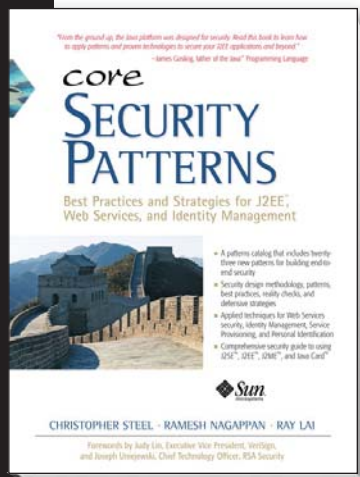


An in-depth treatment of J2EE security architectural patterns and practices  
and how to apply them optimally to enterprise applications

Christopher Steel, Ramesh Nagappan, and Ray Lai



## Core Security Patterns: Best Practices and Strategies for J2EE™, Web Services, and Identity Management

*Core Security Patterns* is the hands-on practitioners guide to building robust end-to-end security into J2EE™ enterprise applications, Web services, identity management, service provisioning, and personal identification solutions. Written by

three leading Java security architects, the patterns-driven approach fully reflects today's best practices for security in large-scale, industrial-strength applications.

The authors explain the fundamentals of Java application security from the ground up, then introduce a powerful, structured security methodology; a vendor-independent security framework; a detailed assessment checklist; and twenty-three proven security architectural patterns. They walk through several realistic scenarios, covering architecture and implementation and presenting detailed sample code. They demonstrate how to apply cryptographic techniques; obfuscate code; establish secure communication; secure J2ME™ applications; authenticate and authorize users; and fortify Web services, enabling single sign-on, effective identity management, and personal identification using Smart Cards and Biometrics.

Core Security Patterns covers all of the following, and more:

- What works and what doesn't: J2EE application-security best practices, and common pitfalls to avoid
- Implementing key Java platform security features in real-world applications
- Establishing Web Services security using XML Signature, XML Encryption, WS-Security, XKMS, and WS-I Basic security profile
- Designing identity management and service provisioning systems using SAML, Liberty, XACML, and SPML
- Designing secure personal identification solutions using Smart Cards and Biometrics
- Security design methodology, patterns, best practices, reality checks, defensive strategies, and evaluation checklists
- End-to-end security architecture case study: architecting, designing, and implementing an end-to-end security solution for large-scale applications

©2006, Cloth, 1088 pages,  
0-13-146307-1, \$59.99

*"Java provides the application developer with essential security mechanisms and support in avoiding critical security bugs common in other languages. A language, however, can only go so far. The developer must understand the security requirements of the application and how to use the features Java provides in order to meet those requirements. Core Security Patterns addresses both aspects of security and will be a guide to developers everywhere in creating more secure applications."*

—Whitfield Diffie,  
inventor of  
Public-Key Cryptography

*"A comprehensive book on Security Patterns, which are critical for secure programming."*

—Li Gong, former Chief Java  
Security Architect, Sun  
Microsystems, and coauthor of  
*Inside Java 2 Platform Security*

For more information visit: [www.phptr.com/title/0131463071](http://www.phptr.com/title/0131463071)  
Available wherever technical books are sold.

Prentice Hall PTR



## TABLE OF CONTENTS

Foreword by Judy Lin

Foreword by Joe Uniejewski

Preface

Acknowledgments

About the Authors

### I. INTRODUCTION

1. Security by Default

2. Basics of Security

### II. JAVA SECURITY ARCHITECTURE AND TECHNOLOGIES

3. The Java 2 Platform Security

4. Java Extensible Security Architecture and APIs

5. J2EE Security Architecture

### III. WEB SERVICES SECURITY AND IDENTITY MANAGEMENT

6. Web Services Security – Standards and Technologies

7. Identity Management Standards and Technologies

### IV. SECURITY DESIGN METHODOLOGY, PATTERNS, AND REALITY CHECKS

8. The Alchemy of Security Design – Methodology, Patterns, and Reality Checks

### V. DESIGN STRATEGIES AND BEST PRACTICES

9. Securing the Web Tier – Design Strategies and Best Practices

10. Securing the Business Tier – Design Strategies and Best Practices

11. Securing Web Services – Design Strategies and Best Practices

12. Securing the Identity – Design Strategies and Best Practices

13. Secure Service Provisioning – Design Strategies and Best Practices

### VI. PUTTING IT ALL TOGETHER

14. Building End-to-End Security Architecture – A Case Study

### VII. PERSONAL IDENTIFICATION USING SMART CARDS AND BIOMETRICS

15. Secure Personal Identification Strategies Using Smart Cards and Biometrics

Index

### About the Authors

**CHRISTOPHER STEEL**, CISSP, ISSAP, is the President and CEO of FortMoon Consulting and was recently the Chief Architect on the U.S. Treasury's Pay.gov project. He has over fifteen years experience in distributed enterprise computing with a strong focus on application security, patterns, and methodologies. He presents regularly at local and industry conferences on security-related topics.

**RAMESH NAGAPPAN** is a Java Technology Architect at Sun Microsystems. With extensive industry experience, he specializes in Java distributed computing and security architectures for mission-critical applications. Previously he coauthored three best-selling books on J2EE, EAI, and Web Services. He is an active contributor to open source applications and industry-standard initiatives, and frequently speaks at industry conferences related to Java, XML, and Security.

**RAY LAI**, Principal Engineer at Sun Microsystems, has developed and architected enterprise applications and Web services solutions for leading multinational companies ranging from HSBC and Visa to American Express and DHL. He is author of *J2EE Platform Web Services* (Prentice Hall, 2004).

### ORDERING INFORMATION:

#### Single Copy Sales:

Visa, MasterCard, American Express, Checks, or Money Orders only —  
Tel: 515-284-6761  
Fax: 515-284-2607  
Toll-Free: 800-811-0912  
Online: [www.phptr.com](http://www.phptr.com)

#### Government Agencies:

Kathryn Bass  
GS-14F-8023A  
703-404-9194  
[www.pearsongovernmentalsales.com](http://www.pearsongovernmentalsales.com)

#### College Professors:

Desk and Review Copies  
Toll-Free: 800-526-0485  
E-mail: [samplingdept@prenhall.com](mailto:samplingdept@prenhall.com)

#### Corporate Accounts:

Corporate purchases and/or Quantity, Bulk Orders. Purchase Orders or Credit Card sales.  
Fax: 317-428-3343  
Toll-Free: 800-382-3419

### INTERNATIONAL ORDERING INFORMATION:

**Canada:**  
[cdn.ordr@pearsoned.com](mailto:cdn.ordr@pearsoned.com)

**UK/EMEA:**  
Europe, Middle East, South Africa  
[enq.orders@pearson.com](mailto:enq.orders@pearson.com)

**BeNeLux:**  
[amsterdam@pearson.com](mailto:amsterdam@pearson.com)

**Australia:**  
[sales@au.penguinroup.com](mailto:sales@au.penguinroup.com)

**South Asia:**  
[asia@pearsoned.com.sg](mailto:asia@pearsoned.com.sg)

**North Asia:**  
[msip@pearsoned.com.hk](mailto:msip@pearsoned.com.hk)

**Other Regions:**  
[tim.galligan@pearsoned.com](mailto:tim.galligan@pearsoned.com)



For more information visit: [www.phptr.com/title/0131463071](http://www.phptr.com/title/0131463071)  
Available wherever technical books are sold.

Prentice Hall PTR