



Capstone Courseware, LLC

33 Boylston Street
Jamaica Plain, MA 02130

877-227-2477
capstonecourseware.com

562. Securing Java Web Services

Version 1.4

This advanced course introduces Java developers to key technology for developing secure Web services. Specifically, we focus on XML signature and encryption standards, the WS-Security specification and token profiles, and the Security Assertions Markup Language (SAML). Students practice signing and encrypting XML message content, and configuring J2EE tools to support signature and encryption of SOAP messages under the Java API for XML-Based RPC (JAX-RPC).

The course emphasizes hands-on exercise, and students will spend roughly half of their classroom time solving specific security problems. Some early labs on XML signature and encryption work to local files; but the bulk of the work is with running JAX-RPC web services: adding WS-Security headers, signing and encrypting message content, and passing SAML assertions among various parties to a messaging scenario.

Although for practical purposes this course relies on a specific platform -- Java and J2EE -- much of the course content teaches interoperable specifications and would be equally useful to developers working on other Web-service-capable platforms such as .NET.

Prerequisites

- Solid Java programming experience is essential; Course 103 provides excellent preparation.
- Experience developing Java Web services is assumed -- either via SAAJ or JAX-RPC. Course 561 is strongly recommended.
- Students are expected to be able to read and write XML fluently, and have some familiarity with XML Schema. Consider courses 501 and 517.



Learning Objectives

- 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 interoperably secure messaging.
- Use emerging Java APIs to configure or implement signature, encryption, and various WS-Security header content for Java Web services.
- Exchange security information between servers, applications, and components, using SAML assertion and protocol models.

Timeline: 4 days.

IDE Support: Eclipse 3.2

In addition to the primary lab files, an optional overlay is available that adds support for Eclipse 3.2. Students can code and build all exercises from within the IDE. JAX-RPC WSDL-to-Java exercises will show a number of "false negative" errors, because the IDE is unaware of the code compiler that runs during final builds. Final build and deploy must be done using Ant, and testing is done from the command line or using prepared tools including Capstone's own SOAPPad and SOAPSniffer. See also our orientation to Using Capstone's Eclipse Overlays, and please be advised that this is an optional feature; it is not a separate version of the course, and the course itself does not contain explicit Eclipse-specific lab instructions.





Chapter 1. Web-Service Security

- Security for Web Services
- Threats
- Technology and Techniques
- Solution Levels
- HTTP Solutions
- The World-Wide Web Consortium
- XML Solutions
- Encryption
- Hashing
- Signature
- OASIS
- Web-Services Solutions
- Technology Stacks: WS-Federation and Liberty Alliance
- WS-Security
- SAML

Chapter 2. HTTP Security

- HTTP Authentication Schemes
- HTTP BASIC
- HTTP DIGEST
- Securing Web-Service URLs
- HTTPS
- JAX-RPC Support
- Axis Support

Chapter 3. XML Signature

- XML Digital Signature
- Canonical XML
- Enveloped, Enveloping, and Detached Signatures
- SignedInfo and References
- The Java Cryptography Architecture
- Keystores
- keytool
- X.509 Certificates
- The KeyStore API
- Java XML Digital Signature API
- Steps to Sign and Verify XML Content
- JAX-RPC Message Handlers
- Foiling the Man in the Middle





Chapter 4. XML Encryption

- XML Encryption
- EncryptedData
- Element vs. Content Encryption
- Encrypted Keys
- The Java Cryptography Extensions
- Apache XML Security
- Steps to Encrypt and Decrypt XML Content

Chapter 5. WS-Security

- The WS-Security Specifications
- Relationship to W3C Specifications
- Security Tokens
- Timestamps
- Tools for WS-Security
- Integrating into JAX-RPC Services and Clients

Chapter 6. Securing Web Services

- Practical Use of WS-Security
- Foiling Replay Attacks
- Dynamic Security Policies

Chapter 7. The Security Assertions Markup Language

- History of SAML
- Goals and Non-Goals
- Authorities
- Assertions
- Protocol

Chapter 8. SAML Assertions

- The Assertions Schema
- Extensibility
- Assertions and Subjects
- NameIdentifiers and SubjectConfirmations
- AuthenticationStatements
- AttributeStatements
- AuthorizationDecisionStatements





Actions and Evidence
SAML Tokens
OpenSAML
Signing SAML Assertions

Chapter 9. SAML Protocol

SAML Messaging
The SAML Protocol Schema
Request Types
Response Types
Status and StatusCode
AuthenticationQuery
AttributeQuery
AuthorizationDecisionQuery
SAML as the Substance

Appendix A. Learning Resources

Appendix B. XML Namespaces for Security Standards

System Requirements

Hardware Requirements (Minimum)

500 MHz, 256 meg RAM, 500 meg disk space.

Hardware Requirements (Recommended)

1.5 GHz, 512 meg RAM, 1 gig disk space.

Operating System

Tested on Windows XP Professional. Course software should be viable on all systems which support the J2EE 1.4 reference implementation.

Network and Security

Limited privileges required -- please see our standard security requirements at <http://capcourse.com/Guides/Security.html>.

Software Requirements

A mix of free downloadable tools - setup is more complex than for most of our courses as we want to let students experiment with diverse tools and techniques.

