Training: Capstone Courseware
107 Java Development for Secure Systems

TRAINING GOALS:

Version 6.0

This course exposes students to the broad range of challenges and techniques that is "**Java security**." Secure coding practice for Java incorporates techniques for **Java SE** and **Java EE**, and increasingly EE applications are using SE techniques such as policy files and **JAAS authentication**. This course spends some time on each platform, so that students will be exposed to SE basics such as access controller, permissions, and policies; and also traditional EE techniques such as web-security declarations and the **EJB authorization model**. Best-practice chapters wrap up coverage of each platform.

The course emphasizes hands-on exercise, and students will spend more than half of their classroom time solving specific security problems. Most labs are organized as scenarios in which a security breach of existing software is possible - students begin by hacking the system in some way. Then the work of the lab is to tighten up the software to eliminate the threat: set a secure policy, sign a file, clean up overexposed parts of an API, require user login, etc.

This version of the course targets Java SE 6 and Java EE 5, but it is largely applicable to Java SE 5 and J2EE 1.4 as well, and groups looking for Java training who know they'll be using those earlier platforms are encouraged to use this course.

CONSPECT:

- Chapter 1. Java SE Security
  - Holistic Security Practices
  - Threats to the User
  - The Class Loader and Bytecode Verifier
  - System Classes and the Core API
  - SecurityManager and AccessController
  - Permissions
  - Implication
  - CodeSources
  - Policies
  - Configuring Java SE Security

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Dynamic Policies
- Privileged Actions

- Chapter 2. Code Signature and Key Management
  - Encryption and Digital Signature
  - Keystores
  - Keys and Certificates
  - Certificate Authorities
  - The KeyStore API
  - Signing JARs
  - Signed CodeSources
  - Additional Policy Semantics
- Chapter 3. Secure Development Practices: Java SE
  - Code Injection
  - Final Classes and Methods
  - Singletons, Factories, and Flyweights
  - Methods, Collections, and Data Hiding
  - Sealing JARs
  - Code Obfuscation
  - Object Serialization
- Chapter 4. Cryptography
  - Threats to Identity and Privacy
  - The Java Cryptography Extensions
  - The Signature Class
  - SignedObjects
  - The Java Cryptography Extensions
  - SecretKeys and KeyGenerator
  - The Cipher Class
  - Dangerous Practices
  - HTTP and JSSE
- Chapter 5. JAAS
  - Pluggable Authentication Logic
  - JAAS
  - Packages and Interfaces
  - Subjects and Principals
  - ANDs and ORs
  - Impersonation Methods

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Permissions for JAAS Use
- LoginContext and LoginModule
- Configuring JAAS
- CallbackHandler and Callbacks
- Implementing a JAAS Client
- Implementing a LoginModule

- Chapter 6. Java EE Security
  - Java EE Servers as Code Hosts
  - Tomcat Security Configuration
  - Declaring Roles
  - Securing URLs
  - HTTP Authentication Schemes
  - Securing EJBs
  - Programmatic Security
  - JAAS in Java EE
  - Realms and LoginModules
  - JAAS in Tomcat
  - JACC
  - Certifying a Java EE Application
  - HTTPS Configuration
- Chapter 7. Secure Development Practices: Java EE
  - Presentation-Tier Vulnerabilities
  - User Accounts
  - MVC and Security
  - Validating User Input
  - SQL Injection
  - Cross-Site Scripting
  - Reflected XSS
  - Defeating XSS
  - OWASP
  - Penetration Testing
  - Error Handling and Information Leakage
  - Logging and Auditing

REQUIREMENTS:

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Solid **Java programming** experience is assumed - Course 103 is excellent preparation.
- Though extensive practical experience with **Java EE development** is not necessary, some knowledge of **Java EE architecture and development** is also recommended - consider Course 108 **Overview of Java EE Development**, which offers a one-day overview of Java EE development, including architecture and working examples.

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Capstone Courseware.

TRAINER:

Authorized Capstone Courseware Trainer.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007