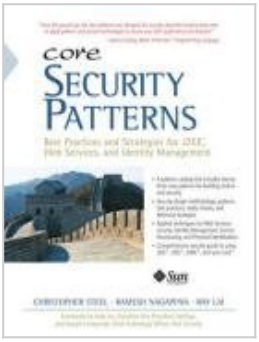

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management

By Christopher Steel, Ramesh Nagappan, Ray Lai

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai

Praise for *Core Security Patterns*

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*

As developers of existing applications, or future innovators that will drive the next generation of highly distributed applications, the patterns and best practices outlined in this book will be an important asset to your development efforts.

--Joe Uniejewski, Chief Technology Officer and Senior Vice President, RSA Security, Inc.

This book makes an important case for taking a proactive approach to security rather than relying on the reactive security approach common in the software industry.

--Judy Lin, Executive Vice President, VeriSign, Inc.

Core Security Patterns provides a comprehensive patterns-driven approach and

methodology for effectively incorporating security into your applications. I recommend that every application developer keep a copy of this indispensable security reference by their side.

--Bill Hamilton, author of *ADO.NET Cookbook*, *ADO.NET in a Nutshell*, and *NUnit Pocket Reference*

As a trusted advisor, this book will serve as a Java developer s security handbook, providing applied patterns and design strategies for securing Java applications.

--Shaheen Nasirudheen, CISSP,Senior Technology Officer, JPMorgan Chase

Like *Core J2EE Patterns*, this book delivers a proactive and patterns-driven approach for designing end-to-end security in your applications. Leveraging the authors strong security experience, they created a must-have book for any designer/developer looking to create secure applications.

--John Crupi, Distinguished Engineer, Sun Microsystems, coauthor of *Core J2EE Patterns*

Core Security Patterns is the hands-on practitioner s 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

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

By Christopher Steel, Ramesh Nagappan, Ray Lai

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai

Praise for *Core Security Patterns*

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*

As developers of existing applications, or future innovators that will drive the next generation of highly distributed applications, the patterns and best practices outlined in this book will be an important asset to your development efforts.

--Joe Uniejewski, Chief Technology Officer and Senior Vice President, RSA Security, Inc.

This book makes an important case for taking a proactive approach to security rather than relying on the reactive security approach common in the software industry.

--Judy Lin, Executive Vice President, VeriSign, Inc.

Core Security Patterns provides a comprehensive patterns-driven approach and methodology for effectively incorporating security into your applications. I recommend that every application developer keep a copy of this indispensable security reference by their side.

--Bill Hamilton, author of *ADO.NET Cookbook*, *ADO.NET in a Nutshell*, and *NUnit Pocket Reference*

As a trusted advisor, this book will serve as a Java developer s security handbook, providing applied patterns and design strategies for securing Java applications.

--Shaheen Nasirudheen, CISSP,Senior Technology Officer, JPMorgan Chase

Like *Core J2EE Patterns*, this book delivers a proactive and patterns-driven approach for designing end-to-end security in your applications. Leveraging the authors strong security experience, they created a must-have book for any designer/developer looking to create secure applications.

--John Crupi, Distinguished Engineer, Sun Microsystems, coauthor of *Core J2EE Patterns*

Core Security Patterns is the hands-on practitioner s 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

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai Bibliography

- Sales Rank: #376724 in Books
- Published on: 2005-10-24
- Ingredients: Example Ingredients
- Original language: English
- Number of items: 1
- Dimensions: 9.62" h x 2.32" w x 7.44" l, 4.15 pounds
- Binding: Hardcover
- 1088 pages

Editorial Review

From the Back Cover

Praise for *Core Security Patterns*

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*

As developers of existing applications, or future innovators that will drive the next generation of highly distributed applications, the patterns and best practices outlined in this book will be an important asset to your development efforts.

--Joe Uniejewski, Chief Technology Officer and Senior Vice President, RSA Security, Inc.

This book makes an important case for taking a proactive approach to security rather than relying on the reactive security approach common in the software industry.

--Judy Lin, Executive Vice President, VeriSign, Inc.

Core Security Patterns provides a comprehensive patterns-driven approach and methodology for effectively incorporating security into your applications. I recommend that every application developer keep a copy of this indispensable security reference by their side.

--Bill Hamilton, author of *ADO.NET Cookbook*, *ADO.NET in a Nutshell*, and *NUnit Pocket Reference*

As a trusted advisor, this book will serve as a Java developer s security handbook, providing applied patterns and design strategies for securing Java applications.

--Shaheen Nasirudheen, CISSP,Senior Technology Officer, JPMorgan Chase

Like *Core J2EE Patterns*, this book delivers a proactive and patterns-driven approach for designing end-to-end security in your applications. Leveraging the authors strong security experience, they created a must-have book for any designer/developer looking to create secure applications.

--John Crupi, Distinguished Engineer, Sun Microsystems, coauthor of *Core J2EE Patterns*

Core Security Patterns is the hands-on practitioner s 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

About the Author

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).

"The problems that exist in the world todaycannot be solved by the level of thinking that created them."--Albert Einstein

Security now has unprecedented importance in the information industry. It compels every business and organization to adopt proactive or reactive measures that protect data, processes, communication, and resources throughout the information lifecycle. In a continuous evolution, every day a new breed of business systems is finding its place and changes to existing systems are becoming common in the industry. These changes are designed to improve organizational efficiency and cost effectiveness and to increase consumer satisfaction. These improvements are often accompanied by newer security risks, to which businesses must respond with appropriate security strategies and processes. At the outset, securing an organization's information requires a thorough understanding of its security-related business challenges, potential threats, and best practices for mitigation of risks by means of appropriate safeguards and countermeasures. More importantly, it becomes essential that organizations adopt trusted proactive security approaches and enforce them at all levels--information processing, information transmittal, and information storage.

What This Book Is About

This book is meant to be a hands-on practitioner's guide to security. It captures a wealth of experience about using patterns-driven and best practices-based approaches to building trustworthy IT applications and services. The primary focus of the book is on the introduction of a security design methodology using a proven set of reusable patterns, best practices, reality checks, defensive strategies, and assessment checklists that can be applied to securing J2EE applications, Web Services, Identity Management, Service Provisioning, and Personal Identification. The book presents a catalog of 23 new security patterns and 101 best practices, identifying use case scenarios, architectural models, design strategies, applied technologies, and validation processes. The best practices and reality checks provide hints on real-world deployment and end-user experience of what works and what does not. The book also describes the architecture, mechanisms, standards, technologies, and implementation principles of applying security in J2EE applications, Web Services, Identity Management, Service Provisioning, and Personal Identification and explains the required fundamentals from the ground up.

Starting with an overview of today's business challenges, including the identification of security threats and exploits and an analysis of the importance of information security, security compliance, basic security concepts, and technologies, the book focuses in depth on the following topics:

- Security mechanisms in J2SE, J2EE, J2ME, and Java Card platforms
- Web Services security standards and technologies
- Identity Management standards and technologies
- Security design methodology, patterns, best practices, and reality checks
- Security patterns and design strategies for J2EE applications
- Security patterns and design strategies for Web Services
- Security patterns and design strategies for Identity Management
- Security patterns and design strategies for Service Provisioning
- Building an end-to-end security architecture--case study
- Secure Personal Identification strategies for using Smart Cards and Biometrics

The book emphasizes the use of the Java platform and stresses its importance in developing and deploying

secure applications and services.

What This Book Is Not

While this book is heavily based on Java technologies, we do not describe the specific Java APIs intended for basic J2EE application development (e.g., JSPs, Servlets, and EJB). If you wish to learn the individual API technologies, we highly recommend the J2EE blueprints, tutorials, and recommended books on the official Java home page at http://java.sun.com.

We use UML diagrams to document the patterns and implementation strategies. If you wish to learn the UML basics, please refer to *The Unified Modeling Language User Guide* by Grady Booch, James Rumbaugh, and Ivar Jacobson (Addison-Wesley, 1999).

Who Should Read This Book?

This book is meant for all security enthusiasts, architects, Java developers, and technical project managers who are involved with securing information systems and business applications. The book is also valuable for those who wish to learn basic security concepts and technologies related to Java applications, Web Services, Identity Management, Service Provisioning, and Personal Identification using Smart Cards and Biometrics.

The book presumes that the reader has a basic conceptual knowledge of development and deployment of business applications using Java. We have attempted to write this book as an introduction to all security mechanisms used in the design, architecture, and development of applications using the Java platform. We intended our use of the methodology, patterns, best practices, and pitfalls to be an invaluable resource for answering the real-world IT security problems that software architects and developers face every day.

Most of us no longer have time to read a software development book from cover to cover. Therefore, we have broken this book into different technology parts; the book may thus be read in almost in any sequence according to the reader's specific interests.

How This Book Is Organized

The content of this book is organized into seven parts:

Part I: Introduction

Part I introduces the current state of the industry, business challenges, and various application security issues and strategies. It then presents the basics of security.

Chapter 1: Security by Default

This first chapter describes current business challenges, the weakest links of security, and critical application flaws and exploits. It introduces the security design strategies, concepts of patterns-driven security development, best practices, and reality checks. It also highlights the importance of security compliance, Identity Management, the Java platform, and Personal Identification technologies such as Smart Cards and Biometrics. In addition, this chapter presents security from a business perspective and offers recommendations for making a case for security as a business enabler that delivers specific benefits.

Chapter 2: Basics of Security

This chapter introduces the fundamentals of security, including the background and guiding principles of various security technologies. It also provides a high-level introduction to securing applications by using popular cryptographic techniques. In addition, it discusses basic concepts about the role of directory services

and identity management in security.

Part II: Java Security Architecture and Technologies

Part II provides in-depth coverage and demonstration of security practices using J2SE, J2EE, J2ME, and Java Card technologies. It delves into the intricate details of Java platform security architecture and its contribution to the end-to-end security of Java-based application solutions.

Chapter 3: The Java 2 Platform Security

This chapter explores the inherent security features of the various Java platforms and the enabling of Java security in stand-alone Java applications, applets, Java Web start (JNLP) applications, J2ME MIDlets, and Java Card applets. It also explores how to use Java security management tools to manage keys and certificates. This chapter also discusses the importance of applying Java code obfuscation techniques.

Chapter 4: Java Extensible Security Architecture and APIs

This chapter provides an in-depth discussion of the Java extensible security architecture and its API framework as well as how to utilize those API implementations for building end-to-end security in Java-based application solutions. In particular, the chapter illustrates how to use Java security APIs for applying cryptographic mechanisms and public-key infrastructure, how to secure application communica*tion, and how to plug in third-party security providers in Java-based applications.

Chapter 5: J2EE Security Architecture

This chapter explains the J2EE security architecture and mechanisms and then illustrates how to apply them in the different application tiers and components. It features in-depth coverage of the J2EE security mechanisms applied to Web components (JSPs, Servlets, and JSFs), business components (EJBs), and integration components (JMS, JDBC, and J2EE connectors). This chapter also highlights J2EE-based Web services security and relevant technologies. In addition, it illustrates the different architectural options for designing a DMZ network topology that delivers security to J2EE applications in production.

Part III: Web Services Security and Identity Management

Part III concentrates on the industry-standard initiatives and technologies used to enable Web services security and identity management.

Chapter 6: Web Services Security--Standards and Technologies

This chapter explains the Web services architecture, its core building blocks, common Web services security threats and vulnerabilities, Web services security requirements and Web services security standards and technologies. It provides in-depth details about how to represent XML-based security using industry-standard initiatives such as XML Signature, XML Encryption, XKMS, WS-Security, SAML Profile, REL Profile and WS-I Basic Security Profile. In addition, this chapter also introduces the Java-based Web services infrastructure providers and XML-aware security appliances that facilitate support for enabling security in Web services.

Chapter 7: Identity Management--Standards and Techn...

Users Review

From reader reviews:

Roger Thomas:

What do you regarding book? It is not important to you? Or just adding material when you really need something to explain what yours problem? How about your free time? Or are you busy individual? If you don't have spare time to accomplish others business, it is give you a sense of feeling bored faster. And you have time? What did you do? All people has many questions above. They must answer that question because just their can do this. It said that about guide. Book is familiar in each person. Yes, it is right. Because start from on jardín de infancia until university need this Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management to read.

Samuel Freeman:

Reading a book can be one of a lot of action that everyone in the world likes. Do you like reading book therefore. There are a lot of reasons why people enjoy it. First reading a publication will give you a lot of new information. When you read a reserve you will get new information since book is one of a number of ways to share the information or maybe their idea. Second, looking at a book will make you more imaginative. When you studying a book especially hype book the author will bring you to definitely imagine the story how the figures do it anything. Third, you may share your knowledge to some others. When you read this Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management, you could tells your family, friends and also soon about yours e-book. Your knowledge can inspire the others, make them reading a guide.

Keith Mayo:

The guide with title Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management includes a lot of information that you can discover it. You can get a lot of benefit after read this book. That book exist new expertise the information that exist in this publication represented the condition of the world now. That is important to yo7u to learn how the improvement of the world. This kind of book will bring you within new era of the glowbal growth. You can read the e-book with your smart phone, so you can read it anywhere you want.

Jason Howell:

Reading a book to get new life style in this yr; every people loves to go through a book. When you read a book you can get a great deal of benefit. When you read guides, you can improve your knowledge, due to the fact book has a lot of information upon it. The information that you will get depend on what kinds of book that you have read. If you would like get information about your review, you can read education books, but if you act like you want to entertain yourself you can read a fiction books, this kind of us novel, comics, and soon. The Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management offer you a new experience in studying a book.

and Strategies for J2EE, Web Services, and Identity Management
By Christopher Steel, Ramesh Nagappan, Ray Lai
#QAMNX2GOPBS

Read Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai for online ebook

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai books to read online.

Online Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai ebook PDF download

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai Doc

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai Mobipocket

Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management By Christopher Steel, Ramesh Nagappan, Ray Lai EPub