Securing Java Web Services v5.0
Course Summary

Description

This advanced course introduces Java developers to key concepts and technology for developing secure web services and securing enterprise software architecture. Though consensus is forming, and standards have largely taken shape, this is still a broad and challenging field. We focus on a few well-defined approaches: XML cryptography, the WS-Security and WS-SecurityPolicy standards, and the Security Assertions Markup Language, or SAML. We also look XACML for authorization policies and at trust and federation not only as envisioned by SAML but also through the WS-Trust and WS-Federation specifications.

These approaches do overlap, and through our primary case studies we present a single, coherent story of assuring confidentiality, integrity and non-repudiation, user authenticity, and proper request authorization with a blend of policy-driven WS-Security, SAML, and even some application-coded digital signature. We also investigate the web-application end of SAML, with an in-depth study of single sign-on and federated identity.

Although for practical purposes this course relies on a specific platform, which is Java EE, the great majority of the course content teaches interoperable specifications, and would be equally useful to developers working on other web-service-capable platforms such as .NET or to those who work with multiple platforms, and do need to understand the interoperable pieces in detail but perhaps don't need to delve into implementation strategies. In fact, customizations are available that essentially leave out the Java to stick more strictly to the XML.

Objectives

At the end of this course, students will be able to:

- Understand the unique challenges in securing interoperable XML-based services.
- Apply W3C standards to digitally sign and encrypt XML fragments and documents.
- Understand the importance of the WS-Security specifications to interoperable secure messaging.
- Use state-of-the-art tools to configure or implement signature, encryption, and various WS-Security header content for Java web services.
- Drive such WSS implementations from WS-SecurityPolicy documents.
- "Vouch for" a user across domains to achieve request authorization without sharing credentials.
- Exchange security information between servers, applications, and components, using SAML assertion and protocol models.
- Understand the role of XACML in policy management and decision-making.
- Understand the WS-Trust and WS-Federation architectures for developing the trust relationships that enable service federations and service-oriented architectures.
- Build web applications that participate in SAML federation and single sign-on.

Topics

- Securing the Service-Oriented Enterprise
- Transport Security
- XML Signature
- XML Encryption
- WS-Security
- WS-SecurityPolicy
- Introduction to SAML
- SAML Assertions
- SAML Protocol
- XACML
- Securing Federated Services
- SAML Bindings
- Federated Identity

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Securing Java Web Services v5.0
Course Summary (cont'd)

Prerequisites

Students are expected to be able to read and write XML fluently, and have some familiarity with XML Schema. Solid Java programming experience is essential experience developing Java Web services is assumed either via SAAJ or JAX-WAS.

Duration

Four days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Securing Java Web Services v5.0
Course Outline

I. Securing the Service-Oriented Enterprise
- A. Security for Web Services
- B. Threats
- C. CIA Goals
- D. Solution Levels: W3C, OASIS, Java EE
- E. Scenario: Secure Multi-Party Conversation
- F. Cryptography
- G. WS-Security and WS-SecurityPolicy
- H. Scenario: Sharing Security Information
- I. SAML and XACML
- J. Scenario: Multiple User Realms
- K. Scenario: Single Sign-On
- L. Technology Stacks: WS-Federation and Liberty Alliance
- M. The WS-I Basic Security Profile

II. Transport Security
- A. Use Case: Secure Transport
- B. HTTP Authentication Schemes
- C. HTTP BASIC
- D. HTTP DIGEST
- E. Securing Web-Service URLs
- F. HTTPS
- G. JAX-WS Support
- H. Axis Support

III. XML Signature
- A. Use Case: Non-Repudiation
- B. XML Digital Signature
- C. Cryptography Backgrounder
- D. Canonical XML
- E. Enveloped, Enveloping, and Detached Signatures
- F. SignedInfo and References
- G. The Java Cryptography Architecture
- H. Keystores
- I. Why Keys Aren't Enough
- J. X.509 Certificates and Certificate Chains
- K. The KeyStore API
- L. Java XML Digital Signature API
- M. Steps to Sign and Verify XML Content
- N. JAX-WS Message Handlers
- O. Foiling the Man in the Middle

IV. XML Encryption
- A. Use Case: Confidentiality
- B. XML Encryption
- C. EncryptedData
- D. Element vs. Content Encryption
- E. Key Wrapping
- F. The Java Cryptography Extensions
- G. Apache XML Security
- H. Steps to Encrypt and Decrypt XML Content
- I. Choosing Algorithms and Key Sizes

V. WS-Security
- A. Use Case: Secure Message Exchange
- B. Use Case: User Login
- C. The WS-Security Specifications
- D. Security Token Types
- E. Timestamps
- F. Username Tokens
- G. Signature and Encryption
- H. Tools for WS-Security
- I. XWSS and JAAS
- J. Foiling Replay Attacks

VI. WS-SecurityPolicy
- A. Use Case: Sharing Metadata
- B. WS-Policy
- C. Normalized vs. Compact Form
- D. Policy Attachment
- E. Policy Scopes
- F. WS-SecurityPolicy
- G. Protection Assertions
- H. Token Assertions
- I. Supporting and Endorsing Tokens
- J. Bindings
- K. Metro and WSIT
- L. Implementing Callbacks
- M. Integrating Security Frameworks

VII. Introduction to SAML
- A. History of SAML
- B. Assertions
- C. Protocol
- D. Bindings
- E. Profiles
- F. Using OpenSAML
- G. SAML and Web Services

VIII. SAML Assertions
- A. Use Case: "Vouching for" a User
- B. The Assertions Schema
- C. Extensibility
- D. Assertions and Subjects

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Securing Java Web Services v5.0
Course Outline (cont'd)

E. NameID Types
F. Conditions
G. Subject Confirmation
H. Confirmation Methods
I. AuthntStatement
J. Authentication Contexts
K. AttributeStatement
L. Attribute Profiles
M. AuthzDecisionStatements
N. Actions and Evidence
O. WS-Security and SAML Tokens
P. OpenSAML Assertions Model
Q. Creating XML Objects
R. Marshalling and Unmarshalling

IX. SAML Protocol
A. Use Case: Back-Channel Queries
B. Requests, Queries, and Responses
C. Status and StatusCode
D. AuthnQuery
E. AttributeQuery
F. AuthzDecisionQuery
G. Other Request and Response Types
H. OpenSAML Protocol Model
I. SAML and XML Signature
J. SAML and XML Encryption

X. XACML
A. Use Case: Back-Channel Authorization
B. Use Case: Sharing Authorization Policies
C. Policies, Policy Sets, and Targets
D. Rules
E. Combining Algorithms
F. Policy Context
G. Request and Response Types
H. The SAML Profile of XACML
I. Authorization Decisions via XACML

XI. Securing Federated Services
A. Publish, Find, Bind ... Execute!
B. UDDI
C. WS-BPEL
D. The Trust Problem
E. WS-Trust
F. The Security Token Service
G. Messaging Model: RST and RSTR
H. Derived Keys
I. WS-SecureConversation
J. Secure Conversation Metrics
K. WS-Federation
L. Value Proposition

M. SAML Bindings
N. Use Case: Speaking "Through" the Browser
O. The SOAP Binding
P. SAML Over HTTP
Q. The Browser as Messenger
R. The Redirect, POST, and Artifact Bindings
S. The PAOS Binding
T. The URI Binding

XII. Federated Identity
A. What is Federation?
B. Problems for Identity Federation
C. SAML 2.0 Federations
D. Single Sign-On
E. Account Linking and Persistent Pseudonyms
F. Transient Pseudonyms
G. Name ID Mapping
H. Federation Termination
I. OpenSSO
J. Fedlets

XIII. Appendix A. Learning Resources

XIV. Appendix B. Web-Service Security Prefixes and Namespaces

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically