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

Christopher Steel
Ramesh Nagappan
Ray Lai
# Contents

<table>
<thead>
<tr>
<th>Foreword by Judy Lin</th>
<th>xxv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword by Joe Uniejewski</td>
<td>xxix</td>
</tr>
<tr>
<td>Preface</td>
<td>xxxi</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>xli</td>
</tr>
<tr>
<td>About the Authors</td>
<td>xlv</td>
</tr>
</tbody>
</table>

## PART I Introduction

### Chapter 1  Security by Default

- Business Challenges Around Security  5
- What Are the Weakest Links?  7
  - The Network Services  7
  - The Host Operating System (OS)  8
  - The Application or Service  8
- The Impact of Application Security  8
  - Critical Application Security Flaws and Exploits  10
- The Four W’s  17
  - Which Applications Are We Protecting?  17
  - Who Are We Protecting the Applications From?  18
## Contents

Where Should We Protect Them? 18
Why Are We Protecting Them? 18

Strategies for Building Robust Security 19
Unified Process for Security Design 19
Design Patterns 19
Best Practices 20
Reality Checks 20
Proactive Assessment 20
Profiling 20
Defensive Strategies 20
Recovery and Continuity Strategies 21

Proactive and Reactive Security 21

The Importance of Security Compliance 21
Sarbanes-Oxley Act 22
Gramm-Leach-Bliley Act 23
HIPPA 24
The Children’s Online Privacy Protection Act 25
EU Directive on Data Protection 25
California’s Notice of Security Breach (1798.29) 26
Security Compliance in Other Countries 26

The Importance of Identity Management 27
Identity Provisioning Services 27
Identity Data Synchronization Services 27
Access Management Services 28
Federation Services 28
Directory Services 28
Auditing and Reporting Services 28

Secure Personal Identification 29
Personal Identification and Authentication 29
Smart Card Identity 30
Biometric Identity 32
RFID-Based Identity 35

The Importance of Java Technology 36
Security in the Java Platform 37

Making Security a “Business Enabler” 37
Case 1—Justifying Identity and Access Management 38
## Contents

**Case 2–Justifying Proactive Security Approaches** 39

**Case 3–Justifying Security Compliance** 42

Summary 42

References 43

### Chapter 2 Basics of Security 48

Security Requirements and Goals 50

- Confidentiality 50
- Integrity 51
- Authentication 51
- Authorization 52
- Non-Repudiation 53

The Role of Cryptography in Security 53

- Cryptographic Algorithms 54

The Role of Secure Sockets Layer (SSL) 69

The Importance and Role of LDAP in Security 73

- The Role of LDAP in J2EE 76

Common Challenges in Cryptography 77

- Random Number Generation 77
- Key Management 77
- Certificate Revocation Issues 78
- Trust Models 79

Threat Modeling 81

Identity Management 83

- Single Sign-on (SSO) 84
- Federated SSO 86

Summary 89

References 89

### PART II Java Security Architecture and Technologies 93

### Chapter 3 The Java 2 Platform Security 94

Java Security Architecture 96

- The Java Virtual Machine (JVM) 96
- The Java Language 97
- Java Built-in Security Model 99
Contents

Java Applet Security 109
  Signed Applets 112
Java Web Start Security 116
Java Security Management Tools 118
  Java Keystore 118
  Keytool 118
  Policytool 125
  Jar sign er 125
J2ME Security Architecture 126
  J2ME Configurations 127
  J2ME Profiles 130
  MIDlet Security 132
Java Card Security Architecture 136
  Understanding Smart Cards 136
  Java Card Technology in Smart Cards 138
  Java Card Platform Security Model 139
  Java Card Applets 140
Securing the Java Code 143
  Reverse Engineering: Disassembling and Decompiling 143
  Code Obfuscation 144
Summary 145
References 146

Chapter 4 Java Extensible Security Architecture and APIs 148
Java Extensible Security Architecture 150
Java Cryptography Architecture (JCA) 151
  JCA Cryptographic Services 152
  Understanding JCA API Programming Model 155
Java Cryptographic Extensions (JCE) 159
  JCE Cryptographic Service Provider 160
  Understanding the JCE API Programming Model 163
  JCE Hardware Acceleration and Smart Card Support 175
  Using Smart Cards as Java Key Stores 176
  Strong versus Unlimited Strength Cryptography 178
Java Certification Path API (CertPath) 179
  Java CertPath—Classes and Interfaces 179
  Java CertPath API Programming Model 180
Chapter 5 J2EE Security Architecture

J2EE Architecture and Its Logical Tiers
J2EE Security Definitions
J2EE Security Infrastructure
J2EE Container-Based Security
  Declarative Security
  Programmatic Security
  J2EE Authentication
  Protection Domains
  J2EE Authorization
  Java Authorization Contract for Client Containers (JACC)
  Transport Layer Security
J2EE Component/Tier-Level Security
  Users, Groups, Roles, and Realms
  Web- or Presentation-Tier Security
J2EE Client Security
  HTTPS Connection
  Secure J2ME Clients
EJB Tier or Business Component Security
  EJB Declarative Authorization
  EJB Programmatic Authorization
  Anonymous or Unprotected EJB Resources
  Principal Delegation in EJBs
PART III  Web Services Security and Identity Management  
Chapter 6  Web Services Security—Standards and Technologies  
Web Services Architecture and Its Building Blocks  
Web Services Operational Model  
Core Web Services Standards  
Web Services Communication Styles  
Web Services Security—Core Issues  
Web Services—Threats, Vulnerabilities, and Risks  
Web Services Security Requirements  
Authentication  
Authorization and Entitlement  
Auditability and Traceability  
Data Integrity  
Data Confidentiality  
Non-repudiation  
Availability and Service Continuity  
Single Sign-on and Delegation  
Identity and Policy Management  
Security Interoperability  
Web Services Security Standards  
XML Signature  
Motivation of XML Signature  
The Anatomy of XML Signature
<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Identity Management Standards and Technologies</th>
<th>356</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Management—Core Issues</td>
<td>358</td>
<td></td>
</tr>
<tr>
<td>Understanding Network Identity and Federated Identity</td>
<td>360</td>
<td></td>
</tr>
<tr>
<td>The Importance of Identity Management</td>
<td>362</td>
<td></td>
</tr>
</tbody>
</table>
Introduction to SAML

The Motivation of SAML

The Role of SAML in SSO

SAML 1.0

SAML 1.1

SAML 2.0

SAML Profiles

SAML Architecture

SAML Assertions

SAML Domain Model

SAML Architecture

Policy Enforcement Point

Policy Administration Point

SAML Request-Reply Model

SAML Authentication Assertion

SAML Attribute Assertion

SAML Authorization Decision Assertion

XML Signatures in SAML

SAML Usage Scenarios

Security Threats and Countermeasures

The Role of SAML in J2EE-Based Applications and Web Services

Introduction to Liberty Alliance and Their Objectives

Liberty Phase 1

Liberty Phase 2

Liberty Alliance Architecture

Relationships

Web Redirection

Web Services

Meta-Data and Schemas

Security Mechanisms

Liberty Usage Scenarios

Federation Management

Liberty Single Sign-on

Federated Single Sign-on

Global Logout

Example–SAML and Liberty Using Sun Java System Access Manager
The Nirvana of Access Control and Policy Management  
  
IETF Policy Management Working Group 404  
Distributed Management Task Force (DMTF) 404  
Parlay Group 405  
Enterprise Privacy Authorization Language (EPAL) 405  
Web Services Policy—WS-Policy and WSPL 408  

Introduction to XACML 411  
XACML 2.0 416  
XACML Data Flow and Architecture 418  
XACML Architecture 420  
XACML Usage Scenarios 421  
Policy Store 421  
Centralizing Security Policy for Web Services Security 421  
Collaborating with SAML 422  
ebXML Registry 422  
Example—XACML Using Sun’s XACML Kit 422  
Sample Scenario 423  
Sample Request 423  
Sample Policy 425  
Use of XACML 2.0 with SAML 2.0 430  
Summary 432  
References 433  

PART IV Security Design Methodology, Patterns, and Reality Checks 437  
Chapter 8 The Alchemy of Security Design—Methodology, Patterns, and Reality Checks 438  
The Rationale 440  
The Security Wheel 441  
Secure UP 444  
Secure UP—Artifacts 449  
Risk Analysis (RA) 452  
Trade-off Analysis (TOA) 455  
Security Patterns 456  
Understanding Existing Security Patterns 456
Security Patterns for J2EE, Web Services, Identity Management, and Service Provisioning 466
  Security Pattern Template 466
  Security Patterns Catalog 467
  Security Patterns and their Relationships 478
  Patterns-Driven Security Design 488
  Security Design Processes 490
  Policy Design 496
  Classification 497
  Application Security Assessment Model 499
Reality Checks 501
Security Testing 523
  Black Box Testing 524
  White Box Testing 524
Adopting a Security Framework 525
  Application Security Provider 527
Refactoring Security Design 529
Service Continuity and Recovery 530
Conclusion 530
References 531
  Unified Process 531
  Security Principles 531
  Security Patterns 531
  Others 532

PART V Design Strategies and Best Practices 533
Chapter 9 Securing the Web Tier—Design Strategies and Best Practices 534
Web-Tier Security Patterns 535
  Authentication Enforcer 535
  Authorization Enforcer 548
  Intercepting Validator 560
  Secure Base Action 569
  Secure Logger 577
  Secure Pipe 590
  Secure Service Proxy 598
  Intercepting Web Agent 606
Chapter 10  Securing the Business Tier—Design Strategies and Best Practices  
Security Considerations in the Business Tier  623
Business Tier Security Patterns  624
Audit Interceptor  624
Container Managed Security  635
Dynamic Service Management  645
Obfuscated Transfer Object  659
Policy Delegate  668
Secure Service Façade  677
Secure Session Object  686
Best Practices and Pitfalls  693
Infrastructure  693
Architecture  694
Policy  695
Pitfalls  696
References  697

Chapter 11  Securing Web Services—Design Strategies and Best Practices  
Web Services Security Protocols Stack  700
Network-Layer Security  701
Transport-Layer Security  701
Message-Layer Security  702
Web Services Security Infrastructure  702
Network Perimeter Security  702
XML Firewall  704
Web Services Infrastructure  704
Identity Provider  704
Directory Services  704
Web Services Security Patterns  705
Message Interceptor Gateway  705
Chapter 12  
Securing the Identity—Design Strategies and Best Practices  
754

Identity Management Security Patterns  
Assertion Builder Pattern  
Single Sign-on (SSO) Delegator Pattern  
Credential Tokenizer Pattern  
756

Best Practices and Pitfalls  
Best Practices  
Pitfalls  
813

References  
814

Chapter 13  
Secure Service Provisioning—Design Strategies and Best Practices  
816

Business Challenges  
Scope of Service Provisioning  
Relationship with Identity Management  
A Typical Scenario of User Account Provisioning  
Current Approaches to User Account Provisioning  
818

User Account Provisioning Architecture  
Centralized Model versus Decentralized Model  
Logical Architecture  
Portal Integration  
Integrating with an Identity Provider Infrastructure  
Other Integration Capability  
Differentiators for Service Provisioning Products  
823

Introduction to SPML  
Service Provisioning Operations  
Features in SPML  
Adopting a SAML Implementation  
833

Service Provisioning Security Pattern  
Password Synchronizer Pattern  
Related Patterns  
840

References  
890
<table>
<thead>
<tr>
<th>Part</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PART VI</td>
<td>Putting It All Together</td>
<td>899</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>Building End-to-End Security Architecture—A Case Study</td>
<td>900</td>
</tr>
<tr>
<td>Overview</td>
<td>902</td>
<td></td>
</tr>
<tr>
<td>Understanding the Security Challenges</td>
<td>902</td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>904</td>
<td></td>
</tr>
<tr>
<td>Use Case Scenarios</td>
<td>905</td>
<td></td>
</tr>
<tr>
<td>Choosing the Right Methodology</td>
<td>905</td>
<td></td>
</tr>
<tr>
<td>Identifying the Requirements</td>
<td>906</td>
<td></td>
</tr>
<tr>
<td>Identifying the Security Requirements</td>
<td>907</td>
<td></td>
</tr>
<tr>
<td>System Constraints</td>
<td>909</td>
<td></td>
</tr>
<tr>
<td>Security Use Cases</td>
<td>909</td>
<td></td>
</tr>
<tr>
<td>System Environment</td>
<td>913</td>
<td></td>
</tr>
<tr>
<td>Application Architecture</td>
<td>913</td>
<td></td>
</tr>
<tr>
<td>Conceptual Security Model</td>
<td>915</td>
<td></td>
</tr>
<tr>
<td>Security Architecture</td>
<td>917</td>
<td></td>
</tr>
<tr>
<td>Risk Analysis and Mitigation</td>
<td>920</td>
<td></td>
</tr>
<tr>
<td>Trade-Off Analysis (TOA)</td>
<td>923</td>
<td></td>
</tr>
<tr>
<td>Applying Security Patterns</td>
<td>924</td>
<td></td>
</tr>
<tr>
<td>Security Architecture—Detailed Components</td>
<td>927</td>
<td></td>
</tr>
<tr>
<td>Design</td>
<td>930</td>
<td></td>
</tr>
<tr>
<td>Policy Design</td>
<td>930</td>
<td></td>
</tr>
<tr>
<td>Factor Analysis</td>
<td>931</td>
<td></td>
</tr>
<tr>
<td>Security Infrastructure</td>
<td>934</td>
<td></td>
</tr>
<tr>
<td>Tier Analysis</td>
<td>935</td>
<td></td>
</tr>
</tbody>
</table>
Trust Model
Threat Profiling
Security Design

Development
Unit and Integration Testing

Testing
White Box Testing
Black Box Testing

Deployment
Configuration
Monitoring

Auditing

Summary
Lessons Learned
Pitfalls
Conclusion

References

PART VII  Personal Identification Using
Smart Cards and Biometrics

Chapter 15  Secure Personal Identification Strategies
Using Smart Cards and Biometrics

Physical and Logical Access Control

The Role of Smart Cards in Access Control
The Role of Biometrics in Access Control

Enabling Technologies
Java Card API
Global Platform
PC/SC Framework
OpenCard Framework (OCF)
OpenSC
BioAPI
Pluggable Authentication Module (PAM)
Graphical Identification and Authentication (GINA)
Java Authentication and Authorization Service (JAAS)
| Contents |
|------------------|---|
| Smart Card-Based Identification and Authentication | 970 |
| Architectural Model | 971 |
| Operational Model | 975 |
| Using Smart Cards for Physical Access Control | 979 |
| Biometric Identification and Authentication | 979 |
| Understanding the Biometric Verification Process | 980 |
| Accuracy of a Biometric Verification Process | 981 |
| Architecture and Implementation | 983 |
| Operational Model | 987 |
| Biometric SSO Strategy | 991 |
| Multi-factor Authentication Using Smart Cards and Biometrics | 993 |
| Match-on-the-Card Biometrics Strategy | 994 |
| Match-off-the-Card Biometrics Strategy | 994 |
| Best Practices and Pitfalls | 995 |
| Using Smart Cards | 995 |
| Using Biometrics | 996 |
| Pitfalls | 997 |
| References | 998 |

| Index | 999 |