

This in-depth, 4-day course introduces the Java web developer to the Spring Security framework. We start with an overview and practical exercises in basic usage: XML configuration for authentication and URL-based authorization. Then we start to dig into Spring Security as a Java model, and develop advanced techniques including custom user realms, custom authorization constraints, method-based authorization, and instance-based authorization.

Then we explore two increasingly popular extensions to Spring Security. We consider the Security Assertions Markup Language, or SAML, and the wide range of identity and security features it offers -- but quickly focus on it's support for single sign-on (SSO), and learn how the Spring Security SAML Extension enables applications to interact with SAML identity providers to implement SSO and single logout. And we look at OAuth for Spring Security, which enables third-party authorization scenarios, and learn how to implement both the server and client sides of the OAuth 2.0 flow.

Course Objectives:

- Configure Spring Security for HTTP BASIC authentication.
- Implement form-based authentication.
- Configure other authentication features including remember-me, anonymous users, and logout.
- Apply authorization constraints to URLs and URL patterns.
- Bind authorization roles to user accounts in relational databases.
- Plug application-specific user realms into Spring Security by implementing UserDetailsService.
- Implement application-specific authorization constraints as AccessDecisionVoters.
- Fix authorization constraints over individual methods of service beans, in lieu of URL authorization or in tandem with it.
- Express user identity in terms of SAML <Subject>s.
- Implement SAML SSO from the service-provider side.
- Implement OAuth 2.0 authorization-server and resource-server roles.
- Implement an OAuth 2.0 client.

Audience: Java programmers wishing to learn Spring Security.

Prerequisites: Java Programming, basic knowledge of XML, and experience with the Spring framework, servlets and/or JSP.

Number of Days: 4 days

1 Spring Security
 Acquiring and Integrating Spring Security
 Relationship to Spring
 Relationship to Java EE Standards
 Basic Configuration
 How It Works
 Integration: LDAP, CAS, X.509, OpenID, etc.

2 Authentication
 Integration: JAAS
 The <http> Configuration
 The <intercept-url> Constraint
 The <form-login> Configuration
 Login Form Design
 "Remember Me"
 Anonymous "Authentication"
 Logout

	The JDBC Authentication Provider	7	Introduction to SAML
	The Authentication/Authorization Schema		History of SAML
	Using Hashed Passwords		Assertions
	Why Hashing Isn't Enough		Protocol
	Using Salts		Bindings
	PasswordEncoder and SaltSource		Profiles
	Key Lengthening		Using OpenSAML
	Channel Security	8	SAML Assertions and Protocol
	Session Management		'Vouching for' a User
3	URL Authorization		Assertions and Subjects
	URL Authorization		NameID Types
	Programmatic Authorization: Servlets		Authentication Contexts
	Programmatic Authorization: Spring Security		Requests, Queries, and Responses
	Role-Based Presentation		Attribute Queries
	The Spring Security Tag Library	9	SAML and XML Signature
4	Under the Hood: Authentication		SAML Bindings
	The Spring Security API		Speaking "Through" the Browser
	The Filter Chain		The SOAP Binding
	Authentication Manager and Providers		SAML Over HTTP
	The Security Context		The Redirect, POST, and Artifact Bindings
	Plug-In Points		The PAOS Binding
	Implementing UserDetailsService	10	The URI Binding
	Connecting User Details to the Domain Model		Federated Identity and SSO
5	Under the Hood: Authorization		SAML 2.0 Federations
	Authorization		Single Sign-On
	FilterSecurityInterceptor and Friends		Account Linking and Persistent Pseudonyms
	The AccessDecisionManager		Transient Pseudonyms
	Voting		Name ID Mapping
	Configuration Attributes		Single Logout
	Access-Decision Strategies		Federation Termination
	Implementing AccessDecision Voter	11	The Spring Security SAML Extension
	The Role Prefix		The Spring Security SAML Extension
6	Method and Instance Authorization		The SAML Entry Point
	Method Authorization		The SAML Filter Chain
	Using Spring AOP		The SSO Processing Filters
	XML vs. Annotations		IdP Discovery
	@PreAuthorize and @PostAuthorize		Login and Logout Handlers
	Spring EL for Authorization		Configuring OpenAM
	@PreFilter and @PostFilter		Configuring an SP
	Domain-Object Authorization		Customization
	The ACL Schema		Combining SSO and Other Authentication Styles
	Interface Model		Authorization and Attributes
	ACL-Base Presentation		

- 12 **OAuth for Spring Security**
 - Third-Party Authorization
 - OAuth
 - Roles and Initial Flow
 - Grant Types
 - Access Tokens
 - The Google OAuth API
 - OAuth for Spring Security
 - Client-Details Services
 - Token Services
 - The AuthorizationEndpoint
 - The TokenEndpoint
 - The UserApprovalHandler
 - The Resource-Server Filter
 - The ScopeVoter
 - The OAuth-Aware RestTemplate
 - AccessTokenProviders
 - The OAuth Redirecting Filter