Java & J2EE Security

Course Summary

Description

This course is designed to teach the fundamentals of security on the Java and J2EE platforms. It provides students with a solid foundation in security that they can use to build secure systems. The course focuses on covering the foundations of security in the context of Java and J2EE. Students will complete the class with the ability to evaluate security options and make appropriate decisions for the various solutions and the tradeoffs involved.

Topics

- Security Primer
- Cryptography Foundations
- Digital Signatures
- SSL Protocol
- Single Sign On Protocols
- XML Security Standards
- JSE Security Model
- Access Control Models
- JEE Security Model
- Common Security Attacks & Deference's
- Engineering for Security

Audience

This course is designed for programmers & Architects who need a gain a deep understanding of the security features of the Java and J2EE platforms.

Prerequisites

Students should have Java Programming experience.

Duration

Five days

Java & J2EE Security

Course Outline

I. Security Primer
- A. Security concepts
- B. Attacks
- C. Vulnerabilities
- D. Security building blocks
- E. Security mindset

II. Cryptography Foundations
- A. Crypto concepts
- B. Symmetric key cryptography
- C. Public key cryptography
- D. One Way Has Functions
- E. Message Authentication Codes
- F. Overview of various crypto algorithms strengths and weaknesses
- G. Security Protocol concepts
- H. Using the Java Cryptography API's

III. Digital Signatures
- A. Digital signature protocol
- B. Certificates
- C. Certificate Authorities
- D. Working with Digital Signatures in Java
- E. PKI infrastructure overview

IV. SSL Protocol
- A. Overview of the SSL protocol
- B. Basic SSL Protocol
- C. Cipher suite combinations
- D. Generating certificates
- E. Key stores
- F. Java support for SSL
- G. Tying the HTTP Session management in J2EE to the SSL Session Id.

V. Single Sign On Protocols
- A. How Single Signon protocols work
- B. Propagating user identity across applications in a distributed infrastructure
- C. SAML overview

VI. XML Security Standards Overview
- A. XML Encryption
- B. XML Digital Signatures

VII. JSE Security Model
- A. Java Security Model
- B. Security Manager
- C. JAAS API

VIII. Access Control Models
- A. Common models for access control
- B. ACL lists
- C. Permissions
- D. Role based access control
- E. Managing permission data

IX. JEE Security Model
- A. Web application security
- B. EJB security
- C. RMI security
- D. Web Services security
- E. Security with the Spring framework
- F. Secure coding principles

X. Common Security Attacks
- A. SQL injection demonstration
- B. Protecting against the attack
- C. Attack demonstration
- D. Protecting against the attack
- E. Overview of other types of attacks

XI. Engineering for security
- A. Security Mindset
- B. Security best practices
- C. Security worst practices
- D. Practical tips for securing J2EE applications
- E. Levers of security (Hardware, OS, App Server, Code, … etc)

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically