

Core Security Patterns

Chris Steel, Ramesh Nagappan, Ray Lai

TABLE OF CONTENTS

Foreword by Judy Lin (Executive Vice President, Verisign)
Foreword by Joseph Uniejewski (SVP and Chief Technology Officer, RSA Security)
Preface
Acknowledgments
About the Authors

Chapter 1: Security by Default

Business Challenges around Security
What are the Weakest Links?
The Network Services
The Host Operating System (OS)
The Application or Service
The Impact of Application Security
Critical Application Security Flaws and Exploits
The Four W's
WHICH applications are we protecting?
WHO are we protecting the applications from?
WHERE should we protect them?
WHY are we protecting them ?
Strategies for Building Robust Security
Unified Process for Security Design
Design Patterns
Best Practices
Reality Checks
Proactive Assessment
Profiling
Defensive Strategies
Recovery and Continuity Strategies
Proactive and Reactive Security
The Importance of Security Compliance
Sarbanes-Oxley Act
Gramm-Leach-Bliley Act
HIPPA
The Children's Online Privacy Protection Act
EU Directive on Data Protection
California's Notice of Security Breach (1798.29)
Security Compliance in Other Countries
The Importance of Identity Management
Identity Provisioning Services
Identity Data Synchronization Services
Access Management Services

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

Federation Services
Directory Services
Auditing and Reporting Services
Secure Personal Identification
Smart Card Identity
Biometric Identity
RFID-Based Identity
The Importance of Java Technology
Security in the Java Platform
Making Security a “Business Enabler”
Case 1 – Justifying Identity and Access Management
Case 2 – Justifying Proactive Security Approaches
Case 3 – Justifying Security Compliance
Summary
References

Chapter 2: Basics of Security 48

Security Requirements and Goals
Confidentiality
Integrity
Authentication
Authorization
Non-repudiation
The Role of Cryptography in Security 53
Cryptographic Algorithms
The Role of Secure Sockets Layer (SSL)
The Importance and Role of LDAP in Security
The Role of LDAP in J2EE
Common Challenges in Cryptography
Random Number Generation
Key Management
Certificate Revocation Issues
Trust Models
Threat Modeling
Identity Management
Single Sign-on (SSO)
Federated SSO
Summary
References

Chapter 3: The Java 2 Platform Security

Java Security Architecture
The Java Virtual Machine (JVM)
The Java Language
Java Built-in Security Model
Java Applet Security
Signed Applets
Java Web Start Security
Java Security Management tools
Java Keystore
Keytool

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

Policytool
Jarsigner
J2ME Security Architecture
J2ME Configurations
J2ME Profiles
MIDlet Security
Java Card Security Architecture
Understanding Smart Cards
Java Card Technology in Smart Cards
Java Card Platform Security Model
Java Card Applets
Securing the Java Code
Reverse Engineering: Disassembling and Decompiling
Code Obfuscation
Summary
References

Chapter 4: Java Extensible Security Architecture & APIs

Java Extensible Security Architecture
Java Cryptography Architecture (JCA)
JCA Cryptographic Services
Understanding JCA API Programming Model
Java Cryptographic Extensions (JCE)
JCE Cryptographic Service Provider
Understanding the JCE API Programming Model
JCE Hardware Acceleration and Smart Card Support
Using Smart Cards as Java Key Stores
Strong vs. Unlimited Strength Cryptography
Java Certification Path API (CertPath)
Java CertPath – Classes & Interfaces
Java CertPath API Programming Model
Java Secure Socket Extension (JSSE)
JSSE Provider (SunJSSE)
JSSE Classes and Interfaces
Understanding the JSSE API Programming Model
Java Authentication and Authorization Service (JAAS)
JAAS Classes and Interfaces
Understanding the JAAS API Programming Model
Implementing a JAAS LoginModule
Java Generic Secure Services API (JGSS)
Comparing JGSS with JSSE and JAAS
Simple Authentication and Security Layer (SASL)
Java SASL
Summary
References

Chapter 5: J2EE Security Architecture

J2EE Architecture & 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
 - Web tier authentication mechanisms*
 - Using JAAS for Web-tier Authentication*
 - Using Agent based Web-tier Authentication*
 - Single Sign-On Authentication for Web Applications*
 - HTTP Session Tracking, Cookies and URL Rewriting*
 - Web-Tier Authorization mechanisms*
- J2EE Client Security
 - HTTPS Connection*
 - Implementing JAAS Client Callbacks*
 - Secure J2ME Clients*
- EJB Tier or Business Component Security
 - EJB Declarative Authorization*
 - EJB Programmatic Authorization*
 - Anonymous or Unprotected EJB Resources*
 - Principal Delegation in EJBs*
- EIS Integration Tier
 - Securing J2EE Connector and EIS*
 - Securing JMS*
 - Securing JDBC*
- J2EE Architecture - Network Topology
 - Designing for Security with Horizontal Scalability*
 - Designing for Security with Vertical Scalability*
- J2EE Web Services Security – Overview
- Summary
- References

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*

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

Identity and Policy Management
Security Interoperability
Web Services Security Standards
XML Signature
Motivation of XML Signature
The Anatomy of XML Signature
Algorithms
XML Signature Examples
Creating an XML Signature
Verifying and Validating an XML Signature
XML Encryption
Motivation of XML Encryption
The Anatomy of XML Encryption
XML Encryption Algorithms
XML Encryption: Example Scenarios
XML Key Management System (XKMS)
Motivation of XKMS
XKMS Specification Overview
XML Key Information Services (X-KISS)
XML Key Registration Service (X-KRSS)
X-BULK
XKMS Service Security Considerations
OASIS Web Services Security (WS-Security)
Motivation of WS-Security
WS-Security Definitions
Using Digital Signatures in WS-Security
Using Encryption in WS-Security
Using Security Tokens in WS-Security
WS-Security: The Anatomy of SOAP Message Security
WS-I Basic Security Profile
Java-based Web services Security Providers
Sun JWSDP
Sun Java System Access Manager
VeriSign TSIK and XKMS Services
RSA BSAFE Secure-WS
XML-Aware Security Appliances
XML Firewall
Summary
References

Chapter 7: Identity Management Standards and Technologies

Identity Management – Core Issues
Understanding Network Identity and Federated Identity
The Importance of Identity Management
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

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

- 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*
 - Distributed Management Task Force (DMTF)*
 - Parlay Group*
 - Enterprise Privacy Authorization Language (EPAL)*
 - Web Services Policy – WS-Policy and WSPL*
- Introduction to XACML
 - XACML 2.0*
- XACML Data Flow and Architecture
 - XACML Architecture*
- XACML Usage Scenarios
 - Policy Store*
 - Centralizing Security Policy for Web Services Security*
 - Collaborating with SAML*
 - ebXML Registry*
 - Example - XACML Using Sun's XACML Kit*
 - Sample Scenario*
 - Sample Request*
 - Sample Policy*
 - Use of XACML 2.0 with SAML 2.0*
- Summary
- References

**Chapter 8: The Alchemy of Security Design:
Methodology, Patterns, and Reality Checks**

The Rationale

This document is intended for educational and read-only purpose only.
©2005 Core Security Patterns - All rights reserved

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

The Security Wheel
Secure UP
Secure UP - Artifacts
Risk Analysis (RA)
Trade-off Analysis (TOA)
Security Patterns
Understanding Existing Security Patterns
Security Patterns for J2EE, Web Services, Identity Management, and Service Provisioning
Security Patterns Catalog
Security Patterns and their Relationships
Patterns-Driven Security Design
Security Design Processes
Policy Design
Classification and Security Labeling
Application Security Assessment Model
Reality Checks
Security Testing
Black Box Testing
White Box Testing
Adopting a Security Framework
Application Security Provider
Refactoring Security Design
Service Continuity and Recovery
Conclusion
References
Unified Process
Security Principles
Security Patterns
Others

**Chapter 9: Securing the Web Tier:
Design Strategies and Best Practices**

Web-tier Security Patterns
Authentication Enforcer
Authorization Enforcer
Intercepting Validator
Secure Base Action
Secure Logger
Secure Pipe
Secure Service Proxy
Intercepting Web Agent
Best Practices and Pitfalls
Infrastructure
Communication
Application
References

**Chapter 10: Securing the Business Tier:
Design Strategies and Best Practices**
Security Considerations in the Business Tier
Business Tier Security Patterns

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

Audit Interceptor
Container Managed Security
Dynamic Service Management
Obfuscated Transfer Object
Policy Delegate
Secure Service Façade
Secure Session Object

Best Practices and Pitfalls

Infrastructure
Architecture
Policy
Pitfalls

References

Chapter 11: Securing Web Services: Design Strategies and Best Practices

Web Services Security Protocols Stack

Network-Layer Security
Transport-Layer Security
Message-Layer Security

Web Services Security Infrastructure

Network Perimeter Security
XML Firewall
Web Services Infrastructure
Identity Provider
Directory Services

Web Services Security Patterns

Message Interceptor Gateway
Message Inspector
Secure Message Router

Best Practices and Pitfalls

Best Practices
Pitfalls

References

Chapter 12: Securing the Identity: Design Strategies and Best Practices

Identity Management Security Patterns

Assertion Builder Pattern
Single Sign-on (SSO) Delegator Pattern
Credential Tokenizer Pattern

Best Practices and Pitfalls

Best Practices
Pitfalls

References

Chapter 13: Secure Service Provisioning: Design Strategies and Best Practices

Business Challenges

Core Security Patterns
Chris Steel, Ramesh Nagappan, Ray Lai

- Scope of Service Provisioning*
- Relationship with Identity Management*
- A Typical Scenario of User Account Provisioning*
- Current Approaches to User Account Provisioning*
- 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*
- Introduction to SPML
 - Service Provisioning Operations*
 - Features in SPML*
 - Adopting a SAML implementation*
- Service Provisioning Security Pattern
 - Password Synchronizer Pattern*
 - Related Patterns*
- Best Practices and Pitfalls
 - Application Design*
 - Quality of Service*
 - Server Sizing Consideration*
 - Security Risk Mitigation*
- Summary
- References
 - General*
 - Some Security Service Provisioning Vendors*
 - Some Password Management or Password Synchronization Vendor Products*

**Chapter 14: Building End-to-End Security Architecture:
A Case Study**

- Overview
 - Understanding the Security Challenges*
 - Assumptions*
- Use Case Scenarios
- Choosing the Right Methodology
- Identifying the Requirements
 - Identifying the Security Requirements*
 - System Constraints*
 - Security Use Cases*
 - System Environment*
- Application Architecture
 - Conceptual Security Model*
- Security Architecture
 - Risk Analysis and Mitigation*
 - Trade-Off Analysis (TOA)*
 - Applying Security Patterns*
 - Security Architecture – Detailed Components*
- Design
 - Policy Design*
 - Factor Analysis*
 - Security Infrastructure*

- Tier Analysis*
- 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

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)*
- Smart Card-Based Identification and Authentication
 - Architecture and Implementation Model*
 - Operational Model*
 - Using Smart Cards for Physical Access Control*
- Biometric Identification and Authentication
 - Understanding the Biometric Verification Process*
 - Accuracy of a Biometric Verification Process*
 - Architecture and Implementation*
 - Operational Model*
 - Biometric SSO Strategy*
- Multi-factor Authentication Using Smart Cards and Biometrics
 - Match-on-the-Card Biometrics Strategy*
 - Match-off-the-Card Biometrics Strategy*
- Best Practices and Pitfalls
 - Using Smart Cards*
 - Using Biometrics*
- Pitfalls*
- References

DRAFT