



TT8610-J Building Secure Software Systems (Java / J2EE Edition) (4 days)

According to research by the National Institute of Standards, 92% of all security vulnerabilities are now considered application vulnerabilities and not network vulnerabilities

Trivera Technologies' *Best Defense™ Security Training Series* is a suite of developer-oriented, application security courses that provide complete coverage of the recently released CWE/SANS *Top 25 Most Dangerous Programming Errors* (<http://cwe.mitre.org/top25/>). These errors, as determined by a consortium of cyber security organizations, enable cyber espionage and crime. Our comprehensive application security and secure coding classes address each of these critical issues head-on, as our courses, seminars and workshops explicitly:

- Teach programmers what these errors are
- Demonstrate, in real terms, the potential impact of each of these errors
- Provide experience in how to recognize and properly address these errors
- Teach stakeholders how to defend against the potential consequences of security breaches in other parts of their IT infrastructure.

Course: TT8610-J Building Secure Software Systems (Java / J2EE Edition)

Duration: 4 days

Skill Level: Intermediate +

Focus: Hands-on programming and analysis class covering why and how to integrate security into the entire software development lifecycle for Java/J2EE applications

Audience: J2EE Architects & stakeholders

Hands-On Format: Approx 50/50 lab to lecture: Extensive hands-on programming labs; Expert lecture combined with open discussions and in-depth demonstrations. Machines required.

Language / Tools: Java 5 or Java 6 delivered with most IDEs: IBM® Rational Application Developer™ (RAD); Oracle® JDeveloper, Eclipse™ / Ganymede, Eclipse WTP, MyEclipse and more. Targets most J2EE complaint application servers including Apache Tomcat™, JBoss™, IBM WebSphere™, Oracle WebLogic™ and more.

Delivery Format: Available for onsite private classroom presentation, or live online / virtual presentation

Customizable: Yes

COURSE SNAPSHOT

Building Secure Software Systems is an intense application security workshop essential for software application designers and architects who need to build secure Java and J2EE applications. Throughout the course, students learn the best practices for designing, architecting, and reviewing secure programs in Java and J2EE. Students will take an application from requirements through to implementation, analyzing and testing for software vulnerabilities. This approach builds a strong appreciation for why software needs to be designed from the ground up in a secure fashion. Security experts agree that the least effective approach to security is "penetrate and patch". It is far more effective to "bake" security into an application throughout its lifecycle. This course explores how design and analysis can be used to build stronger applications from the beginning of the software lifecycle.

A key component to our *Best Defense Security Training Series*, this workshop is a companion course with several developer-oriented courses and seminars.

► Course Objectives: What You'll Learn

Students who attend **Building Secure Software Systems** will leave the course armed with the skills required to understand, work with, and build secure software applications.

This course provides students with a foundation of motivation, terminology, and best practices, prior to jumping into an overview of cryptography and best cryptographic practices. Students are then taught how to recognize software

vulnerabilities (actual and potential) and design defenses for those vulnerabilities. This course quickly introduces developers to the various types of threats against their software. The concept and process of Threat Modeling is introduced as a key enabler for architecting effective and appropriate security for software and information assets.

Working in a dynamic learning environment attendees will learn to:

- Understand the concepts and terminology behind defensive

coding

- Understand and use Threat Modeling as a tool in identifying software vulnerabilities based on realistic threats against meaningful assets
- Examine and work with cryptographic aspects of systems and applications, recognizing and applying best practices.
- Learn the entire spectrum of threats and attacks that take place against software applications in today's world
- Use Threat Modeling to identify potential vulnerabilities in a real life case study
- Understand and implement the processes and measures associated with the security development lifecycle (SDL)
- Acquire the skills, tools, and best practices for design reviews as well as testing initiatives
- Understand the basics of security testing and planning
- Work through a comprehensive testing plan for recognized vulnerabilities and weaknesses

The course provides a solid foundation in basic terminology and concepts, extended and built upon throughout the engagement. Students will examine various recognized attacks against applications.

Processes and best practices are discussed and illustrated through both discussions and group activities. Attending students will be led through a series of advanced topics comprised of integrated lectures, group discussions and comprehensive demonstrations.

► **Experiential Learning – Course Structure**

Attending students will be led through a web application-based case study that involves a database, several interfaces including HTML and web services, and various types of activities that are supported by the application.

The initial portion of the course lays down the foundation in basic terminology and concepts that is built upon in subsequent lessons. The second portion of the course steps through a series of vulnerabilities illustrating in very real terms the right way to implement secure software applications. Many of the vulnerabilities are incorporated into an implementation of the case study. With those examples fresh in their minds, students then embark on a process of planning security-related activities and then implementing them. These will include such things as asset identification, determination of security requirements, and risk analysis. Subsequent activities use these to drive design, code, and application reviews and testing.

Many examples are threaded into the course, designed to reinforce fundamental skills and concepts learned in the lessons. Because these lessons, demonstrations are presented in a building-block fashion, students will gain a solid understanding of not only the core concepts, but also how all the pieces fit together in a complete application.

At the end of each lesson, developers will be tested with a set of review questions to ensure that he/she has fully understands

that topic.

► **Audience & Pre-requisites: Who Should Attend**

This is an **intermediate-level** course designed for application project stakeholders and architects who wish to get up and running on developing well defended web applications.

Familiarity with software design and technologies is required and real world programming experience is highly recommended. Ideally students should have approximately 6 months to a year of working knowledge of J2EE and web applications.

► **Related Courses – Suggested Learning Path**

Take Before: Students should have an understanding and a working knowledge in basic Java and J2EE programming. Depending on the language of choice, students should have experience similar to:

- **TT4000 Understanding Internet Architectures**
- **TT2100 Core Java Programming Fundamentals**
- **TT5100 J2EE Web Application Fundamentals (Servlets, JSPs, JDBC, Security, etc)**

Take Instead: We offer other courses that provide different levels of knowledge or focus:

- For a higher level view of security and related issues, please consider **TT8020 Understanding Web Application Security**
- For in-depth developer training with a lifecycle orientation, consider: **TT8325-J Securing J2EE Web Applications - Lifecycle**
- For complete focus on web services, consider **TT8500-J Securing J2EE Web Services**
- For in-depth developer training with less of a web application orientation, consider: **TT8200-J Secure Java Coding**
- For a web application orientation not specific to J2EE, consider: **TT8120 Secure Web Application Development Seminar (Language Neutral Edition)**

Take After: We offer a variety of introductory through advanced security, development, project management, engineering, architecture and design courses. Students may want to consider the following topics as a follow-on to this course.

- Additional advanced Security or Secure Programming & Coding topics
- Service-Oriented Analysis and Design
- Web Services – Intro through Advanced
- AJAX, XML or other Web Development topics
- Java EE topics: EJB3.0; Spring; Hibernate; Design Patterns & more.
- Advanced .Net developer topics
- Architecture & Analysis courses
- Software Engineering, Design or Project Management tracks

Please note all development courses may also be offered in

other programming languages or tailored to suit your unique requirements.

We will work with you to structure with the best solution to ensure your needs are met, whether we customize the material, or devise a different educational path to help your team best prepare for this training. Please contact us for recommended next steps tailored to your longer term education, project or development objectives.

► **Delivery Environment: Tools to Use**

Although this training is skills-centric, this course can be delivered using a variety of software combinations, including but not limited to: Eclipse / Ganymede, MyEclipse, IBM® WebSphere Rational Application Developer (RAD7), Oracle JDeveloper or other IDEs. This course may also run using Java 5 or Java 6. Please inquire for details and options.

Our detailed lab workbooks are complete with software-specific instructions, screen shots and step-by-step tutorials for using the software you select. In most cases we can easily port our classes to run in the environment of your choosing.

► **Easy Set Up! LoadNGo™ Instant Classroom Kit**

For course deliveries or virtual presentation using open-source tools, we'll provide our unique **LoadNGo Instant Classroom Kit**, which enables students to run the entire course off of a DVD that hosts the entire course set up software, labs, and other pertinent useful educational resources, whitepapers and more. You only need to provide the hardware and appropriate O/S, and we'll do the rest. No installation needed. **Great for secure environments.** Minimum set up burden for your team or firm, with maximum results for your students.

No matter which set up option or software your firm requires, we're pleased to provide a detailed set up guide for all private or on-site courses, and as much assistance as you require to prepare your students or classroom for the course. Our support personnel and instructors can be contacted for any advice you may require to prepare your classroom and/or students for attendance.

► **Student Materials: What You'll Receive**

Our robust course materials include much more than a simple

slideshow presentation handout. Student materials include a comprehensive hard-copy course manual, complete with detailed course notes, code samples, diagrams and current reference materials, all directly related to the course at hand, indexed for ease of use. Step-by-step lab instructions and project descriptions are clearly illustrated and commented for maximum learning.

In addition to everything students need for the course, the **LoadNGo Instant Classroom Kit** described above also includes of workshop labs and solutions; non-restricted workshop software, APIs, documentation, technical education papers, and specifications and tutorials pertinent to the training course. Our course kits are designed to serve as an excellent and useful reference set, long after we leave your classroom.

► **Optional Pre / Post-Testing & Skills Assessment**

We work with you to ensure that your resources are well spent. Through our basic course pre-testing and/or post-course assessments, we ensure your team is up to the challenges that this course offers. Our goal is to structure the best solution to ensure your needs are met, whether we customize the material, or devise a different educational path to prepare for this course.

► **Bridging the Gap: Collaborative Mentoring Services**

Our team of technical experts is also available for various project assistance services to help your team apply their newly-learned classroom skills to their real-world project in a meaningful, practical way, right after the training ends.

Our custom **collaborative mentoring programs** integrate with or extend your team's classroom training experience, to help bring these skills into existing (or inherited) legacy projects, into new projects, or to simply keep your students sharp them in between projects. Our programs can be highly involved and closely integrated with your project timelines or group development efforts, or can be less involved, serving simply as an overarching educational framework or 'spot check' to keep your group skills moving forward in between projects or waiting for projects to begin. Please contact us for details about this exciting custom service.

Workshop Topics Covered

Session: Defensive Coding Overview

- Misconceptions
 - Thriving Industry of Identify Theft
 - Dishonor Roll of Data Breaches
 - TJX: Anatomy of a Disaster
 - Heartland: What? Again?
- Security Concepts
 - Terminology and Players

- Assets, Threats, and Attacks
- OWASP
- CWE/SANS Top 25 Programming Errors
 - Categories
- What they mean to your systems and applications
- Defensive Coding Principles
 - Security Is A Lifecycle Issue
 - Minimize Attack Surface

- Manage Resources
- Application States
- Compartmentalize
- Defense In Depth - Layered Defense
- Consider All Application States
- Not Trusting The Untrusted
- Security Defect Mitigation
- Leverage Experience
- Reality

- Recent, Relevant Incidents
- Find Security Defects In Web Application

Session: Defensive Coding Applied

- Basic Principles Revisited
- Defensive Coding

Session: Security Design Patterns

- Authentication Enforcer
- Authorization Enforcer
- Intercepting Validator
- Secure Base Action
- Secure Logger
- Secure Pipe
- Secure Service Proxy
- Intercepting Web Agent

Session: Secure Software Development (SSD)

- SSD Process Overview
 - CLASP Defined
 - CLASP Applied
- Asset, Boundary, and Vulnerability Identification
- Vulnerability Response
- Design and Code Reviews
- Applying Processes and Practices
- Risk Analysis

Session: Security Testing

- Testing as Lifecycle Process

- Testing Planning and Documentation
- Testing Tools And Processes
 - Principles
 - Reviews
 - Testing
 - Tools
- Static and Dynamic Code Analysis
- Testing Practices
 - Authentication Testing
 - Session Management Testing
 - Data Validation Testing
 - Denial Of Service Testing
 - Web Services Testing
 - Ajax Testing
 - Web Services

Session: Cryptography Overview

- Foundation for Cryptography
- Key Management and Other Issues
- Cryptography Applied to Authentication
- Cryptography Applied to Information Security
- Cryptography Applied to XML

Session: Vulnerabilities

- Unvalidated Input
- Broken Authentication
- Cross Site Scripting (XSS/CSRF)
- Injection Flaws
- Error Handling, Logging, and Information Leakage
- Insecure Storage
- Direct Object Access
- XML Vulnerabilities
- Web Services Vulnerabilities
- Ajax Vulnerabilities
- Configuration Vulnerabilities (System Hardening)

Need more info? Please note that a more detailed outline of the course table of contents, lists of lab exercises and project descriptions is available. Please contact us at Training@triveratech.com for info.

Need courseware? This course is fully customizable, and also available for license with complete support for qualified organizations. Please contact Courseware@triveratech.com for details.

► Why Work With Trivera Technologies?

Whether you are a project leader choosing a training provider or course to bring to your team, or an organization or an instructor looking to potentially license or use course materials to train your own team, or a student looking for an exciting, targeted training class to attend or to recommend to your colleagues - **Our single focus is to make YOUR training event or experience a success.** Here's why choosing Trivera Technologies as your education resource takes the risk right out of your decision making process...

- **We provide a solid secure, design, coding and implementation foundation.** Students will learn how to code, use (and reuse!) essential secure programming and design skills and concepts properly, using best coding practices, grounding them for advanced curriculum, and will be prepared for designing and implementing solutions. **Students will learn the importance of developing well-defended applications.**
- **Our courses are focused - no "fluff" included.** We offer more than a "laundry list" approach to teaching. All lessons have clear objectives, are fundamental to core secure application development and design practices, and are reinforced by hands-on labs and solid practical examples. Each lesson has performance driven objectives that ensure students will learn technologies and skills core to fundamental server-side application design – nothing more, nothing less.
- **Our materials are comprehensive, and current.** Our comprehensive manuals include not only a hard copy of the course presentation, but also detailed reference notes, pertinent diagrams and charts, current lists of suggested online resources and articles, and often technical tutorials or white papers geared to the topics at hand. Our dedicated course development team keeps everything as current as possible with both industry trends and software editions to ensure your team is getting the most current information available.
- **We set you up!** Hands-on courses also include our unique materials for each student, complete with our **LoadNGo Instant Classroom** course set up DVD, software, and a multitude of learning resources that complement the course. Run the course right off the DVD – minimal set up for your company – maximum results for your students.
- **We foster "Learning by Doing".** Progressive labs are designed in such a way that students get a firm grasp on fundamental skills while they work toward designing a complete application. All labs are take-home, and all solution code is presented in an easy to use self-study format for future use and review.
- **We have to adhere to higher standards.** As a courseware provider to other organizations, training firms or independent instructors,

our content and hands-on lab materials are licensed internationally by dozens of firms, and are therefore subject to very stringent quality requirements. Not only will your organization benefit from our own technical team's technical expertise, but also the feedback of hundreds of students and trainers using these materials, worldwide, on a regular basis. This unique fact guarantees that our materials are not only robust and interesting, but also technically correct, current and of the highest quality and usability.

- **We bring years of practical, current experience into the classroom and content.** Our instructors and course authors are also skilled mentors, Java, JEE/JavaEE, J2EE, .Net, Agile, SOA, and web services developers, architects and security-oriented professionals. We believe that learning, using and maintaining solid software execution and delivery methods are as important as gaining sharp coding skills. Best Practices for software development and execution, beyond technical coding skills, are enforced throughout all of our courses and discussions. Our team brings this extensive experience into every classroom and engagement. Our team has trained thousands of students.
- **We're skills-centric.** Although our team has extensive experience using a variety of tools and solutions, our core content is "technology-centric". Our aim is to teach you the best skills and solutions out there – not to sell you software from any particular vendor.
- **We're Java & JEE / J2EE authors and industry speakers.** Our team was selected to write the online *J2EE, EJB, EJB CMP-CMR and Web Services Tutorial Series for IBM developerWorks®* (www.ibm.com) These are the same instructors who train our classes and author the courseware. Most of our trainers/consultants have also authored additional articles on web services, EJB, Struts, J2EE / JEE and advanced Java topics, and are recognized speakers and presenters on the industry technical seminar circuit. Our team is comprised on several successful published authors. Members of our team have written or contributed to: *Eclipse Kick Start, Mastering Eclipse; Professional Jakarta Struts; Using Java Tools for Extreme Programming; Mastering Resin; Mastering TomCat and others.*
- **Our services are guaranteed.** Whether you're a stakeholder organizing your firm's educational services, a student in our live or virtual classroom or a trainer using our materials to educate your own client or team – **Our core mission is to make YOU a success in the classroom.**

► For Additional Information

Need dedicated training? All courses can be brought onsite or run virtually for a **private presentation, anywhere around the world**, customized to suit your unique requirements or goals. Please contact Training@triveratech.com for course details, Public Schedule dates and locations, and Special Discount Offers.



Trivera Technologies is a 100%
Female-Owned Small Business Concern
GSA Schedule #GS-35F-0188T
Please contact us for details & pricing.

Need courseware? **Let us take the risk out of your classroom delivery!** All materials are also available on a worldwide basis for corporate license with complete instructor support and free corporate branding. Our LoadNGo Set up is available to partners as well! We guarantee our pricing and service. Samples of our course materials, as well as live client references for all of our services are available upon request. Please contact Courseware@triveratech.com for details.

For more information about our training, mentoring or courseware development or licensing options, or to see our complete list of course offerings and services, please visit us at www.triveratech.com, email Training@triveratech.com or call 609.953.1515.