

# Java Development for Secure Systems (2 Days)

**Custom Training Institute**  
9085 Coyote Springs Road  
Prescott Valley, AZ 86314  
(928) 772-3811  
FAX (928) 441-6444

## Java Development for Secure Systems (CTI 240)

*Students will learn about security problems for Java applications and components, and the diverse solutions found in various places in the Java architecture. We cover basic concepts of code security - how a J2SE runtime protects the system from Java code, and Java code from other Java code - and good secure-code practices; basic cryptography skills using the appropriate Java APIs; enterprise software; issues related to component-based architectures such as Web applications, EJBs, and Java messaging components.*

*Prerequisites: Solid Java programming experience is assumed - both structured and object-oriented techniques. Some knowledge of J2EE architecture and development is also required, though extensive practical experience with J2EE development is not necessary.*

*Minimum software requirements: Microsoft Windows or Linux systems that support J2EE 1.4. A mix of free downloadable tools will be specified for setup.*

*Minimum hardware requirements for all machines: Pentium 2+GHz or equivalent CPU, 512 meg RAM, 1 gig HD space.*

*Microsoft PowerPoint and Internet access on instructor's workstation for presentation purposes.*

### Module 1: Secure Development Practices

- Threats to the Code
- Using SQL
- Multi-Tier Architecture
- Encapsulation
- Interface/Implementation Split
- Observable vs. Mutable Objects
- Immutable Collections
- Package Design
- Inner Classes and Objects
- Ease of Use vs. Security
- Code Obfuscation
- Logging
- Auditing
- Object Serialization
- Multi-Threading

### Module 2: Java SE Security

- Threats to the User
- Protections in the Java Language
- The Class Loader and Bytecode Verifier
- System Classes and the Core API
- SecurityManager and AccessController
- Privileged Actions
- Signing and Sealing Java Code
- Key Management
- Policies
- Trust Relationships

### Module 3: Cryptography

- Threats to Application Data
- Public-Key Encryption
- Digital Signature
- Configuring Components for Secure Protocols
- Optional Section:*
- The Java Cryptography Extensions
- Encrypting and Signing Content
- Dangerous Practices
- DIY Algorithms

### Module 4: The Java Authentication and Authorization Service

- Heterogenous Security Systems
- JAAS
- Principals and Credentials
- Authentication
- Authorization
- Implementing a LoginModule
- Adapting Authentication Systems
- Best Practices: Lockouts and Blacklists

### Module 5: Java EE Security

- Threats for Enterprise Software
- Solutions and Patterns
- Layers and Repetition
- Validation
- Session Management
- Declaring Roles
- Securing Web Applications
- Securing EJBs
- Programmatic Security

### Appendix A: Learning Resources