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

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

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
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)
      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

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

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

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