems

Mark Herring is responsible for helping to define, set, and drive Sun Microsystems' product direction in the Java, Web Services & Tools Business. Prior to his current role, Herring was director of corporate

strategy & planning, looking after Sun's interest in the Project Liberty Alliance and Network Identity. Herring joined Sun Microsystems in October 1999 as a result of Sun's acquisition of Forte Software. Forte Software was a leading provider of enterprise-class development and integration products. During his four years at the company, he ran several aspects of Forte's marketing organization, including product marketing and the Web channel.



Miguel de Icaza
Cofounder and CTO



As the founder and leader of the GNOME Foundation, Miguel de Icaza is one of the foremost luminaries in the Linux development community. With his seemingly boundless energy, de Icaza has galvanized the effort to make Linux

accessible and available to the average computer user. He brings this same excitement to his role as CTO of Ximian. de Icaza was instrumental in porting Linux to the SPARC architecture and led development of the Midnight Commander file manager and the Gnumeric spreadsheet. He is also a primary author of the design of the Bonobo component model, which leads the way in the development of large-scale applications in GNOME.



Mark Hapner
Distinguished Engineer, Sun Microsystems

Mark Hapner is a Sun Distinguished Engineer and is currently lead architect for Java™ 2 Platform, Enterprise

Edition (J2EE™). He has guided the overall architecture for J2EE 1.2, 1.3, and now the upcoming 1.4 release. In March of 1996, he joined

Sun's JavaSoftware Division to participate in the development of the Java database connectivity API (JDBC). Following that, he was co-spec lead of the Enterprise JavaBeans specification and spec lead of the Java Message Service specification.



Simon Phipps
Chief Technology Evangelist, Sun Microsystems

Simon Phipps, currently chief technology evangelist at Sun Microsystems, speaks frequently at industry conferences on the subject of technology trends and futures. He was previously involved in OSI standards in the 1980s, in the earliest collaborative conferencing software in the early 1990s, and in introducing Java and XML to IBM.



Dave Chappell
VP, Chief Technology Evangelist, Sonic Software

Dave Chappell is the vice president and chief technology evangelist for Sonic Software. He has more than 18 years of industry experience building software tools and infrastructure for application developers, spanning all aspects of R&D, sales, marketing, and support services. Chappell has published in numerous technical journals, and is currently writing a series of contributed articles for *Java Developer's Journal*.



Eric Newcomer
Chief Technology Officer, IONA

In the role of chief technology officer at IONA, Eric Newcomer is responsible for IONA's technology roadmap and the direction of IONA's Orbix E2A e-Business Platforms as relates to standards adoption, architecture, and product design. Newcomer joined IONA in November 1999, and most recently served as IONA's vice president of engineering, Web Services Integration Products. He is a member of the XML Protocols and Web Services Architecture working groups at the W3C and IONA's Advisory Committee representative to UDDI.org.



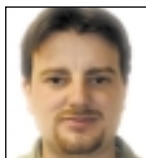
Dean Guida
CEO and President, Infragistics

Dean Guida is CEO and president of Infragistics and was CEO and a cofounder of ProtoView Development Corporation. Mr. Guida has over 15 years of experience in the technical industry and oversees all aspects of the company's business operations and corporate direction. He is also responsible for cultivating strategic alliances and other external relationships, as well as managing corporate financial affairs.

Conference Advisory Board



Sean Rhody
Editor in Chief,
Web Services Journal
Partner, CSC



Alan Williamson
Editor in Chief,
Java Developer's Journal
Chief Technology
Officer, n-ary



Derek Ferguson
Editor in Chief,
.NET Developer's Journal
Chief Technology Evangelist,
Expand Beyond Corp.



Bob Familiar
.NET Architect,
Microsoft
New England



Thomas Robbins
Senior Technology Specialist,
Microsoft
New England



Hitesh Seth
Editor in Chief,
XML-Journal
Chief Technology Officer, iigo



J.P. Morgenthal
Chief Services Architect,
Software AG









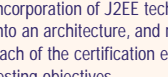
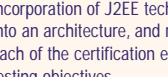
Special Insert: Web Services Edge East Conference & Expo

Featuring FREE Tutorials, Training Sessions, Case Studies and Exposition

Conference at-a-Glance

THE LARGEST AND THE MOST

		JAVA	WEB SERVICES	.NET
TUESDAY MARCH 18	8:00AM – 4:00PM	Registration Open		
	9:00AM – 9:50AM	(JV1) Squeezing the Best Out of Java Alan Williamson, Java Developer's Journal	(WS1) Web Services Infrastructure Carl Sjogreen, BEA	(NT1) .NET Framework Overview Bob Familiar, Microsoft
	10:00AM – 10:50AM	Web Services Keynote: John Magee, Oracle		
	11:00AM – 11:50AM	(JV2) Testing Your Java Using JUnit Kyle Gabhart, LearningPatterns	(WS2) Web Services Management James Phillips, Actional	(NT2) Introduction to ASP.NET Russ Fustino, Microsoft
	1:00PM – 1:50PM	WS-I Panel: "A Road Map for Web Services Standards" - Moderated by Rob Cheng, WS-I		
	2:00PM – 2:50PM	.NET Keynote: "The MONO Project" - Miguel de Icaza, Ximian		
	3:00PM – 3:50PM	(JV3) Building/Deploying the Ant Way Kyle Gabhart, LearningPatterns	(WS3) Strategies for Using Databases in a World of Web Services Mike Lehmann, Oracle	(NT3) Introduction to VB.NET Russ Fustino, Microsoft
	4:00PM – 4:50PM	(JV4) Unlocking the Secrets of JDK1.4 Raghavan Srinivas, Sun Microsystems	(WS4) Using Web Services to Integrate J2EE and .NET Enterprise Applications - Odysseas Pentakalos, SYSNET International	(NT4) How to Develop an End-to End .NET Connected Application Allan da Costa Pinto, Microsoft
WEDNESDAY MARCH 19	8:00AM – 4:00PM	Registration Open		
	9:00AM – 9:50AM	(JV5) Java APIs for Web Services Security Standards Sang Shin, Sun Microsystems	(WS5) Combining BPM and BRM Technologies: A Major Step Towards Corporate Agility Henry Bowers, ILOG	(NT5) .NET: The Virtualized Execution Engine Yahya Mirz, Aurora Borealis
	10:00AM – 10:50AM	Java Keynote: Mark Herring, Sun Microsystems		
	11:00AM – 6:00PM	EXPO OPEN 11:00 a.m. - 6:00 p.m.		
	11:00AM – 11:50AM	(JV6) Using SWT Under Eclipse\ Alternative - IBM	(WS6) Web Services for Real-Time Data Access in an Industrial Setting Stephan Van Dijk, ABB/SKYVA	(NT6) Introduction to DotGNU Barry Fitzgerald, DotGNU
	12:00PM – 2:00PM	BREAK & EXPO		
	2:00PM – 2:50PM	.NET Panel Discussion - Moderated by Derek Ferguson, .NET Developer's Journal		
	3:00PM – 3:50PM	(JV7) Unlocking the Power of XML Hitesh Seth, ikigo	(WS7) Web Services Architecture: The Next Big Spec. from the Mouths of the W3C Eric Newcomer, IONA (moderator)	(NT7) Introduction to SSCLI Yahya Mirz, Aurora Borealis
THURSDAY MARCH 20	4:00PM – 4:50PM	(JV8) Java and .NET Derek Ferguson, Expand Beyond	(WS8) Web Services: Next Steps After the Hype Claire Dessaux, Oracle	(NT8) Mobile Development with the Compact Framework Brad McCabe, Infragistics
	8:00AM – 4:00PM	Registration Open		
	9:00AM – 9:50AM	(JV9) Writing SOAP Services Nigel Thomas, SpiritSoft	(WS9) Web Services Best Practices Chris Peltz, HP	(NT9) Best Practices for .NET Development Joe Stagner, Microsoft
	10:00AM – 10:50AM	.NET Keynote - Jesse Liberty, Liberty Associates		
	11:00AM – 4:00PM	EXPO OPEN 11:00 a.m. - 4:00 p.m.		
	11:00AM – 11:50AM	(JV10) Working with Data the JDO Way Patrick Linsky, SolarMetric	(WS10) Web Services Startups: Telltails of the Future Simeon Simeonov, Polaris Venture Partners	(NT10) Best Practices for ADO.NET Development Thom Robbins, Microsoft
	12:00PM – 2:00PM	BREAK & EXPO		
	2:00PM – 2:50PM	Java Panel - "The Future of Java", Moderated by Alan Williamson, Java Developer's Journal		
	3:00PM – 3:50PM	(JV11) Enterprise: The Next Generation Mark Hapner, Sun Microsystems	(WS11) Open Standards for Web Services Messaging Dave Chappell, Sonic Software	(NT11) How to Debug with .NET Tony Denbow, STAR Information Technology
	4:00PM – 4:50PM	(JV12) Overcoming the Challenges of J2ME Dr. Jeff Capone, Aligo	(WS12) Web Services Security Marc Chanliau, Netegrity	(NT12) XML and Web-Enabling Legacy Applications Using BizTalk Mike Cramer, Microsoft

XML		VENDOR	JAVA UNIVERSITY PROGRAM	FAST TRACKS & TUTORIALS
(XM1) XML - A Manager's Guide JP Morgenthal, Software AG		Visit www.sys-con.com for details	 9:00AM – 5:00PM Web Services Programming Using Java™ Technology and XML This one-day seminar provides in-depth knowledge on Web services and shows how to develop Web services using the Java programming language and XML, the technologies of portable code and portable data respectively.	 9:00AM – 5:00PM XML Certified Developer Fast Path This tutorial is for programmers who have some knowledge of XML and related technologies and would like to pass the IBM Certified Developer Test 141 on XML and Related Technologies.
(XM2) OASIS Standards Update Karl Best, OASIS		(VN2) The XMLSPY 5 Enterprise Edition Development Environment Trace Galloway, Altova		
(XM3) A Definitive Introduction to XML Schemas Hitesh Seth, ikigo		(VN3) SOAP and Java: Marrying Them Off Skip Marler, Parasoft		
(XM4) XML in Print - XSL:FO Frank Neugebauer, IBM		Visit www.sys-con.com for details	 9:00AM – 5:00PM Java 2 Platform Programmer Certification Fast Path This session, developed and delivered by Philip Heller, author of the two leading Java technology certification preparation manuals, helps to prepare you for the Sun Certified Programmer for the Java 2 Platform exam. Philip provides code-level, detailed review of the skills and knowledge needed to confidently approach the exam.	 9:00AM – 5:00PM Russ' Tool Shed Join Russ as he shows you how to use Visual Studio.NET. 9:00-12:15 - Introduction to Web Services Using VS.NET 1:00-2:30 - Advanced Web Services Using ASP.NET 2:45-4:15 - .NET Remoting Essentials 
(XM5) XML Security Integration Challenges Phil Steitz, American Express		(VN5) Process-Centric Enterprises Eric Pulier, Digital Evolution		
(XM6) Case Study: XML in Life Sciences Tim Matthews, Ipedo		(VN6) Pattern Driven Application Development Tom Shore, Compuware		
(XM7) Using XML for EAI - Best Practices Dan Enache, TIBCO		(VN7) Managing the Developer Relationship Mike Bellissimo, Sun Microsystems	 9:00AM – 5:00PM Java 2 Platform Architect Certification Fast Path This intense one-day session helps prepare attendees to pass the Sun Certified Enterprise Architect for J2EE Technology exam. This session provides an overview of the components comprising the J2EE architecture as a whole, emphasizes the incorporation of J2EE technology into an architecture, and reviews each of the certification exam's testing objectives.	 9:00AM – 5:00PM Mobile .NET In this session, Derek Ferguson, editor-in-chief of <i>.NET Developer's Journal</i> , will give you a thorough introduction to the use of .NET with all manner of mobile computing devices. 
(XM8) Delivering Web Services to Mobile Clients with XML Transformation Frameworks Paul Lipton, Computer Associates		(VN8) Web Services Diagnostics Dave Seidel, Mindreef		
(XM9) Delivering Web Services to Mobile clients with XML Transformation Frameworks - Paul Lipton, computer Associates		Visit www.sys-con.com for details		
(XM10) XQuery Mike Champion, Software AG		(VN10) Model Driven Development of Web Services in UML for the J2ME Bill Graham, Rational Software	 9:00AM – 5:00PM Java 2 Platform Architect Certification Fast Path This intense one-day session helps prepare attendees to pass the Sun Certified Enterprise Architect for J2EE Technology exam. This session provides an overview of the components comprising the J2EE architecture as a whole, emphasizes the incorporation of J2EE technology into an architecture, and reviews each of the certification exam's testing objectives.	 9:00AM – 5:00PM Java 2 Platform Architect Certification Fast Path This intense one-day session helps prepare attendees to pass the Sun Certified Enterprise Architect for J2EE Technology exam. This session provides an overview of the components comprising the J2EE architecture as a whole, emphasizes the incorporation of J2EE technology into an architecture, and reviews each of the certification exam's testing objectives.
(XM11) XPath & XSLT 2.0 Kurt Cagle, Cagle Communications		(VN11) Why Web Services Management? Jon Atkins, HP		
(XM12) Third Generation XML Tools Michael Leventhal, Commerce One		Visit www.sys-con.com for details		

Special Insert: Web Services Edge East Conference & Expo

Featuring FREE Tutorials, Training Sessions, Case Studies and Exposition

Java Technology Track



The Java track has been specifically designed to allow you to squeeze as much information out of

each session as possible. This track is designed for the Java developer who wishes to catch up on the latest techniques and APIs and will be led by industry-leading speakers and authors.

The Java track has been designed with you, the more experienced Java developer, in mind. We know you don't have a lot of spare time, and we've designed the track to ensure that your time is maximized and you are armed with all the necessary tools to take your development to the next level.

(JV1) Squeezing the Best Out of Java

ALAN WILLIAMSON, JAVA DEVELOPER'S JOURNAL

Tuesday March 18, 2003 9:00 A.M. - 9:50 A.M.

Java is a very powerful language, and while it offers the developer a rich array of tools, the fundamentals should not be overlooked. Improving your code at the core layer will result in great improvements in efficiency and fewer bugs. We'll look at the dos and don'ts of programming and learn lots of hints and tips that will accelerate your Java coding.



BIO: Alan Williamson is editor-in-chief of *Java Developer's Journal*. In his spare time, he holds the post of chief technical officer @ n-ary (consulting) Ltd, one of the first companies in the UK to specialize in Java at the server side. Reach him at alan@n-ary.com (<http://www.n-ary.com>). Rumor has it he welcomes all suggestions and comments!

(JV2) Testing Your Java the JUnit Way

KYLE GABHART, LEARNINGPATTERNS

Tuesday March 18, 2003 11:00 A.M. - 11:50 A.M.

A critical measure of the success of software can be found in whether or not it executes successfully. Equally important, however, is whether or not that software does what it was intended to do. JUnit is an open-source testing framework that provides a simple means for developers to define their intentions for how their software should work. JUnit then provides test runners that process your intentions and verify that your code performs as intended. The result is software that not only works, but works in the correct way.



BIO: Kyle Gabhart is a senior mentor for LearningPatterns, a dynamic knowledge company providing consulting, training, and mentoring in emerging technologies. He is a prolific writer, with more than two dozen technical articles and books to his name. Kyle is highly regarded as a dynamic and enthusiastic public speaker with an innovative perspective on technology.



(JV3) Building/Deploying the Ant Way

KYLE GABHART, LEARNINGPATTERNS

Tuesday March 18, 2003 3:00 P.M. - 3:50 P.M.

A defined and easily repeatable process is one of the most necessary but often least-used aspects of good software development. A defined build process ensures that your project's software is built, deployed, and tested identically each time. Without this type of control and predictability, valuable time is often lost chasing down bugs that don't exist or rejecting solutions that were only partially implemented.

Apache's Ant is a powerful scripting tool that enables developers to define and execute routine software development tasks using the simplicity and extensibility of XML. Ant provides a comprehensive mechanism for managing software development projects, including compilation, deployment, testing and execution. Additionally, it is compatible with any IDE or operating system.

BIO: Kyle Gabhart is a senior mentor for LearningPatterns, a dynamic knowledge company providing consulting, training, and mentoring in emerging technologies. He is a prolific writer, with more than two dozen technical articles and books to his name. Kyle is highly regarded as a dynamic and enthusiastic public speaker with an innovative perspective on technology.

(JV4) Unlocking the Secrets of JDK 1.4

RAGHAVAN SRINIVAS, SUN MICROSYSTEMS

Tuesday March 18, 2003 4:00 P.M. - 4:50 P.M.

With the release of JDK 1.4, a number of new features were added to the core API, such as nonblocking IO, regular expressions, assertions, and XML. This session will take you through the major additions and demonstrate where you might use them.



BIO: Raghavan Srinivas is a Java technology evangelist at Sun Microsystems who specializes in Java and distributed systems. He has spoken on a variety of technical topics at conferences around the world, and brings with him more than 15 years of software development experience. Prior to joining Sun, Raghavan worked for Digital Equipment Corporation. He has worked in several technology areas, including internals of VMS, UNIX, and NT.

(JV5) Java APIs for Web Services Security Standards

SANG SHIN, JAVA TECHNOLOGY EVANGELIST, SUN MICROSYSTEMS

Wednesday March 19, 2003 9:00 A.M. - 9:50 A.M.

Everybody is talking about Web services as a way to perform business transactions over the Web in ways never done before. Yet, security is the most critical piece that still needs to be addressed before the promise of Web services can be realized. This session introduces the various Web services security standards, such as XML signature, XML encryption, XKMS (XML Key Management Services), XACML (eXtensible Access Control Markup Language), SAML (Security Assertion Markup Language), WS-Security, and Liberty First and their corresponding Java APIs, especially the standards APIs that are currently being defined through the Java Community Process (JCP). Wherever possible, example code will be presented.



BIO: Sang Shin has been with Sun Microsystems for over 12 years, working in various research and engineering projects mostly in data communication, networking, Internet, and Java-related areas. Prior to Sun, he worked in several startup companies in various engineering and managerial capacities. He currently teaches two graduate-level software engineering courses (XML, Distributed programming using Jini networking technology) in Brandeis University's continuing education program in Massachusetts.

(JV6) Using SWT Under Eclipse

TO BE ANNOUNCED

Wednesday March 19, 2003 11:00 A.M. - 11:50 A.M.

The release of the Eclipse project introduced a new windowing toolkit, the Standard Widget Toolkit. Discover what all the fuss is about with the Standard Widget Toolkit and why everyone is talking about it. This session will detail the underlying windowing infrastructure of the SWT Toolkit.



(JV7) Unlocking the Power of XML

HITESH SETH, *ikigo*

Wednesday March 19, 2003 3:00 P.M. - 3:50 P.M.

There is more to XML than just one block of String. Understand the difference between a DTD and a schema and the APIs you can utilize within Java that will bring the power of XML to your Java development.



BIO: Hitesh Seth is the chief technology officer of *ikigo*, Inc., a provider of XML-based Web services monitoring and management software. A freelance author and well-known speaker, he regularly writes for technology publications on VoiceXML, Web services, J2EE and Microsoft .NET, wireless computing, and enterprise/B2B integration. He is also the editor-in-chief of *XML-Journal*.

(JV8) Integrating Java and .NET

DEREK FERGUSON, *EXPAND BEYOND CORPORATION*

Wednesday March 19, 2003 4:00 p.m. - 4:50 p.m.

Two technologies that aren't often mentioned in the same breath are Java and Microsoft. However, it is the rare developer who is able to completely avoid either of these two worlds nowadays. In this presentation, we will examine several tools both free and commercial that can be used to bring these two development platforms together. Some knowledge of Java and Windows development is advisable.



BIO: Derek Ferguson is chief technology evangelist for Expand Beyond Corporation (www.xb.com), the worldwide leader in mobile software for enterprise management. He is also editor-in-chief of *.NET Developer's Journal* and author of the book *Mobile .NET*.

(JV9) Writing SOAP Services

NIGEL THOMAS, *SPIRITSOFT, INC.*

Thursday March 20, 2003 9:00 A.M. - 9:50 A.M.

J2EE 1.4 mandates the use of JMX to manage compliant products. Early adopters of JMX mostly use protocols like RMI and HTTP to communicate between the management application and the agents it is managing. This presentation describes how JMS is utilized to manage large deployments of managed agents in the Enterprise and optimize the delivery of alerts and notifications in complex environments. The processing of management alerts, using open source components (such as Jelly) to provide an Event-Condition Action (ECA) framework, will also be discussed.



BIO: Nigel Thomas joined SpiritSoft as director of product marketing in April 2001. Prior to SpiritSoft, Nigel spent five years with EAI pioneer Constellar, serving in consulting, support, sales support, and development roles. He became product architect and then director of product manage-

ment for the flagship Constellar Hub product. Nigel spent over eight years at Oracle, architecting and delivering Oracle's Accounting products and then moving on to worldwide performance consulting and CASE development assignments.

(JV10) Working with Data the JDO Way

PATRICK LINSKEY, *SOLARMETRIC*

Thursday March 20, 2003 11:00 A.M. - 11:50 A.M.

Java Data Objects is an alternative way of looking at your data compared to JDBC. Looking at your data in an object-oriented way offers many advantages over the sequential manner of JDBC. Learn how JDO can be adopted for your own requirements through practical examples.

BIO: Patrick Linskey manages and drives SolarMetric's technology development as vice president of Engineering. Patrick has been intimately working with JDO for nearly two years and has been involved in object/relational mapping for over four years. Over the past year, Patrick has evangelized the JDO specification at local Java User Groups and software symposiums throughout the world.

(JV11) Enterprise: The Next Generation

MARK HAPNER, *SUN MICROSYSTEMS*

Thursday March 20, 2003 3:00 P.M. - 3:50 P.M.

With the latest release of the J2EE 1.4 framework, a whole new suite of APIs have been added to this already comprehensive edition. Chances are, there are goodies lurking in there you didn't even know about. This session will take a look at unearthing some of the gems of the J2EE framework.



BIO: Mark Hapner is a Sun Distinguished Engineer and is currently lead architect for Java™ 2 Platform, Enterprise Edition (J2EE™). He has guided the overall architecture for J2EE 1.2, 1.3 and now the upcoming 1.4 release. In March of 1996, he joined Sun's JavaSoftware Division to participate in the development of the Java database connectivity API (JDBC). Following that he was co spec lead of the Enterprise JavaBeans specification and spec lead of the Java Message Service specification.

Prior to his work on Java enterprise APIs, Mark was a member of Sun's Object Services Group where he wrote several of Sun's initial CORBA object services submissions and worked on the integration of object oriented and relational databases with Sun's ORB.

(JV12) Overcoming the Challenges of J2ME

DR. JEFF CAPONE, *ALIGO*

Thursday March 20, 2003 4:00 P.M. - 4:50 P.M.

J2ME has brought the power of Java to the mobile space. However, it is fair to note that not all the JDK is available to you. Discover what is and what isn't available to you and how you can potentially work around some of what seems to be "must have" tools.



BIO: Dr. Jeff Capone has devoted his career to researching wireless and wireline networks and applications. As Aligo's CTO, Jeff leads the technology development and is the principal architect of the innovative M-1 Server. Prior to leading Aligo's engineering team, he was an assistant professor at Arizona State University and director of the Network Engineering and Wireless Telecom Lab.



Web Services Track



The Web Services track focuses on issues and topics that are at the forefront of development efforts in Web services. Although the current specifications provide a minimum set of protocols, issues such as security, transaction management, service management and coordination remain in flux. This track presents some of the leading authorities in the field on these urgent topics and addresses all of the questions that currently concern designers, developers and consumers of Web services.

(WS1) Web Services Infrastructure

CARL SJOGREEN, BEA

Tuesday March 18, 2003 9:00 A.M. - 9:50 A.M.

Web services have evolved from an over-hyped vision of an interconnected world to a set of real standards and technologies that can solve real-world problems in the enterprise. Building, deploying, and managing Web services in an enterprise-class environment, however, still raises many questions about the infrastructure on which those Web services are deployed.

This session will introduce several real-world Web services case studies, the requirements placed on Web services infrastructure, and several hands-on examples of enterprise-class Web services implementations that address the issues raised above.

BIO: Carl Sjogreen is product manager for BEA WebLogic Workshop, BEA's latest Java innovation and an integrated development environment for building Web services. He has been involved with XML, Web services, and developer tools since 1998, when he founded Transformis, a software startup specializing in XML tools. Passionate about the power of XML and bringing new technologies to the masses, he is a key contributor to growing the BEA WebLogic development community.

(WS2) Web Services Management

JAMES PHILLIPS, ACTIONAL

Tuesday March 18, 2003 11:00 A.M. - 11:50 A.M.

Service-oriented architectures (SOAs) have been held out for years as a substantially more cost-effective and flexible approach to architecting enterprise software systems than historical strategies such as monolithic system design or tightly coupled client/server approaches. Many customers and industry observers believe Web services technology finally makes possible the widespread adoption of the SOA approach. But while Web services and SOAs substantially ease the application development and integration burden, they bring with them a new collection of management challenges. In this session, you will learn about the essential management criteria for growing and sustaining a "mission-critical" service-oriented architecture.



BIO: In his role at Actional, James has worldwide responsibility for Actional's product and market strategy and market execution. Prior to joining Actional, he served as CSO and vice president of product marketing and business development with Ensim Corporation. James is a frequent speaker and editorial contributor on Web services-related issues and serves on the international advisory board of *Web Services Journal*.

(WS3) Strategies for Using Databases in a World of Web Services

MIKE LEHMANN, ORACLE

Tuesday March 18, 2003 3:00 P.M. - 3:50 P.M.

Databases continue to be at the core of most IT infrastructures yet the knowledge of how they play in the world of SOAP-based Web services is less well understood. This presentation covers strategies for publishing database components as Web services and, as important, techniques for consuming Web services within databases. Find out how to plug your database infrastructure into the world of Web services.

BIO: Mike Lehmann has worked in the IT industry for over 12 years as a developer,

consultant, and project manager in emerging technologies. His current areas of focus include J2EE and Web services. Mike frequently authors articles and papers on Web services and speaks regularly at industry events.

(WS4) Using Web Services to Integrate J2EE and .NET Enterprise Applications

ODYSSEAS PENTAKALOS, PH.D.,

SYSNET INTERNATIONAL, INC.

Tuesday March 18, 2003 4:00 P.M. - 4:50 P.M.

The Web services phenomenon promises to resolve all interoperability issues through an open architecture that is based on widely accepted industry standards such as SOAP, WSDL, and HTTP. This session will explore component reuse across the two major enterprise application platforms, J2EE and .NET, using Web services as the medium of interaction. Through examples, this tutorial will cover the current state of interoperability between J2EE and .NET and will focus on best practices and issues that arise. The Axis SOAP implementation will be used in this session as the Web services platform for exposing J2EE components.



BIO: Odysseas Pentakalos is vice president of SYSNET International, Inc., where he focuses on architecture, design, and development of large distributed systems that utilize Java and J2EE technologies. He holds a Ph.D. in computer science, is the author of the *Windows 2000 Performance Guide*, has published over two dozen papers in conference proceedings and journals, and is a frequent speaker at industry conferences.

(WS5) Combining BPM and BRM Technologies: A Major Step Towards Corporate Agility

HENRY BOWERS, ILOG

Wednesday March 19, 2003 9:00 A.M. - 9:50 A.M.

Corporate agility: the ability to quickly respond to unexpected change inside and outside the corporation, is a coveted quality of the modern enterprise. This presentation discusses how corporate agility is driven by technical agility. It introduces business rule management (BRM), business process management (BPM), and Web Services technologies, and explains how together these technologies provide an enabling foundation for technical agility.



BIO: Henry Bowers has spent more than 15 years in the high-tech sector, building and managing software products for both private industry and government. He has more than 7 years' experience working with rules-based systems and business rules in general. Henry is currently a product manager for business rules at ILOG.

(WS6) Web Services for Real-Time Data Access in an Industrial Setting

STEPHAN VAN DIJCK, ABB/SKYVA

Wednesday March 19, 2003 11:00 A.M. - 11:50 A.M.

Real-time processes deliver and require data in order to participate in business transactions. We will present an application under development at ABB for linking real-time process control with business processes via Web services, and explore how plant floor control can be a consumer and producer of Web services. We will use solutions from ABB, IBM WebSphere, and Microsoft .NET.



BIO: Stephan Van Dijck holds a master's degree in engineering mechanics from K.U. Leuven, Belgium, and a degree in business management from I.A.G. U.C., Louvain, Belgium. He has worked as a process engineer at the EXXON facility in Antwerp, Belgium, where he supervised logistics planning and optimization of loading and unloading operations with Honeywell Europe as an application and software development manager, product line marketing manager for Batch control systems, and marketing manager for the chemicals and pharmaceuticals business unit Europe. In 1998 he joined SKYVA, a provider of e-manufacturing solutions by making use of Web services.

(WS7) Web Services Architecture: The Next Big Spec, from the Mouths of the W3C Authors

ERIC NEWCOMER, IONA (MODERATOR)

Wednesday March 19, 2003 3:00 P.M. - 3:50 P.M.

The World Wide Web Consortium (W3C) was created to develop interoperable technolo-

gies and to provide an open forum for discussion about the future of the Web. A significant effort currently underway within the W3C's Web Services Activity is the development of a Web Services Architecture Specification to help guide the future direction of Web services.

This panel session will discuss the role of the W3C in the development of Web services standards through this effort. The panel includes coauthors of the working group and editors of the spec, with representatives from BEA Systems, Contivo, IBM, IONA, and Software AG. Providing conference attendees with an opportunity to learn more about what the W3C is doing with regard to Web services, this panel will demonstrate the benefits and examine the challenges of working together to develop an open standard architecture.



BIO: In the role of chief technology officer at IONA, Eric is responsible for IONA's technology roadmap and the direction of IONA's Orbix E2A e-Business Platforms as relates to standards adoption, architecture, and product design. Eric joined IONA in November 1999, and most recently served as IONA's vice president of engineering, Web Services Integration Products. Eric is a member of the XML Protocols and Web Services Architecture working groups at the W3C and IONA's Advisory Committee representative to UDDI.org.

(WS8) – Web Services: The Next Steps After the Hype

CLAIRE DESSAUX, ORACLE

Wednesday March 19, 2003 4:00 P.M. - 4:50 P.M.

Because Web services are still very new, many companies have yet to understand what Web services mean for their line of business and how they can make the most of this evolutionary technology. This session will highlight real-life examples where Web services have been successfully implemented and examines where services make sense, especially as they relate to integration. It will conclude with recommendations on how to best plan for a Web service strategy.



BIO: Claire Dessaux joined Oracle Alliances in 1994 with a main focus on helping partners implementing Oracle technology. Since then she has worked in various capacities on the incorporation of J2EE, XML and Web services into Oracle's product lines.

(WS9) Best Practices for Web Services Development

CHRIS PELTZ, HP

Thursday March 20, 2003 9:00 A.M. - 9:50 A.M.

There has been a fair amount of hype around Web services and the benefits they can bring to an organization. For many, it is difficult to determine how to best get started with Web services. This talk will outline a number of first steps that can be taken to begin planning a Web services pilot. It will also address a series of design guidelines, patterns, and architectural recommendations to enable an organization to build robust, flexible, and secure services. The talk will conclude with a look at tips and techniques for developing, testing, and managing Web services.



BIO: Chris Peltz is a senior software consultant within HP's Developer Resources Organization. He provides technical and architectural consulting to enterprise customers on J2EE, Web services, and mobile development. Chris has over 10 years of software experience in object-oriented technologies, 4GL development, GIS, and Web applications design.



(WS10) Web Services Startups: Telltale of the Future

SIMEON SIMEONOV, POLARIS VENTURE PARTNERS

Thursday March 20, 2003 11:00 A.M. - 11:50 A.M.

You must have seen them; they're everywhere. Web services startups are popping up like mushrooms after rain. Or has the Web services hype created a microcosm of startup activity that is going to mirror the boom and bust cycle of the late '90s? As a Web services technologist, where should you focus your energies? As a customer, how should you choose your vendor? As an investor, where should you put your money to work? In this presentation you'll get an overview of startup activity in the Web services space within the context of emerging industry dynamics and evolving customer needs. We will cover Web services tools, appliances, runtimes, integration, security, testing, and management.



BIO: Simeon Simeonov is a principal at Polaris Venture Partners, a leading early-stage venture firm, where he focuses on investments in information technology. Prior to joining Polaris, Sim was chief architect and vice president of emerging technologies at Macromedia, where he led the development of Web services technologies and platform infrastructure for next-generation Internet applications. Prior to that, he was a founding member and chief architect at Allaire, where he was responsible for the ColdFusion application server and cross-product technology strategy.

(WS11) Open Standards for Web Services Messaging

DAVE CHAPPELL, SONIC SOFTWARE

Thursday March 20, 2003 3:00 P.M. - 3:50 P.M.

Web services hold the promise of driving down the cost and complexity of application integration both between internal systems and between business partners. But unless Web services communications are made reliable, organizations will not be able to trust them for mission-critical operations, such as complex business-to-business transactions or real-time enterprise integration.

In this session, Dave Chappell, a coauthor of the WS-Reliability specification, will examine the emerging Web services reliability standards, including a detailed discussion on WS-Reliability, a new specification for open Web services messaging.



BIO: Dave Chappell, vice president and chief technology evangelist for Sonic Software, has over 18 years of experience in the software industry covering a broad range of roles including R&D, code-slinger, sales, support, and marketing. Dave has a strong passion for shaping the future of technology and enjoys sharing his knowledge and experience with others.

(WS12) – Web Services Security

MARC CHANLIAU, NETEGRITY

Thursday March 20, 2003 4:00 P.M. - 4:50 P.M.

Web services deployments typically use transport-level security for authentication and application-based access control for authorization. This presentation shows the limitations of transport-level security and introduces the XML technologies that complement the transport-level approach to provide a secure authentication solution. This presentation also covers the issues involved in providing access control in back-end applications and suggests a better, centralized approach to abstract authorization information out of back-end applications and into a single point of control using XML-based query technologies.

BIO: Marc Chanliau is a product manager for Netegrity, Inc. He has been in the software industry for over 20 years in many different capacities. Marc started the OASIS Security Services Technical Committee which culminated in the adoption of SAML as an official OASIS standard in November 2002. He holds an MS in linguistics from the University of Paris-Jussieu, France.



Microsoft .NET Track



Microsoft .NET represents a major evolution in how applications are developed, deployed, and managed on the Microsoft platform. The .NET Framework gives developers an object-oriented development environment for building all types of applications, including desktop, client/server, dynamic Web page, wireless devices, server-based as well as complete support for XML Web services and the related XML standards. The sessions in the .NET Track will give you a broad as well as deep understanding of the capabilities in the .NET Framework and how applications built on .NET are easily integrated with applications running in heterogeneous environments, including main-frame, UNIX, and J2EE platforms.

development department and created several client/server application and system software products. Russ's specialties include development with VB.NET, XML Web services, ASP.NET, and debugging.

(NT3) Introduction to VB.NET

RUSS FUSTINO, MICROSOFT

Tuesday March 18, 2003 3:00 P.M. - 3:50 P.M.

Looking to learn the latest release of Visual Basic, VB.NET? Wait no longer and jump right in! See first hand why VB is the language of choice for developers. Whether you are changing from another language or just re-tooling, make sure you hit this session. You won't regret it! We will cover the Visual Studio Integrated Development Environment, Win Forms, Web forms and ASP.NET, classes and objects, XML Web services, ADO.NET introduction for data access and debugging.

BIO: Russ Fustino is a Microsoft Principal Technology Specialist and a Microsoft Certified Professional with over 20 years of software development experience. He has an expertise in developing Visual Basic and Web-based solutions using Microsoft tools. Prior to Microsoft, Russ was a VB instructor, headed up a development department, and created several client/server application and system software products. Russ's specialties include development with VB.NET, XML Web services, ASP.NET, and debugging.

(NT1) .NET Framework Overview

BOB FAMILIAR, MICROSOFT

Tuesday March 18, 2003 9:00 A.M. - 9:50 A.M.

This session will introduce the architecture and technologies within the .NET Framework, including the Common Language Runtime, ASP.NET, and ADO.NET, as well as XML and SOAP support. Integration with COM and COM+ services will be covered, as well as a discussion of the .NET Framework SDK.



BIO: Bob Familiar is a Microsoft Architectural Engineer and Certified Microsoft Solution Developer with over 14 years of experience in software engineering. He has developed solutions in C, C++, Java, SQL, and Visual Basic, and has over 7 years of experience using Microsoft Development Tools. Bob holds a patent for technology that maps relational database tables to object-oriented software components. His current areas of interest include object oriented analysis and design of distributed object models and distributed computing using COM+.

(NT4) How to Develop an End-to-End .NET-Connected Application

ALLAN DE COSTA PINTO, MICROSOFT

Tuesday March 18, 2003 4:00 P.M. - 4:50 P.M.

This session will show you how to design and create a sample application using multiple Microsoft .NET Enterprise Server products. We will show you how to integrate .NET technologies into an effective solution. The following products and technologies will be covered in this session: VS.NET, ASP.NET, VB.NET, C#, XML Web services, BizTalk, and SQL Server 2000. (Note: The demos in this session have been updated for VS.NET RTM version.)



BIO: Allan da Costa Pinto is a Microsoft Certified Application Developer for .NET and works for Microsoft Consulting in the Connecticut Area. Allan focuses on architecting and building solutions using Microsoft Visual Studio® .NET and XML Web services.

(NT2) Introduction to ASP.NET

RUSS FUSTINO, MICROSOFT

Tuesday March 18, 2003 11:00 A.M. - 11:50 A.M.

We will look at the next version of Active Server Pages, ASP.NET, a major upgrade to the current version of ASP. Xcopy deployment; control-based encapsulation; clean separation of code from HTML; strongly typed, compiled languages; and event-based page processing will change the way you develop UI for server-based Web applications. This session covers the ASP.NET Page Framework from the ground up: architecture; ASP.NET syntax; server controls; control families: intrinsic controls, list controls, and rich controls. Finally, this session will cover business objects, Web services, and migration issues.



BIO: Russ Fustino is a Microsoft Principal Technology Specialist and a Microsoft Certified Professional with over 20 years of software development experience. He has an expertise in developing Visual Basic and Web-based solutions using Microsoft tools. Prior to Microsoft, Russ was a VB instructor, headed up a

(NT5) .NET, the Virtualized Execution Engine

YAHYA MIRZ, AURORA BOREALIS

Wednesday March 19, 2003 9:00 A.M. - 9:50 A.M.

With .NET, Microsoft has introduced a major evolution in their computing platform. At the core of .NET, is a language agnostic runtime, currently being standardized by ECMA. This effort is called the Common Language Infrastructure or the CLI. The objective of this presentation will be to provide insight into the design decisions that led to the CLI's Execution Engine and their rationale. Additionally, I will explain through an example, how a component works its way through the Virtualized Execution Engine of the CLI.

BIO: Yahya Mirza is striving to balance commercial development with component-based language research. Since 1999, Mr. Mirza has been working on .NET projects at Microsoft, Source Dynamics and Safeco Life. His passion lies in language design for music and computer animation.

(NT6) Introduction to DotGNU

BARRY FITZGERALD, DOTGNU

Wednesday March 19, 2003 11:00 A.M. - 11:50 A.M.

This session will feature a brief overview of the many GNU projects currently implementing and extending ECMA CLI standards. These projects include SEE, phpGroupWare, Portable.NET, Web Services, and Virtual Identities.

BIO: Barry Fitzgerald is one of the cofounders of the DotGNU Free Software Project to create a 100% open source GNU implementation of the ECMA Common Language Infrastructure (CLI). He is also a member of the Steering Committee for DotGNU.

(NT7) Intro to SSCLI

YAHYA MIRZ, AURORA BOREALIS

Wednesday March 19, 2003 3:00 P.M. - 3:50 P.M.

In early 2002, Microsoft released a "Shared Source" implementation of the .NET





Common Language Infrastructure available on BSD UNIX, Linux, Mac OSX, and the Windows platform codenamed "Rotor". For enthusiasts, Rotor provides an opportunity to understand the .NET technology at a deeper level. For language designers, Rotor can serve as an effective runtime core for experimentation at the language feature level. For compiler and virtual machine researchers, Rotor provides a context for applied research into alternative object representations, method dispatch, garbage collectors, JIT compilers, etc. My goal will be to provide an introduction into the Rotor code base.

BIO: Yahya Mirza is striving to balance commercial development with component-based language research. Since 1999, He has been working on .NET projects at Microsoft, Source Dynamics and Safeco Life. His passion lies in language design for music and computer animation.

(NT8) Mobile Development with the Compact Framework

BRAD MCCABE, INFRAGISTICS

Wednesday March 19, 2003 4:00 P.M. - 4:50 P.M.

With the release of the Compact Framework, Microsoft has brought mobile development to the masses. In this session we will look at some of the differences and similarities between the .NET Framework and the Compact Framework. We will also examine the consideration that must be factored into the architecture and development of mobile application such as dealing with user interface considerations and effective mobile data strategies



BIO: Prior to joining Infragistics, Brad McCabe served as systems architect for the network solutions development team at Verizon Communications. Concurrently, Brad held the position of lead .NET Evangelist within Ajilon Consulting and was responsible for content and delivery of material for the national Inside .NET tour. Brad has been working as a senior developer and a software engineer, and his current responsibilities include developing reference applications and working with enterprise customers on project implementation.

(NT9) Best Practices for .NET Development

JOE STAGNER, MICROSOFT

Thursday March 20, 2003 9:00 A.M. - 9:50 A.M.

This advanced session covers the wide array of best practices for the most productive .NET development topics. We'll start with an overview of design guidelines for .NET, ensuring that developers write consistent, predictable code that integrates well between languages. We will cover memory management and the garbage collector as well as the best methods for cleaning up unmanaged resources. A section will cover how to best use ADO.NET to access relational data, and how to assimilate that data with the .NET XML classes. We'll look at tips for creating both components and controls, how to best use the System.NET classes to access HTTP responses, the .NET threading model, and key security concepts will also be examined.



BIO: Joe Stagner is a technical evangelist of Developer Technologies at Microsoft, and has been developing software for 25 years, on Microsoft platforms since DOS 1.0. Joe currently focuses on helping Microsoft's Independent Software Vendors make the most of .NET Developer technologies and also works with medium business developers and the academic community in New England.

(NT10) Best Practices for ADO.NET Development

THOM ROBBINS, MICROSOFT

Thursday March 20, 2003 11:00 A.M. - 11:50 A.M.

One of the biggest changes in data access recently is that common clients and servers on the Internet work in a disconnected, stateless fashion. ADO.NET provides an optimized, XML-based framework for data access in a disconnected environment. With the advent of XML, programming for data access and manipulation, the mechanism is changing from a relational to a hierarchical form. ADO.NET classes read and write XML at their core. The ADO.NET framework fully supports disconnected reads and writes, and we'll discuss the performance implications of this as well as how to use different types of objects in their various states. ADO.NET also has classes that provide optimized performance with SQL Server or other OLE DB data sources. This session covers the best practices on how to handle data access for best performance, error handling, transaction support, and security. We'll discuss the best practices for retrieving, single item, single row and multiple rows of data as well as transaction handling, and look at examples of the performance differences in using DataReaders versus DataSets. This session will also cover the best ways to cache data from data sources and the transformation to XML.



BIO: Thom Robbins is a senior technology specialist with Microsoft. He is a frequent contributor to various magazines include .NET, Visual Studio.NET and the Web Services Journal. Thom is also a frequent speaker at a variety of events that include VS Live and others. When not writing code and helping customers, he spends his time with his wife at their home in New Hampshire.

(NT11) How to Debug with .NET

TOBY DENBOW, STAR IT

Thursday March 20, 2003 3:00 P.M. - 3:50 P.M.

This session shows how the rules for debugging have completely changed with the advent of Microsoft .NET Framework. It will cover the core debugging concepts using the Microsoft .NET Framework. In addition, this session will discuss many advanced features that allow you to write better diagnostic and error-handling code.

BIO: Toby Denbow is VP of technology at STAR Information Technology. He has been a featured speaker at several Microsoft and industry trade shows. Toby has been working with .NET for over a year and was trained directly by the .NET developers in Redmond. He works with a wide variety of customers in various emerging technologies and has personally trained over 500 developers on Visual Studio.NET.

(NT12) XML and Web-Enabling Legacy Applications Using BizTalk

MIKE CRAMER, SENIOR PRINCIPAL TECHNOLOGY SPECIALIST, MICROSOFT

Thursday March 20, 2003 4:00 P.M. - 4:50 P.M.

This session examines how to integrate legacy line-of-business applications using BizTalk 2000 Server. It will examine BizTalk Server tools that allow you to create the components necessary to interface to legacy systems. This includes a scenario with four phases that demonstrates integration by using industry-standard XML and EDI file formats, delimited and positional files, and COM bridges.

BIO: As a member of the New England BSG Team and focusing on integrating heterogeneous applications, Mike Cramer works with existing and prospective Microsoft customers in New England on adopting the .NET platform. Mike joined Microsoft during the 1995 acquisition of Netwise Inc. (Boulder, CO). Prior to the acquisition, Mike worked for Netwise for approximately three years as a consultant and later consulting manager.



XML Technology Track



Whether you're looking to understand different XML standards, application techniques, or development tools; or using XML to develop the next generation of Web applications and services, the XML Track is your ultimate training, collaboration, and innovation ground. Sessions include fast-track, in-depth training on XML Schemas and XSL-FO. We will update you on standards development and offer a comprehensive review of the various technologies related to XML that are essential for today's IT manager. The XML Track is armed with real-world applications of XML in financial services, life sciences, enterprise and B2B integration, and mobile computing. We will discuss new developments around XForms, a recent W3C Standard which marks another era of standards-based application development; XPath and XSLT 2.0 XML; and Query.

The XML Track explores the technology and standards, real-world applications, and trends which will set the course for the future.

(XM1) XML: A Manager's Guide

JP MORGENTHAL, SOFTWARE AG

Tuesday March 18, 2003 9:00 A.M. - 9:50 A.M.

This session will provide an essential introduction to XML from a manager's perspective. As more and more IT projects utilize XML and its derivatives as fundamental technologies, it is key for today's manager to be aware of the various ingredients of XML. From core XML processing, transformation, metadata definition and schemas, applications in Web, wireless and speech applications, Web services, industry-standard vocabularies, and more, the session will offer a comprehensive review of the various technologies related to XML that today's IT Manager must be aware of.



BIO: JP Morgenthal serves as the chief services architect for Software AG, Inc. He is an internationally prominent authority on XML with more than 15 years of experience designing, developing, and analyzing software and technology. In his role as chief services architect, JP will explore and manage the design of complete professional services solutions based on Software AG technology and partner products in existing and emerging industries.

(XM2) OASIS Standards Update

KARL F. BEST, OASIS

Tuesday March 18, 2003 11:00 A.M. - 11:50 A.M.

OASIS is a not-for-profit, global consortium that drives the development, convergence, and adoption of e-business standards. Members of OASIS are providers, users, and specialists in standards-based technologies, and include organizations, individuals, and industry groups. The OASIS standards process can best be described as open, lightweight, and independent.

This session will address, OASIS Initiatives, current TC status, OASIS Technical Agenda, collaborative work at OASIS, EbXML, ISO/IEC/ITU/ECE Memorandum of Understanding (MoU) for electronic business, standards, liaison memberships in various ISO TCs and ISO/IEC JTC1 SCs and more ongoing, sponsor of Interoperability Summit, vendors submit specs to OASIS, dot-orgs move to OASIS, convergence at OASIS, and current Technical Committees.



BIO: Karl F. Best is the director of technical operations for OASIS, where he is responsible for managing the consortium's industry standards efforts. He is a former chief strategy officer and board member of the consortium, and has been involved in the XML/SGML industry since the early 1990s. Karl has been a member of a number of industry standards committees for SGML, XML, and associated standards, and a speaker at many industry conferences. He was previously employed by Novell, Adobe, and Sun Microsystems, designing and implementing electronic documentation systems.

(XM3) A Definitive Introduction to XML Schemas

HITESH SETH, IKIGO

Tuesday March 18, 2003 3:00 P.M. - 3:50 P.M.

XML Schemas have emerged as the standard way of representing XML vocabularies. Schemas extend the basic mechanism for defining the structure and content of XML documents established by Document Type Definitions (DTDs) to include rich data-type information and features such as simple/complex types, extensions/restrictions, etc. Get started with XML Schema development with this introduction to the standard and best practices for XML Schema design. We will also preview how XML Schema compares to RELAX NG.

BIO: Hitesh Seth is the chief technology officer of ikigo, Inc., a provider of XML-based Web services monitoring and management software. A freelance author and well-known speaker, he regularly writes for technology publications on VoiceXML, Web services, J2EE and Microsoft .NET, wireless computing, and enterprise/B2B integration.

(XM4) XML in Print: XSL-FO

FRANK NEUGEBAUER, IBM

Tuesday March 18, 2003 4:00 P.M. - 4:50 P.M.

Today developers frequently use XSLT to convert XML into markup languages such as HTML. XSL Formatting Objects (XSL-FO) promises to abstract the details of rendering and allow developers to specify the layout and semantic properties of presentation regardless of rendering. This presentation will provide a thorough introduction to XSL-FO and how it relates to the other XML processing standards and will highlight the benefits of XSL-FO in XML application development. Using demonstrations, the session will highlight the features that XSL-FO provides for creating an open standards-based print process and its applications.



BIO: Frank Neugebauer is a consultant in the Insurance Solutions division of IBM Global Services, specializing in distributed Java solutions based on IBM's Insurance Applications Architecture (IAA). He is also a freelance writer and has contributed several articles to leading industry publications.

(XM5) XML Security Integration Challenges

PHIL STEITZ, AMERICAN EXPRESS

Wednesday March 19, 2003 9:00 A.M. - 9:50 A.M.

This session will highlight the key security integration challenges faced by application teams developing enterprise solutions using loosely coupled, XML-based interfaces and service-oriented architectures. We will discuss how emerging standards and technologies address the practical security problems faced by development teams, the gaps that still remain, and the tradeoffs and compromises that architects and developers need to make to implement secure solutions today.

BIO: Phil Steitz is vice president, e-commerce applications development, at American Express. He has over 20 years of experience as a developer, architect, and technology leader involved in distributed systems development. Before joining American Express, Phil served as a middleware architecture consultant, designing large-scale distributed systems for enterprise customers. He holds a PhD in mathematics from the University of Maryland.



(XM6) Case Study: XML in the Life Sciences

TIM MATTHEWS, IPEDO

Wednesday March 19, 2003 11:00 A.M. - 11:50 A.M.

The importance of XML-based information in the health care and biotech industries has grown tremendously over the last two years, from R&D to clinical trials to manufacturing. Life sciences companies today are required to transfer and share huge quantities of information among the myriad of researchers and partners involved in the product development life cycle. The future of the life sciences market will be influenced by how well companies acquire, share, and apply knowledge to exploit the wealth of new opportunities while minimizing the deluge of new risks and costs. This session will provide a case study of how one life sciences company is implementing XML for a competitive advantage. It will also discuss how XML Management technology was used to provide scientists and analytic applications with the ability to efficiently search and analyze the data using sophisticated queries.



BIO: Tim Matthews has extensive experience in high-tech engineering, marketing, and sales. Prior to cofounding Ipedo in 2000, he was director of product marketing at RSA Security, where he oversaw a line of developer security products and a line of security infrastructure servers. Previously, Tim worked in international sales and business development at Digital Equipment Corporation in Tokyo and Irvine, California.

(XM7) Using XML for EAI: Best Practices

DAN ENACHE, TIBCO SOFTWARE

Wednesday March 19, 2003 3:00 P.M. - 3:50 P.M.

According to Gartner Group, EAI is the hottest IT market. Even in a slow economy, the EAI market is expected to grow at a steady pace, faster than most of the other sectors. How can you take advantage of EAI and help your company reap the benefits? What are the best practices in using XML to implement large EAI systems? What are the pros and cons in using XML as a "lingua franca"? How are people in the trenches using XML and EAI to build systems that work?



BIO: Dan Enache is a senior software architect for TIBCO Software. He is an expert in large integrations both in the EAI space and on the Web, as well as large portals and Single Sign-On integration solutions. Dan has extensive experience with high volume/high availability transactional/financial systems, and a great deal of expertise in implementing large security systems. He is a J2EE developer and Sun Java Architect.

(XM8) Delivering Web Services to Mobile Clients with XML Transformation Frameworks

PAUL LIPTON, COMPUTER ASSOCIATES

Wednesday March 19, 2003 4:00 P.M. - 4:50 P.M.

Much of the discussion on Web services focuses on the server side, but careful consideration of the delivery of Web services to client platforms is also necessary. Important technology and business trends will increase the diversity of client platforms, and will require that you consider mobile devices at the earliest stages of design. In fact, proper visualization, aggregation, and delivery of Web services in the new world of highly variable client platforms will be essential for the ultimate success of many projects.



BIO: Paul Lipton is the Web services technology leader for the field services organization and a technology strategist in the Office of the CTO. He has been an architect and developer of enterprise systems for more than 20 years, and has worked closely with key CA customers to architect distributed solutions using J2EE, .NET, wireless, and Web services technology.

(XM9) XML, Ontologies & the Semantic Web

AYESHA MALIK, OBJECT MACHINES

Thursday March 20, 2003 9:00 A.M. - 9:50 A.M.

The Semantic Web has generated much talk ever since Tim Berners-Lee, the inventor of the World Wide Web, first mentioned it a few years ago. Get the architecture details behind a Semantic Web. In particular, the session links the study of ontologies for modeling knowledge representation with the requirements of a Semantic Web. Track W3C's standardization activity in building XML standards for the Semantic Web including and RDF and OWL (Web Ontology Language).



BIO: Ayesha Malik is a senior consultant for Object Machines, a software engineering firm providing Java technology and XML solutions to businesses. Ayesha has worked extensively on large XML and messaging systems for companies such as Deutsche Bank and American International Group (AIG). Most recently, she has been researching new ways to make schemas extensible and object oriented.

(XM10) XQuery

**MIKE CHAMPION, RESEARCH AND DEVELOPMENT
SPECIALIST, SOFTWARE AG**

Thursday March 20, 2003 11:00 A.M. - 11:50 A.M.

As the ubiquitous data description and encapsulation standard, XML has quickly evolved into a container for all kinds of data. It is imperative that a standardized and flexible query and processing language be available to utilize the immense wealth of data that XML stores represent. Currently, even though established standards such as XSLT/XPath are available for transforming XML documents, the development around XQuery language has demonstrated the need for a flexible language for extracting data from XML documents. This session provides an introduction to XQuery language and illustrates its application through real-world scenarios.



BIO: Michael Champion is a research and development specialist at Software AG, working out of Ann Arbor, Michigan. He has been a software developer in the USA for 20 years, working primarily in the area of middleware for client/server document and image management systems. He has been active in the W3C's Document Object Model (DOM) Working Group for more than three years and was an editor of the core XML portion of the DOM Level 1 Recommendation. He is now cochair of the Web Services Architecture Working Group.

(XM11) XPath & XSLT 2.0

KURT CAGLE, CAGLE COMMUNICATIONS

Thursday March 20, 2003 3:00 P.M. - 3:50 P.M.

XPath and XSLT 1.0 are about to get a face-lift. Most of the improvements to the languages center on support for XML Schema, XML's official type system, although there are other compelling improvements that make the languages more usable as well. We'll walk you through "what's new" in both XPath and XSLT 2.0 and provide several examples using a reference implementation.



BIO: Kurt Cagle is the president of Cagle Communications, a consulting firm specializing in XML-related technologies, and is the author of 14 books on XML, XSLT, XQuery, and SVG. He is a columnist for *XML Magazine*, and publishes an e-newsletter that can be subscribed to from The Metaphorical Web.

(XM12) Third-Generation XML Tools

MICHAEL LEVENTHAL

Thursday March 20, 2003 4:00 P.M. - 4:50 P.M.

XML has become the ubiquitous infrastructure for Web services and a host of other software applications. The tools for building XML applications have progressed from the first generation of "hackerware" to a mature second generation of public and private domain tools providing SAX and DOM programming interfaces, robust parsing, well-formed and validation checking, and transformation with XSLT. Is there anything more to come? This presentation looks at two areas where interesting, third-generation tools are beginning to emerge: XML programming objects and streaming. With XML programming objects developers deal directly with document-specific classes derived from XML Schemas rather than generic document structures, as in the DOM or document events in SAX. JAXB reference implementation and Castor are two tools in this area, but there are also interesting developments coming that tightly mesh XML objects into programming languages. Streaming is based on the event model of XML parsing but goes beyond SAX with sophisticated techniques for analysis and processing of XML documents with ultra-low memory usage and high throughput. Streaming is being used in SOAP processors, search engines, entity resolvers, and transformation tools. Examples include the STX and XST transformation engines, Apache AXIS, and sequential XPATH implementations. At the end of this session we'll discuss ideas for next-generation XML tools.



BIO: Michael Leventhal led the team that architected and developed a document-style SOAP framework for Commerce One. He has led numerous projects in the area of Web applications and infrastructure and XML (and SGML) over the last 10 years and wrote the first book on XML software development for the Internet in 1998.

(VN2) The XMLSPY 5 Enterprise Edition Development Environment

TRACE GALLOWAY, CORPORATE SALES MANAGER, ALTOVA

Tuesday March 18, 2003 11:00 A.M. - 11:50 A.M.

XML-related technologies have begun to reach critical mass in many areas of business today. From e-commerce solutions to data integration initiatives to content authoring and publishing, XML related technologies are being used to meet many of the present and future business challenges. Altova™'s XMLSPY 5 Enterprise Edition Development Environment is ideally suited to meet the needs of developers, Web designers, and line of business users that are required to develop and work with XML related technologies. XMLSPY 5 Enterprise Edition is the industry-standard XML Development Environment for designing, editing, and debugging enterprise-class applications involving XML, XML Schema, XSL/XSLT, SOAP, WSDL and Web Services technologies. It is the ultimate productivity enhancer for J2EE, .NET and database developers. In this presentation, attendees will be introduced to many of the features available in the Development Environment.



BIO: Trace Galloway is the corporate sales manager at Altova, Inc, creators of XMLSPY, the award-winning and industry-leading tool suite for XML. Prior to joining Altova, Trace served as the chief evangelist for Infoteria Corporation, a global technology company specializing in the development of B2B-centric, XML-based servers and components. He has presented at numerous industry conferences including Web Services Edge New York, XML Conference Baltimore, and ASP.NET & XML Web Services Solutions Conference. He was co-author of a chapter entitled "Lead Tracking by Web and Email" in the *XML Handbook* Third Edition.

(VN3) SOAP and Java: Marrying Them Off

ALEXANDER MARLER, PARASOFT

Tuesday March 18, 2003 3:00 P.M. - 3:50 P.M.

SOAP is a lightweight, XML-based protocol for exchanging structured and typed information between peers in a decentralized, distributed environment. Although SOAP strives to be agnostic with respect to programming languages, some languages facilitate working with SOAP better than others. The combination of Java's strong typing system and its reflection API make Java especially conducive to implementing SOAP-based Web services. The presentation will explore how Java facilitates the automation of activities such as WSDL (Web Services Description Language) generation and SOAP deployment. It will also discuss how these features are influencing the development of Java-based SOAP tools.



BIO: Alexander Marler, software technical consultant, joined Parasoft to provide technical pre and post sales support along with business development for specific product lines. He has over 15 years of sales and technical expertise in the high tech industry. He has been responsible for product and business development at Sybase Inc., Charles Schwab, and Hunt-Wesson Foods. Marler received his Bachelor of Science in Management Information Systems from Washington State University.

(VN5) Process-Centric Enterprises: The Coming Revolution in Web Services-Driven Business Analytics

ERIC PULIER, CHAIRMAN AND CEO, DIGITAL EVOLUTION

Wednesday March 19, 2003 9:00 A.M. - 9:50 A.M.

As major companies transition to Web services and the Service Oriented Architecture (SOA), they are beginning to tap into the SOAs ability to provide greater visibility into business operations in real time. This presentation will explore how exposing the IT functions of a given business process as Web services makes it possible to monitor the activities of that process, even if the process occurs across multiple lines of business and IT systems. The result is what Mr. Pulier terms the "Process-centric" enterprise, which benefits from the functionality of integrated applications and systems without the rigid, time-consuming, and costly process of actual application integration. This session will address these issues and others as he lays out his vision of where enterprise computing is heading.



BIO: Recently named one of 30 e-Visionaries by VAR Business, Eric Pulier is a popular speaker at many elite technology conferences. As CEO and founder of Digital Evolution, he drives the operations and strategic vision of a company that is making the service-oriented architecture revolution a reality. Pulier has been a pioneer in the interactive industry for over 15 years. In 1997, the Presidential Inaugural Committee selected Mr. Pulier to create and execute the Presidential Technology Exhibition in Washington, D.C. He is a graduate of Harvard University.

(VN6) Pattern-Driven Application Development

TOM SHORE, SENIOR PRODUCT CONSULTANT, COMPUWARE

Wednesday March 19, 2003 11:00 A.M. - 11:50 A.M.

OMG's model-driven architecture (MDA) allows organizations to build platform and language neutral models and specifications of functionality. This approach will improve the stability, durability, and reuse of models, as they are not bound to any specific technology. Furthermore, it will boost developer productivity by increasing the code generation capabilities of development tools. As models are translated from a platform independent model (PIM) to a platform specific model (PSM), and further to an implementation (code) model, intelligent code generation engines are able to produce more and better code. Compuware's OptimaJ J2EE development tool is the only implementation of the OMG MDA so far. This presentation discusses how OptimaJ implements OMG's MDA.

BIO: Thomas S. Shore is a senior product consultant with Compuware Corporation's Application Development & Portal Solutions Software Division. Thomas joined Compuware in 1993 and held various positions before focusing on J2EE and related technologies. He has also held various software engineering and consulting positions in the manufacturing, oil & gas exploration and database software markets.

(VN7) Managing the Developer Relationship

MIKE BELLISSIMO, SUN MICROSYSTEMS

Wednesday March 19, 2003 3:00 P.M. - 3:50 P.M.

More and more vendors are developing extensive programs to capture developer interest and loyalty. These programs must adopt a philosophy of managing and enhancing the individual developer's entire experience through the life cycle of the relationship. This includes managing the developer's experience in all places where it touches the vendor. Mike Bellissimo, senior director of Sun Microsystems Software Developer Marketing and Management, will discuss how he believes developers can and should be supported with programs that help them learn, plan, evaluate, and develop their products and services.

BIO: In over a decade at Sun, Mike Bellissimo has managed sales operations for iPlanet and JavaSoft, software training and services for SunSoft, and developer programs and strategy in Sun's market development organization. Previously he managed product training for field and reseller organizations.

(VN10) Model Driven Development of Web Services in UML for the J2ME Platform

BILL GRAHAM, RATIONAL SOFTWARE

Thursday March 20, 2003 11:00 A.M. - 11:50 A.M.

Mobile and wireless clients are an integral part of the vision for Web services. The hardware computing and memory limitations of handheld and wireless devices require the use of lean-and-mean utilities to make Web services practical. This presentation looks at some of the possible solutions in the context of a typical J2ME platform. Models of possible architectures for J2ME applications are explored through the use of UML. Using models to generate code and therefore applications through Model Driven Development (MDD) are also introduced.

BIO: Bill Graham is the embedded Java evangelist at Rational Software. He has over 14 years of experience in working with real-time and embedded systems. He has presented at JavaOne, the Rational Users Conference, and the IEEE International Performance, Computing, and Communications Conference (IPCCC). Bill has a B. Eng. and a M. Eng. from Carleton University, Ottawa.

(VN11) Why Web Services Management?

JON ATKINS, HP

Thursday March 20, 2003 3:00 P.M. - 3:50 P.M.

The popularity of Web services continues to grow because they reduce integration costs and enable greater flexibility and ease in exposing applications as new sources of revenue. However, this benefit is achieved with less secure, less reliable communications. To get the most out of Web services, you must be able to manage and control the new risks that come with them. This lively and informative presentation will answer these questions and reveal the importance of developing Web services with manageability in mind.

BIO: Jon Atkins is the product manager for HP's Web Service Management Platform. He brings 10 years of marketing, sales and advertising experience, primarily in high technology.



Java UniversitySM Program: Aggressive, code-level training courses for experienced developers using Java[™] technology, brought to you by Sun Microsystems, Inc. Attend seminars designed by industry luminaries and recognized experts. Sessions cover Sun certification and Web services technology. Whether you're a beginner or a veteran developer, architect, or software engineer, you'll benefit from these value-packed full-day courses. Register now. Seating is limited.

The Java UniversitySM program complements this year's Web Services Edge conference by offering 3 full-day training lectures for experienced software developers, architects, and engineers.

Java UniversitySM Program Take-Aways:

- Training designed and presented by expert Java technology engineers
- Student guides full of source code, examples, references and copies of instructors' materials
- Free Web-based training courses from Sun Educational Services

Tuesday, March 18, 2003 Web Services Using Java[™] Technology and XML

**SANG SHIN,
SUN MICROSYSTEMS, INC.**

Who Should Attend

Web services designers and programmers, application developers, and programmers using the Java programming language who have experience using the Java[™] 2 Platform, Enterprise Edition (J2EE[™]).

Prerequisites

Experience using the Java programming language and basic knowledge of XML

Overview

This one-day seminar provides in-depth knowledge on Web services and shows how to develop Web services using the Java programming language and XML, the technologies of portable code and portable data respectively.

The session will start with an introduction on fundamental concepts and characteristics of Web services. This will be followed by a detailed explanation of how to implement, describe, register, discover, and invoke Web services using core Web services standards - Simple Object Access Protocol (SOAP); Web Services Description Language (WSDL); and Universal Description, Discovery, and Integration (UDDI). In addition, the ebXML standard, which defines the framework for the global electronic marketplace will be talked about in detail. Also, the tools for building and deploying Web services will be discussed. Each topic will be presented with concrete examples and demonstrations when possible.

Attendees will also learn how to use standard Java APIs for Web services, mainly Java API for XML Messaging (JAXM), Java technology API for XML-based RPC (JAX-RPC), and Java technology API for XML Registries (JAXR) for developing and deploying Web services.

Benefits

- Learn the fundamental concepts and characteristics of Web services. Gain detailed understanding on core Web services standards: SOAP, WSDL, UDDI.
- Gain a detailed understanding of ebXML, the standard framework for electronic business.
- Learn Java programming language APIs for Web services - JAXM, JAX-RPC, JAXR

Wednesday, March 19, 2003 Java[™] 2 Platform: Programmer Certification Fast Path

**PHILIP HELLER, PRESIDENT,
HELLER ASSOCIATES**

Who Should Attend

This session is designed for programmers who have some exposure to the Java[™] programming language, and are ready to prepare for the Sun Certified Programmer for Java 2 Platform exam.

Prerequisites

Object-oriented software development experience and familiarity with the syntax and structure of Java technology-based development.

Overview

The development community recognizes that competency developing solutions using Java technology is vital to productivity, reaffirms your value to your organization, and increases your career advancement opportunities. This session, developed and delivered by Philip Heller, author of the two leading Java technology certification preparation manuals, helps to prepare you for the Sun Certified Programmer for the Java 2 Platform exam. Philip provides code-level, detailed review of the skills and knowledge needed to confidently approach the exam.

Benefits

- Receive an intensive review of the advanced topics covered on the Sun Certified Programmer for the Java 2 Platform Exam
- Increase your understanding and knowledge of Java programming language syntax and structure
- Prepare for the exam by reviewing practice tests and questions
- Gain a strong understanding of Java fundamentals



Thursday, March 20, 2003 Java[™] 2 Platform: Architect Certification Fast Path

**SIMON ROBERTS, TECHNOLOGY
EXPERT AND COURSE DEVELOPER,
SUN MICROSYSTEMS, INC.**

Who Should Attend

This session is designed for enterprise application architects, system analysts, experienced technologists, and developers using Java[™] technology seeking certification as an architect for the Java[™] 2 Platform, Enterprise Edition (J2EE[™]).

Prerequisites

Understand the benefits of Java technology solutions; experience with object-oriented analysis and design; familiarity with concepts of distributed computing.

Overview

Many of the solutions in today's "Net economy" are, or soon will be, developed using the Java 2 Platform, Enterprise Edition (J2EE) architecture. Gaining recognized competency architecting J2EE platform-based solutions is vital to your success as an architect, reaffirms your value, and increases your career opportunities.

This intense one-day session helps prepare attendees to pass the Sun Certified Enterprise Architect for J2EE Technology exam. This session provides an overview of the components comprising the J2EE architecture as a whole, emphasizes the incorporation of J2EE technology into an architecture, and reviews each of the certification exam's testing objectives. Multiple real-world case studies are used to demonstrate correctly architected J2EE technology-based solutions and pinpoint key topics presented within the architect exam.

Additionally, you will learn how to interpret exam objectives, what each of the three exam phases contains, and clear guidelines and resources to use after the course.

Benefits

- Receive an intensive review of the topics covered on the Sun Certified Enterprise Architect for the Java 2 Platform, Enterprise Edition Exam
- Increase your understanding and knowledge of successfully architecting solutions using J2EE technology
- Understand the system qualities: scalability, availability, extensibility, performance, and security
- Understand trade-offs of different architectural choices as they pertain to system qualities.
- Describe the benefits and weaknesses of potential J2EE technology-based architectures
- State benefits and costs of persistence management strategies
- Review real-world case studies of J2EE technology-based architecture
- Prepare for the exam by reviewing practice tests and questions

XML Certified Developer *Fast Path*

Tuesday, March 18, 2003
9:00 am - 5:00 pm

Audience

This tutorial is for programmers who have some knowledge of XML and related technologies and would like to pass the IBM Certified Developer Test 141 on XML and Related Technologies

Prerequisites

Background in object-oriented programming and knowledge of Hypertext Markup Language (HTML). Exposure to XML and related technologies.

Overview

XML is the foundation of two important emerging technologies: Web services and the Semantic Web. XML

expertise and certification is critical for developers who want to remain competitive in the current tight IT job market. The practice tests and questions in this course are specially designed to teach you XML essentials and the key concepts to successfully pass IBM® Test 141 on XML and related technologies.

Outline

- Well formed XML documents
- XML Infoset
- XML namespaces
- Document analysis and modeling
- Document Type Definitions (DTDs)
- XML Schemas
- The SAX API
- The DOM API
- XPath and XSLT

- XSL Formatting Objects (XSL FOs)
- Formatting XML with CSS
- XLink and XPointer
- XML Encryption
- XML Signatures
- SOAP, UDDI, and WSDL
- XML architectures based on business and technical considerations
- Optimization and testing of XML applications

Presenter Bio

Joel Amoussou is the founder and chief learning architect of XMLMentor. Joel is the author of the first XML training course specially designed to prepare developers for IBM® Test 141 on XML and related technologies. He has created XML content management applications for the aerospace, pharmaceutical, and publishing industries.

Microsoft® FREE .NET Web Services Tutorial



Russ' Tool Shed
Wednesday, March 19, 2003
9:00 a.m. – 5:00 p.m.

Join Russ as he shows you how to use Visual Studio .NET

9-12:15 Intro to Web Services Using VS.NET by Russ Fustino

One of the key ideas behind the .NET strategy is the concept of software as a service, or in short, Web services. This session will explain what a Web service is and provide an overview of its related technologies like XML, SOAP and UDDI. We will demonstrate how the .NET Framework makes it easy to implement them for new and existing applications. This session will also provide concrete best practices for building XML Web services using Visual Studio .NET. We'll answer many common questions like: How will my Web service scale? How can my XML Web services enable interoperability with Web services from other vendors as well as within my own organization? We'll delve into building highly reliable and secure Web services. Also, we will discuss issues such as

dealing with complex data types using WSDL (Web Services Description Language), as well as securing SOAP messages using encryption. We'll see how developers can use enterprise-level XML Web services to simplify customer solutions.

1-2:30 - Advanced Web Services Using ASP.NET by Thom Robbins

This session will explore some of the more advanced areas of SOAP in ASP.NET's support for Web services. ASP.NET Web services are the preferred way for Web developers to expose Web services on the Internet. The goal is quick, easy, and high-performing SOAP services. We will look at how to use the SOAP extension classes to create some very interesting applications on top of the core SOAP architecture found within the .NET Framework. For instance, you can implement an encryption algorithm or screen scraping on top of the Web service call. We'll dig into more advanced topics, explore the SOAP headers, and see ways to ensure security in our Web services.

2:45-4:15 - .NET Remoting Essentials by Thom Robbins

Microsoft .NET Remoting is the .NET technology that allows you to easily and quickly build distributed applications. All of the application components can be on one computer or they can be on multiple computers around the world. .NET Remoting allows client applications to use objects in other processes on the same computer or on any other computer to which it can connect over its network. During this presentation we will discuss what you will need to know to get started with .NET Remoting. We will talk about how .NET Remoting compares with DCOM, how to host remoted objects in a variety of applications, how to call remoted objects from a client application, how to control the life time of remoted objects, and how to secure remoting applications.



To learn more, visit
www.sys-con.com

Mobile .NET



Thursday, March 20, 2003
9:00 am - 5:00 pm

Overview

In this session, Derek Ferguson, editor-in-chief of *.NET Developer's Journal*, will give you a thorough introduction to the use of .NET with all manner of mobile computing devices.

The morning will begin with a comprehensive survey of the five most popular mobile computing platforms: Pocket PC, Palm OS, WAP, i-Mode, and J2ME. It will conclude with a thorough examination of how the Mobile Internet Toolkit (a.k.a. "the MIT"), a key part of

Microsoft's mobile .NET strategy, can be leveraged to build Web-based applications capable of working with any of these devices.

In the afternoon, we will discuss Microsoft's technology for building self-contained .NET applications for execution on "smart devices" the .NET Compact Framework. Before the end of the session, such advanced topics as COM Interoperability, SQL Server CE, and MIT extensibility will be covered.

Presenter Bio

Derek Ferguson is chief technology evangelist for Expand Beyond Corporation (www.xb.com), the world-

wide leader in mobile software for enterprise management. He is also editor-in-chief of *.NET Developer's Journal* and author of the book *Mobile .NET*.



Derek Ferguson

Editor-in-Chief, *.NET Developer's Journal*
Chief Technology Evangelist, Expand Beyond Corp.

Major Sponsors at the World's Largest Web Services, Java, XML, and .NET Conference and Expo

2003 East Gold Sponsors



Compuware will be the best worldwide provider of quality software products and services designed to increase productivity. We will continue to create practical solutions that meet our customers needs and surpass their expectations. We will provide an environment for our employees where excellence is encouraged and rewarded and where diversity is promoted at all levels of the company. Compuware is built upon a diverse employee population with a set of key attributes that is common to every individual: Secure, Moral, Ethical, In Agreement with Economic Purpose, Team Player, Other Oriented, Positive, Optimistic, Energetic Achiever and Bright.

Microsoft®

Introducing Visual Studio .NET; visionary yet practical, the single comprehensive development tool for creating the next generation of applications has arrived. Developers can use Visual Studio .NET to:

- Build the next-generation Internet.
- Create powerful applications fast and effectively.
- Span any platform or device.

Visual Studio .NET is the only development environment built from the ground up for XML Web services. By allowing applications to share data over the Internet, XML Web services enable developers to assemble applications from new and existing code, regardless of platform, programming language, or object model.

ORACLE®

Oracle Corporation (Nasdaq: ORCL) is the world's largest enterprise software company, providing enterprise software to the world's largest and most successful businesses. With annual revenues of more than \$9.4 billion, the company offers its database, tools, and application products, along with related consulting, education, and support services. Headquartered in Redwood Shores, California, Oracle is the first software company to develop and deploy 100 per cent Internet-enabled enterprise software across its entire product line: database, server, enterprise business applications, and application development, and decision support tools.

2003 East Silver Sponsor



HP is a leading provider of products, technologies, solutions and services to consumers and business. The company's offerings span IT infrastructure, personal computing and access devices, global services, and imaging and printing. Our \$4 billion (U.S.) annual R&D investment fuels the invention of products, solutions and new technologies, so that we can better serve customers and enter new markets. We invent, engineer, and deliver technology solutions that drive business value, create social value, and improve the lives of our customers.

2003 East Featured Sponsor



Sun was founded with one driving vision. A vision of computers that talk to each other no matter who built them. A vision in which technology works for you, not the other way around. While others protected proprietary, stand-alone architectures, we focused on taking companies into the network age, providing systems and software with the scalability and reliability needed to drive the electronic marketplace.

2003 East Corporate Sponsors



IONA is the leading e-Business Platform provider for Web Services Integration. IONA Orbix E2A enables the flow of information across disparate systems and the liberation of application assets for new business opportunities. For additional information about IONA, visit our Web site at <http://www.iona.com>.



Rational Software provides a software development platform that improves the speed, quality, and predictability of software projects. This integrated, full life-cycle solution combines software engineering best practices, market-leading tools, and professional services. Ninety-six of the Fortune 100 rely on Rational tools and services to build better software, faster. Additional information is available on the Internet at <http://www.rational.com>



Sams Publishing has more than 500 titles in print, and is one of the most successful computer book publishers in the world. From introductory tutorials to comprehensive reference books, Sams Publishing focuses on teaching tomorrow's programmers, developers and system administrators the skills they need to build and manage emerging technologies.



Sybase has always delivered solutions that help customers to share data, is platform independent, and integrates everything: platforms, application servers, components, databases, portals, processes, message brokers, and mobile/wireless. Our technologies have the insight that will promote ease of use, leverage best practices, ensure positive ROI, and help your organization build a successful, pragmatic strategy based on next-generation technologies. Check us out at <http://www.sybase.com/solutions/e-business>



DE solutions and thought leadership deliver the value of Web services to business users today. DE unleashes the value of underlying IT assets, giving enterprises the freedom to innovate and evolve business processes within a standards-based, vendor neutral, loosely coupled framework. Some of the largest corporations in the world rely on DE's Web services solutions. www.digev.com

Special Insert: Web Services Edge East Conference & Expo

Featuring FREE Tutorials, Training Sessions, Case Studies and Exposition

REGISTER ONLINE TODAY @ SYS-CON.COM



*Meet with the industry
experts, professionals,
and visionaries
connecting the enterprise
with today's i-technology!*

Conference
March 18-20, 2003

Exposition
March 19-20, 2003

Hynes Convention Center, Boston

WEB SERVICES EDGE CONFERENCE PAST SPONSORS & EXHIBITORS



Multi-Pack Subscriptions

SAVE UP TO \$400

Pick a 3-Pack, a 6-Pack or a 9-Pack for incredible savings and receive as many as **3 FREE BONUS CDs!**



Two Years / 24 issues - \$99.99
One Year / 12 issues - \$69.99
One Year - Canada & Mexico - \$89.99
One Year - All Other Countries - \$99.99



Two Years / 24 issues - \$89
One Year / 12 issues - \$49.99
One Year - Canada & Mexico - \$79.99
One Year - All Other Countries - \$99.99



Two Years / 24 issues - \$99.99
One Year / 12 issues - \$69.99
One Year - Canada & Mexico - \$89.99
One Year - All Other Countries - \$170



Two Years / 24 issues - \$99.99
One Year / 12 issues - \$69.99
One Year - Canada & Mexico - \$89.99
One Year - All Other Countries - \$99.99



Two Years / 24 issues - \$169.99
One Year / 12 issues - \$149
One Year - Canada & Mexico - \$169
One Year - All Other Countries - \$180



Two Years / 24 issues - \$169.99
One Year / 12 issues - \$149
One Year - Canada & Mexico - \$169
One Year - All Other Countries - \$179



Two Years / 24 issues - \$129
One Year / 12 issues - \$89.99
One Year - Canada & Mexico - \$99.99
One Year - All Other Countries - \$129.99



Two Years / 24 issues - \$89
One Year / 12 issues - \$49.99
One Year - Canada & Mexico - \$79.99
One Year - All Other Countries - \$99.99



Two Years / 24 issues - \$169.99
One Year / 12 issues - \$149
One Year - Canada & Mexico - \$169
One Year - All Other Countries - \$179

RECEIVE
YOUR DIGITAL
EDITION
ACCESS CODE
INSTANTLY
WITH YOUR PAID
SUBSCRIPTIONS

3-Pack

Pick any 3 of our magazines for only \$175⁰⁰ and save up to \$275 for a 1 year subscription plus a **FREE CD**

- 2 Year - \$299.00
- Can/Mex - \$245.00
- All Other Countries - \$315.00

6-Pack

Pick any 6 of our magazines for only \$395⁰⁰ and save up to \$350 for a 1 year subscription plus 2 **FREE CDs**

- 2 Year - \$669.00
- Can/Mex - \$555.00
- All Other Countries - \$710.00

9-Pack

Pick all 9 of our magazines for only \$495⁰⁰ and save up to \$400 for a 1 year subscription plus 3 **FREE CDs**

- 2 Year - \$839.00
- Can/Mex - \$695.00
- All Other Countries - \$890.00

Subscribe online today www.sys-con.com/suboffer.cfm

OFFER SUBJECT TO CHANGE WITHOUT NOTICE

SYS-CON
MEDIA



James Phillips

James Phillips is senior vice president of marketing and product management with worldwide responsibility for Actional's product and market strategy and market execution. He is a frequent speaker and editorial contributor on Web services-related issues and serves on the international advisory board for Web Services Journal.
JAMESP@ACTIONAL.COM

Security: Walk Before You Run – But Don't Stand Still

In survey after survey, security is the most frequently cited barrier to developing distributed applications using Web services technology. In some cases, the findings indicate that the overall level of security concerns among information technology professionals appears to be increasing (Evans). Yet in spite of these trends, enterprise adoption of Web services technology is clearly accelerating. Smart organizations recognize that they must move forward with Web services deployments – employing a variety of security tactics – to avoid the greater risk of being left behind as their competitors embrace and benefit from Web services technology.

SOAs have been held out for years as a substantially more cost-effective and flexible strategy for architecting enterprise software

systems than historical approaches including monolithic system design and tightly coupled client/server models. Many enterprise CIOs and industry observers believe Web services technology, and widespread vendor support of these standards, will enable the widespread adoption of SOA.

There is clear evidence that not only is adoption possible, but that it is well underway in the Global 2000. It's impossible to ignore the daily drumbeat of case studies, articles, and speeches from CIOs declaring their adoption of Web services-based SOAs as funded, high-priority strategic IT initiatives. Gartner Group predicts that SOAs will move to the mainstream in 2003 because “the fact is that Web services are pivotal to future actively managed, flexible and responsive enterprise architecture. It is not possible to sit back while competitors explore this territory without risking that they will open a strategic business lead [companies] will find hard to close.” (Gartner)

The reasons for forging ahead are compelling. Nonetheless, security concerns must be adequately addressed to ensure the success of these projects as well as overall systems integrity. A clear pattern is emerging for how to best deal with the issue of Web services security.

Ensure that security is modular and pluggable. One fact is incontrovertible – security models, protocols, and techniques will evolve. The key to ensuring that a system can evolve with them is to isolate and make pluggable the code that enforces security policy. By separating security policy enforcement logic (authentication, authorization, privacy) from Web service business logic, it is easier to enhance the security model to meet more sophisticated security requirements over time. The vast majority of Web services implementations today are secured via HTTPS. In fact, this is the only model endorsed by the WS-I in its Basic Profile (cur-

rently in draft form), which aims to ensure Web service interoperability. In the future, systems must evolve to adopt emerging standards such as WS-Security and SAML if they are to participate in more complex – and more interesting – Web services usage patterns.

Stage the introduction of Web services technology to mitigate the complexity of the security problem. Most organizations are adopting Web services technology in bite-sized chunks, identifying projects that are limited in scope and low risk, but high in potential payback if successful. These “low-hanging fruit” initiatives allow the organization to gain experience with the technology and to assess its viability for more widespread and sophisticated deployment. As a side effect, they also tend to contain the complexity of the security problem. The vast majority of initial Web services projects are internal and often limited to a single security policy domain. Moreover, service consumers and providers tend to communicate directly instead of through chains of active SOAP intermediaries.

Leverage proven Web-based security models for initial projects. By limiting the complexity of the security problem in early deployments, it's possible to use existing security tools and techniques. HTTPS is a mature model for channel-based security. In initial projects, channel-based security is often sufficient to ascertain the identity of the consuming application and to ensure message privacy and integrity. Leveraging these existing and familiar investments means one less learning hurdle for the organization to jump as it adopts Web services technology. And as noted before, HTTPS is the only WS-I Basic Profile 1.0-endorsed security mechanism and therefore the only guaranteed path to interoperability with WS-I-compliant implementations.

Embrace emerging standards as tools and vendors support them and as architectural complexity requires them. As organizations mature in their use of Web services, existing security models, protocols, and tools fall short. Emerging standards, such as WS-Security, aim to fill the holes exposed in existing standards (federation, policy, trust) in the light of complex Web services usage scenarios. Implementations of proposed standards are just beginning to find their way into vendor offerings.

Security concerns are not a reason to delay the introduction of Web services technology into the enterprise. Successful IT organizations are employing this technology to solve real business problems and to gain competitive advantage. Ensuring implementation flexibility and taking a “walk before you run” approach to Web services adoption will ensure that systems are both secure today and poised to be secured in more complex deployments in the future. ©

- Evans Data Corporation, North American Developer Survey 2002: Volume 2
- Gartner Group, “CIO ‘Must Do’ Resolutions for 2003” (December 24, 2002).

Sitraka

(Now part of Quest Software)

www.sitraka.com/jclass/ws

Swingtide

www.swingtide.com/testdrive