Sun公司核心技术丛书

Java平台的设计初衷就是为了安全。本书指导读者如何应用模式和经过实践检验的技术来保护J2EE应用等解决方案。

——James Gosling (Java编程语言之父)

# 安全模式

## J2EE、Web服务和身份管理最佳实践与策略

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

Christopher Steel
(美) Ramesh Nagappan 著
Ray Lai

陈秋萍 罗邓 袁国忠 等译

- 包含23种构建端到端安全的新模式
- 安全设计方法、模式、最佳实践、可行性检查和防范策略
- 实用的Web服务安全、身份管理、服务供应和身份识别技巧
- 使用J2SE、J2EE、J2ME和Java Card的综合安全指南

VeriSign执行副总裁Judy Lin和RSA首席技术官Joseph Uniejewski作序

机械工业出版社
China Machine Press

Sun 公司核心技术丛书



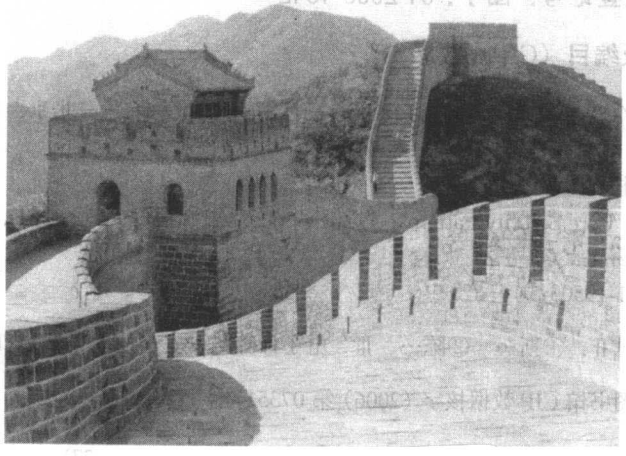
# 安全模式

## J2EE、Web服务和身份管理最佳实践和策略

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

Christopher Steel
（美） Ramesh Nagappan 著
Ray Lai

陈秋萍 罗邓 袁国忠 等译



机械工业出版社
China Machine Press

本书汇集了作者在安全领域的丰富经验，全面阐述 Java 应用安全的基本知识和结构化安全设计方法。本书介绍如何使用模式驱动和最佳实践构建可靠应用和服务。全书分为两大部分，第一部分介绍用于 J2EE 应用、Web 服务、身份管理、服务供应和身份识别的安全架构、机制、标准、技术和实现原则，第二部分介绍 23 种全新的安全模式和 101 项最佳实践，帮助开发人员构建端到端安全 J2EE 应用。

本书可供从事计算机安全技术工作的开发人员、设计人员和管理人员参考。



**本书版权登记号：图字：01-2006-1942**

**图书在版编目（CIP）数据**

安全模式/（美）斯蒂尔（Steel, C.）等著；陈秋萍等译. －北京：机械工业出版社，2006.8

（Sun 公司核心技术丛书）

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

ISBN 7-111-19503-5

Ⅰ. 安…　Ⅱ. ①斯…　②陈…　Ⅲ. 电子计算机－安全技术　Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2006）第 073517 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）

责任编辑：陈冀康

北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行

2006 年 9 月第 1 版第 1 次印刷

186mm×240mm · 37.25 印张

定价：75.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

# 对本书的赞誉

Java 向应用开发人员提供了不可或缺的安全机制，从而避免了其他语言中常见的严重安全问题。然而，语言只能做到这样的程度；开发人员必须了解应用的安全需要，并使用 Java 提供的特性满足这些需要。本书致力于解决安全问题的这两个方面，指导开发人员创建更安全的应用。

——Whitfield Diffie(公钥加密算法发明人)

这是一本关于安全模式的综合性图书，而对安全编程而言，安全模式是不可或缺的。

——Li Gong(Sun 公司前首席架构师和《Inside Java 2 Platform Security》作者之一)

已有应用的开发者或推动下一代分布式应用的革新者最需要本书介绍的信息和最佳实践，这将是你完成开发工作的重要资产。

——Joe Uniejewski(RSA Security 公司 CTO 兼高级副总裁)

本书证明了一个重要的事实：应采用主动的安全方法，而不能像软件业通常的那样依赖于被动安全方法。

——Judy Lin(VeriSign 公司执行副总裁)

本书有效地在应用中集成安全提供了一种模式驱动的综合方法。建议每位应用开发人员都将这本必不可少的安全参考书放在身边。

——Bill Hamilton(《ADO.NET Cookbook》、《ADO.NET in a Nutshell》和《NUnit Pocket Reference》的作者)

本书提供了确保 Java 应用安全的实用模式和设计策略，是 Java 开发人员的安全手册和可信赖的参谋。

——Shaheen Nasirudheen(JPMorgan Chase 高级技术主管，CISSP)

# 译 者 序

在信息行业，安全从来没有像今天这样重要。为确保组织的信息安全，组织必须深刻理解与安全相关的业务挑战、潜在威胁以及能够降低风险的最佳实践；更重要的是，组织必须采取可靠的主动安全方法，并在信息处理、传输和存储各个层面实施它们。安全不再是出现问题或遭受攻击后的亡羊补牢，而必须未雨绸缪。安全已日渐成为应用开发过程中不可分割的一部分。

本书旨在为安全从业者提供实用指南。它包含大量使用模式驱动和最佳实践构建可靠的 IT 应用和服务的经验之谈。本书介绍一种安全设计方法，该方法使用一组经过实践检验的可重用模式、最佳实践、可行性检查、防范策略和评估核对表，以确保 J2EE 应用、Web 服务、身份管理、服务供应和身份识别的安全。本书首先讨论用于 J2EE 应用、Web 服务、身份管理、服务供应和身份识别的安全架构、机制、标准、技术和实现原则；然后介绍 23 种全新的安全模式和 101 项最佳实践。

本书第 1～7 章由罗邓组织翻译，参加翻译的人员包括乔红宇、由宗铭、付静波、王晖、郭亮、林爱生等；第 8～15 章由陈秋萍组织翻译，参加翻译的人员包括黄挺、王进征、邓郑祥、李佩乾、宫晋博、刘丽风、侯学民、蒋蓉芳等；最后，由袁国忠、张海燕负责全书的统稿和译审工作。

衷心感谢机械工业出版社华章分社编辑所做的大量工作。没有他们的辛勤劳动，本书不可能如此顺利、快捷地出版。

由于翻译量大、译者水平有限，译文中欠妥和纰漏之处在所难免，恳请读者不吝赐教和指正。

译 者

2006 年 6 月

# Judy Lin 序

1869 年 5 月 10 日，太平洋联合铁路和太平洋中央铁路接轨，形成一条横跨美国大陆的铁路系统。这离第一条公用铁路(连接利物浦和曼彻斯特的 35 英里铁轨)通车不到 40 年。此时，从纽约到旧金山只需几天就可以到达，而不像从前需要几个月。

当时的铁路就像现在的 Internet。快捷、价廉、可靠的运输让所有人受益，但跨越高山、穿越河流建造数千英里的铁路面临重大挑战。横贯美国的铁路必将出现，对此几乎无人持怀疑态度，但尝试去实现这种目标需要脚踏实地和奋斗勇气。

人们常将 Internet 同铁路相比，因为它们都在相应的时代给经济和社会带来了重大转变。可能正是由于这种原因，它们都经历了怀疑、狂热、投机热潮和失望的过程。倘若 1845 年铁路建设的狂潮成为铁路建设的终点，那么 1869 年横贯美国的铁路将不会出现。

在 Internet 时代，业务应用的 Internet 基础设施相当于横贯美国的铁路。每天都有数百万工作人员坐在电脑前生成订单和发票，这些订单和发票被发送给更多的工作人员，而后者的大部分工作时间都用在将这些信息输入到更多的计算机中。

10 年前，几乎所有业务都以这种方式开展。而现在，很大一部分业务都是通过 Web 完成的，消费者已习惯在网上订购图书、服装和旅行服务，并期望客户服务能够得到改善。

在 .com 时代，电子商务是一个时髦的话题，似乎 Internet 将带来一种全新的商务形式，并将迅速取代传统形式。虽然很多基于这种错误假设而组建的公司纷纷破产，但电子商务却空前繁荣。在 .com 繁荣顶峰的 2000 年，VeriSign 签发了 27.5 万份 SSL 证书，处理了 3500 万项交易支付，总价值 13 亿美元；而在 2003 年，VeriSign 签发了 39 万份证书，处理了 3.45 亿项交易支付，总价值为 250 亿美元。

现在人们知道，将企业归类到“电子商务”就像将其归类到“电话商务”或“传真商务”一样毫无意义。在每个经济部门，企业无论规模大小都在使用 Internet 和 Web，水管工人和木匠通过网站做广告已司空见惯。

显然，新出现的 Internet 业务基础设施将连接起来，自动化电子流程将取代当前的传真方式；当这种连接最终完成时，它将像铁路一样给商务带来根本性转变。然而，要使这些成为现实，必须解决两个重要问题。

第一个问题是复杂性。虽然要成功进行网上零售需要克服很多实际困难，但传统的邮购业务流程已经有 100 多年的历史。要通过网站而不是信件或电话下订单，必须修改人们已经非常熟悉的业务流程。与开发支持网上零售的系统相比，编写支持 B2B 交易的系统要复杂得多；B2B 交易千变万化，企业为支持它们而制定的内部流程也是如此。

铁路工程师通过标准化解决了类似的问题。按专用设计建造的火车头必须由专家来维修，如果零件坏了，为制造替换零件，需要使用几千英里外的原厂设备。理论上来说，可互换零件意味着火车头出现故障时，可以使用库存标准零件来修理。

软件重用策略适用于构建任何应用系统，编写 B2B 应用系统时它也不可或缺。如果使用专用技术来构建系统，除需要的时间更长、成本更高外，将更难以管理、维护和扩展。

软件模式提供了构建系统的现成模板；而行业标准确保软件能够跨实现平台进行交互。对于需要同合作伙伴通信的业务系统来说，互操作性是不可或缺的。

需要解决的第二个问题是安全。除非对风险有全面的认识，否则企业绝不会为进行网上交易而拿声誉和财产去冒险。

对于电子系统而言，安全性仅仅局限于现有水平是不够的。与被取代的纸质流程相比，电子系统对安全的要求无疑要高得多。

今天，铁路是最安全的旅行方式之一，但并非一开始就如此。与当今的 Internet 安全一样，铁路安全也曾被人视为难以解决的问题。在维多利亚时代，火车出轨的频率令人恐怖，铁路桥可能坍塌、货物可能着火，几乎任何方面都可能出问题。最终，工程师认识到，导致这些事故的罪魁祸首是设计缺陷，而并非运气不好。安全成为铁路工程考虑的核心因素，而不是事故后的亡羊补牢。

通过采用标准化，可替换零件在提高铁路安全方面发挥了重要作用。无论是设计桥梁的支撑架还是机车的刹车，使用标准工程设计模式手册都可以提高速度并降低出错概率。

在安全领域，一种被人们长期接受的观点是：与几乎未经外部人员审核的规范相比，经广泛审核的公开规范出现问题的概率更低。在现代软件工程中，SSL 和 SAML 等标准安全协议相当于以前的标准工程零件手册。

本书应运而生，它解决了部署 Internet 业务基础设施面临的挑战。安全模式描述了一种在应用中提供安全的方式，它是可重用和可靠的模式。通过采用标准化软件模式原则，可以构建有助于驱动 Internet 业务的引擎。

具体地说，本书证明了一个重要的事实：应采用主动的安全方法，而不能像软件业通常的那样依赖于被动安全方法。大多数安全问题方法都属于“后发制人”的方法，即受到攻击后才做出反应。采用被动安全方法失去了主动权，将优势拱手让给了攻击者。要将问题消灭在萌芽状态，必须采用主动的安全方法。

当前，垃圾邮件以及与垃圾邮件相关的欺骗(垃圾邮件诈骗)泛滥成灾，这折射出了被动安全方法的后果。当系统规模增大，攻击者有利可图时，任何系统都必须在部署基础设施时就采取应对攻击的措施。

虽然电子邮件和 Web 应用非常多，但电子邮件只不过是一种消息收发协议，而 Web 只不过是一种发布协议。创建 Internet 业务基础设施面临的挑战要复杂和困难得多。显然，任何软件开发人员都必须获得最佳的安全专业知识，但在这些知识为稀缺资源的情况下，如何获取这些知识呢?

通过在应用中重用熟悉的安全组件，应用设计人员可以利用重要的行业专家拥有的经验和知识，从而控制风险。另外，还可以使用系统性框架，以提高可预测性并降低开发成本。

计算机网络架构已跨越周边安全模型的边界，这并不意味着防火墙将消失以及周边安全无关紧要。从安全的角度看，这意味着跨越防火墙在企业之间开展的工作与在安全周边内开展的工作同样重要，因此必须理解端到端安全模型及其用途。

在铁路时代，企业已意识到有些安全任务(如押运钞票)最好交给专家去做。这也适用于计算机安全领域，下面的做法既没有必要也不会收到令人满意的效果：每家公司都连接到支付基础设施、运行 PKI 或其他身份基础设施、管理自己的安全基础设施以及执行与安全相关的任务。通过使用标准 Web 服务基础设施，可以将这些安全任务交给专家去完成。

采用业务应用基础设施的优点已得到广泛认可。本书将为读者提供构建安全基础设施所需的工具，我对此深信不疑!

Judy Lin

VeriSign 执行副总裁

# Joe Uniejewski 序

在过去的 20 年中，无论是在网络级还是应用级，计算架构和技术都发生了巨大变化。很多工作都是在网络基础设施层完成的：入侵检测、反病毒、防火墙、VPN、服务质量、策略管理和实施、拒绝访问攻击的检测和防范以及端点安全。这些是必不可少的但还不够，必须在设计应用安全和部署应用安全基础设施方面做更大的努力。网络安全侧重于检测、防范和保护，而应用安全侧重于支持(enablement)以及遵守法规(如 Sarbanes-Oxley、HIPPA、GLB 等法案)。

无论是对于技术还是对于业务，都必须确保应用安全。安全程度高的公司将拥有竞争优势，能够降低成本并打入新市场，以及改善用户体验；无论是 B2B 应用(如供应链应用)还是 B2C 应用(如金融服务、电子零售)皆如此。随着网络连接到全球的各个角落以及带宽不断增加，开展业务的方式发生了重大转变，访问信息和资源的方式前所未有，安全已成为用户、企业、政府以及应用提供者和开发人员面临的重要问题。

基于 J2EE 和 Web 服务的松散耦合分布式应用已成为开发基于标准的多厂商应用的首选模型，而主要的应用开发和部署平台提供的安全水平越来越高。安全不再是出现问题或攻击后添加的一层或多层，而必须纳入设计的考虑之中，它是应用开发过程中不可分割的一部分。安全是事先需要考虑的因素，而不是事后的亡羊补牢。

本书全面介绍了开发应用安全策略和实现时需要考虑的各种要素和因素。作为网络计算、分布式应用和 Java 系统的先锋和领先者，Sun Microsystems 在这个领域处于独一无二的地位。作为已有应用的开发者或推动下一代分布式应用的革新者，本书介绍的信息和最佳实践将是你完成开发工作的重要资产。确保企业和最终用户自信、安全地体验 Internet 的重任将由你们承担。

Joe Uniejewski
RSA Security 公司 CTO 兼负责企业开发的高级副总裁

# 前　言

现有的思考水平无法解决它所提出的问题。
——阿尔伯特·爱因斯坦

在信息行业，安全从未像今天这样重要。这促使所有企业和组织都采取主动或被动的措施，在整个信息生命周期内保护数据、流程、通信和资源。在不断发展的信息行业，每天都有新的业务系统面世，对现有系统进行修改随处可见。这些修改旨在提高组织效率和成本效率，以及消费者的满意度。这些改进常常带来新的安全风险，企业必须采取合适的安全策略和规程来应对安全风险。为确保组织的信息安全，必须深入了解与安全相关的业务挑战和潜在威胁，广泛认识为采取保护和应对措施降低风险的最佳实践。更重要的是，组织必须采取可靠的主动安全方法，并在各个层面(信息处理、信息传输和信息存储)实施它们。

## 本书内容

本书旨在为安全从业者提供实用指南，提供大量使用模式驱动和基于最佳实践的方法来构建可靠的IT应用和服务的经验之谈。本书重点介绍一种安全设计方法，它使用一组经过实践检验的可重用模式、最佳实践、可行性检查、防范策略和评估核对表，确保J2EE应用、Web服务、身份管理、服务供应和身份识别的安全。本书介绍了23种全新的安全模式和101项最佳实践，讨论了用例场景、架构模型、设计策略、实用技术和验证过程。最佳实践和可行性检查从实际部署和最终用户体验的角度出发，阐述了哪些方法奏效和哪些方法不可取。本书还讨论了为J2EE应用、Web服务、身份管理、服务供应和身份识别提供安全的架构、机制、标准、技术和实现原则，并全面阐述了所需的基本知识。

本书首先概述当今的业务挑战(包括安全威胁和攻击)，分析信息安全和遵守安全法规的重要性，讨论基本安全的概念和技术。本书深入探讨下述主题：

- J2SE、J2EE、J2ME和Java Card平台中的安全机制
- Web服务安全标准和技术
- 身份管理标准和技术
- 安全设计方法、模式、最佳实践和可行性检查
- 用于J2EE应用的安全模式和设计策略
- 用于Web服务的安全模式和设计策略
- 用于身份管理的安全模式和设计策略
- 用于服务供应的安全模式和设计策略
- 用实例介绍构建端到端安全架构
- 使用智能卡和生物特征技术的安全身份识别策略

本书针对的是Java平台，并突出Java平台在开发和部署安全的应用和服务中的重要性。

## 本书不介绍的内容

虽然本书依赖于大量的Java技术，但并没有介绍用于开发J2EE应用(如JSP、Servlet和EJB)的Java API。如果读者要学习各种API技术，强烈推荐参考Java官方网站中的J2EE计划、教程及推荐的图书，其网址为http://java.sun.com。

本书使用 UML 图描述模式和实现策略。如果读者要学习 UML 基本知识，请参阅 Grady Booch、James Rumbaugh 和 Ivar Jacobson 编写的《UML 用户手册》[⊖]。

## 本书面向的读者

本书可供负责确保信息系统和业务应用安全的架构师、Java 开发人员和技术项目经理使用。对于想了解与 Java 应用、Web 服务、身份管理、服务供应和使用智能卡和生物特征进行身份识别相关的安全概念和技术的读者，本书也很有参考价值。

本书假设读者具备使用 Java 开发和部署业务应用的基本知识。本书旨在介绍使用 Java 平台设计、构建和开发应用时用到的所有安全机制，阐述如何使用设计方法、模式和最佳实践以及需要注意的陷阱，为软件架构师和开发人员提供宝贵的参考资料，以解决每天面临的实际 IT 安全问题。

大多数人都没有时间完整地阅读软件开发书籍，因此本书分为几个不同的技术部分，让读者能够根据兴趣以任意顺序阅读。

## 本书的组织结构

本书分为七部分。

**第一部分：引言**

介绍当前行业状况、业务挑战以及各种应用安全问题和应对策略，阐述有关安全的基本知识。

*第 1 章：默认安全*

描述当前业务挑战、最薄弱的安全环节和严重的应用缺陷及漏洞。本章简要介绍了安全设计策略、模式驱动的安全开发概念、最佳实践和可行性检查；阐述了遵守安全法规的重要性以及身份管理、Java 平台和身份识别技术(如智能卡和生物特征)；从业务的角度讨论了安全，并展示安全技术可以推进业务，并能够带来收益。

*第 2 章：安全基本知识*

本章介绍有关安全的基本知识，其中包括各种安全技术的背景知识和指导原则；概述使用流行的加密技术确保应用的安全，还讨论目录服务和身份管理在安全中的作用。

**第二部分：Java 安全架构与技术**

这部分深入介绍和演示了使用 J2SE、J2EE、J2ME 和 Java Card 技术的安全实践；深入研究 Java 平台安全架构中复杂的技术细节，及其在为基于 Java 的应用提供端到端安全解决方案中的作用。

*第 3 章：Java 2 平台安全*

本章讨论了各种 Java 平台固有的安全特性，以及如何在独立的 Java 应用、applet、Java Web start (JNLP)应用、J2ME MIDlet 和 Java Card applet 中实现 Java 安全；阐述如何使用 Java 安全管理工具来管理密钥和证书；还讨论使用 Java 代码混淆技术的重要性。

*第 4 章：Java 可扩展安全与 API*

本章深入讨论 Java 可扩展安全架构及其 API 框架，以及如何使用这些 API 实现在基于 Java 的应用解决方案中构建端到端安全。具体地说，本章演示如何使用 Java 安全 API 来应用加密机制和公钥基础设施，如何确保应用通信的安全。

*第 5 章：J2EE 安全架构*

本章解释 J2EE 安全架构和机制以及如何将其应用于各种应用层和组件中；深入讨论应用于 Web 组件(JSP、Servlet 和 JSF)、业务组件(EJB)和集成组件(JMS、JDBC 和 J2EE 连接器)的 J2EE 安全机制；阐述基

---

⊖ 该书已由机械工业出版社引进出版，ISBN：7-111-07564。

于 J2EE 的 Web 服务安全及相关技术；还阐述各种用于设计 DMZ 网络拓扑的架构方案，以便在产品环境中确保 J2EE 应用的安全。

**第三部分：Web 服务安全和身份管理**

这部分重点介绍支持 Web 服务安全和身份管理的行业标准计划和技术。

第 6 章：Web 服务安全标准与技术

本章解释 Web 服务架构及其核心构件、常见的 Web 服务安全威胁和攻击、Web 服务安全需求以及 Web 服务安全标准和技术；深入介绍如何使用诸如 XML 签名、XML 加密、XKMS、WS-Security、SAML 概要、REL 概要和 WS-I 基本安全概要等行业标准计划来表示基于 XML 的安全；还介绍基于 Java 的 Web 服务基础设施提供者，以及有助于确保 Web 服务安全的支持 XML 的安全设备。

第 7 章：身份管理标准与技术

本章深入讨论对管理身份信息来说不可或缺的标准和技术；介绍身份管理面临的挑战，以及实现基于标准的身份管理的架构模型；还演示如何使用 SAML、XACML 和 Liberty Alliance 规范等 XML 标准来实现联合身份管理和支持身份的服务。

**第四部分：安全设计方法、模式和可行性检查**

这部分描述一种安全设计方法并介绍一种模式驱动的安全设计方法，在软件设计和开发过程中可以使用它们。

第 8 章：安全设计点金术：方法、模式和可行性检查

本章首先简要地讨论使用安全设计方法的重要性，然后详细地讨论安全设计过程：在整个软件生命周期内确定并应用安全模式，包括架构、设计、开发、部署、生产和废弃。该章描述安全设计中的各种角色及其职责，解释风险分析、权衡分析、效果分析、因素分析、层分析、威胁剖析和信任建模等核心安全分析过程。还介绍安全设计模式目录和安全评估核对表；在应用开发过程中，可以使用它们来解决安全需求或提供解决方案。

**第五部分：设计策略和最佳实践**

这部分介绍安全模式、策略和最佳实践，并按 J2EE 应用层、Web 服务、身份管理和服务供应将它们进行分类。

第 9 章：确保 Web 层安全：设计策略与最佳实践

本章介绍 7 种安全模式，它们与设计和部署 J2EE Web 层和表示层组件相关，如 JSP、Servlet 以及其他相关组件。每种模式都针对一种与 Web 层或表示层逻辑相关的常见问题，描述演示各种实现策略的设计解决方案；阐述使用模式的效果，强调使用模式时的安全因素和相关风险，并使用可行性检查验证模式的适用性。该章还列出了用于确保 J2EE Web 组件和基于 Web 的应用的最佳实践。

第 10 章：确保业务层安全：设计策略与最佳实践

本章介绍 7 种安全模式，它们与设计和部署 J2EE 业务层组件相关，如 EJB、JMS 以及其他相关组件。每种模式都针对一组与业务层相关的安全问题，描述演示各种实现策略的设计解决方案以及使用模式的效果；强调使用业务层安全模式的安全因素和相关风险，并使用可行性检查验证模式的适用性。该章还列出用于确保 J2EE 业务组件安全的最佳实践和陷阱。

第 11 章：确保 Web 服务的安全：设计策略与最佳实践

本章介绍 3 种安全模式，它们与设计和部署 Web 服务相关。首先讨论 Web 服务安全基础设施和有助于确保安全的重要组件。然后描述各种安全模式，每种模式都针对与业务层相关的安全问题，描述演示各种实现策略的设计解决方案以及使用 Web 服务模式的效果；强调使用安全模式的安全因素和相关风险，并使用可行性检查验证模式的适用性。最后，本章列出了用于确保 Web 服务安全的最佳实践和陷阱。

第 12 章：确保身份安全：设计策略与最佳实践

本章介绍 3 种与身份管理相关的安全模式。每种模式都针对一个身份管理问题，描述演示各种实现策略的设计解决方案以及使用模式的效果；强调使用业务层模式的安全因素和相关风险，并使用可行性检查验证模式的适用性。最后，列出用于身份管理的最佳实践。

第 13 章：安全服务供应：设计策略与最佳实践

本章首先简要地讨论业务挑战、服务供应的范围以及服务供应与身份管理的关系，然后详细介绍用户账户供应过程并讨论各种架构和应用场景。该章介绍一种用户账户供应的安全模式，并阐述实现策略和使用该模式的效果；然后指出使用该模式的安全因素和相关风险，并使用可行性检查验证该模式的适用性。还介绍 SPML 及其同服务供应的关系。最后，本章列出服务供应最佳实践。

**第六部分：综合应用**

这部分通过案例研究说明实际的安全实现情形，描述如何使用模式和最佳实践完成安全设计过程。

第 14 章：构建端到端安全架构：案例研究

本章通过一个实际的 Web 门户，说明如何使用本书介绍的安全设计方法、设计模式和最佳实践来定义和实现端到端安全解决方案。本章通过完成整个安全设计过程，演示如何分析和识别风险，如何进行权衡，如何选择并应用安全模式，以及如何执行因素分析、层分析、威胁剖析和可行性检查。还详细介绍如何采用模式驱动的设计过程和注意事项，并描述如何协调不同逻辑层的安全以提供端到端安全。

**第七部分：使用智能卡和生物特征的身份识别**

这部分深入讨论使用智能卡和生物特征的身份识别，深入研究使用智能卡、生物特征和结合使用它们时的支持技术、架构和实现策略。

第 15 章：使用智能卡和生物特征的身份识别

本章探讨使用智能卡和生物特征实现身份识别和认证的概念、技术、架构策略和最佳实践。首先讨论融合物理和逻辑访问控制的重要性，以及智能卡和生物特征在身份识别中的作用；然后阐述在基于 J2EE 的企业应用、UNIX 和 Windows 环境中支持基于智能卡和生物特征认证的架构和实现策略；最后，列出将智能卡和生物特征用于安全身份识别的最佳实践。

## 配套网站

本书的官方配套网站为 www.coresecuritypatterns.com，书中所有的示例都可从这里下载。该网站还包含勘误、修改、修订以及推荐读物和参考资源。

在 Prentice Hall 出版社的网站中，本书英文版的网址为 http://www.phptr.com/title/0131463071。

## 反馈

我们非常欢迎读者的反馈，读者可以在配套网站链接的讨论论坛上发布问题。读者也可以通过电子邮件与作者联系，作者的电子邮件地址可在配套网站上找到。该网站还包括一个可随便订阅和参与的读者论坛，读者可在这里发布问题，分享观点，讨论相关主题。

欢迎阅读本书，希望读者阅读时能像我们编写时一样充满乐趣。我们坚信，读者在设计、部署和升级 IT 系统的安全时，将会采用本书讨论的理论、概念、技巧和方法，让这些系统以后免受所有安全风险和攻击的困扰。

Chris、Ramesh 和 Ray

www.coresecuritypatterns.com

# 致　谢

相比于我们的无知，我们的知识和学问简直不值一提。
柏拉图(公元前427—347年)

我们要感谢Prentice Hall出版社在本书出版过程中持之以恒的帮助和支持，其成员包括Greg Doench、Ralph Moore、Bonnie Granat和Lara Wysong。

我们还要感谢Judy Lin、Joe Uniejewski、Whitfield Diffie、Li Gong、John Crupi、Danny Malks、Deepak Alur、Radia Perlman、Glenn Brunette、Bill Hamilton和Shaheen Nasirudheen提供的反馈以及宝贵的意见和建议。

很多人对本书进行了详细审阅，并从专家的角度提出宝贵的意见；如果没有他们的帮助，本书将难以付梓。衷心感谢Seth Proctor、Anne Anderson、Tommy Szeto、Dwight Hare、Eve Maler、Sang Shin、Sameer Tyagi、Rafat Alvi、Tejash Shah、Robert Skoczylas、Matthew MacLeod、Bruce Chapman、Tom Duell、Annie Kuo、Reid Williams、Frank Hurley、Jason Miller、Aprameya Puduthonse、Michael Howard、Tao Huang和Sen Zhang。

我们要感谢Sun Microsystems、RSA Security、VeriSign、Microsoft、Oracle、Agilent Technologies、JPMorganChase、FortMoon Consulting、AC Technology、Advanced Biometric Controls和美国财政部Pay.Gov项目的朋友，感谢他们直接或间接的支持和鼓励。

## Chris Steel

这里要感谢众多给我的工作提供帮助的人员。首先，要感谢参与本书编写的人员：

- Frank Hurley独自撰写了第2章，并撰写了大量有关安全基础知识的材料和参考资料。如果没有他，我将遗漏很多有关安全的基础知识。
- Aprameya Paduthonse撰写了多种用于Web层和业务层的模式，还审阅了几章的内容，让我得以快速添加内容和填补空白。如果没有他，编写进度将更慢。
- Jason Miller撰写了大量有关Web层的内容并负责有关如何结合使用Web层模式的技术细节，他对Struts和Web层框架的认识无人能出其右。

我还要对众多审阅者致以最诚挚的谢意。正是由于他们抽出宝贵的时间审阅本书，才使我们没有偏离航向。

这里尤其要感谢Robert Skoczylas，他详细审阅了有关Web层和业务层模式的章节，并提出了大量的建议。正是由于他的工作才使这些内容更为连贯易懂。Robert是我遇到的最好的审阅人员。

## Ramesh Nagappan

从进入Sun Microsystems起，安全就是我喜爱的主题之一。虽然我从事的主要工作是Java分布式计算，但有大量的机会尝试安全技术。鉴于对著述的热情，编写有关安全的图书一直是我的夙愿，随着这部巨著的完成，这个夙愿终于得以实现。

回想本书的起源很有趣。那是Sun's JavaSmart Day——2002年9月16日在波士顿召开的开发人员会议，向众多听众发表有关Web服务安全的演讲后，Chris和我疲惫不堪而又饥肠辘辘地离开。我们在The

Cheesecake Factory 落座，在休息期间冒出了这样一个念头：为 Java 开发人员编写一本有关实用安全的书，将我们珍藏已久的密诀、技巧和方法拿出来让大家分享。在接下来的几天中，我们向 Prentice Hall 出版社的 Greg Doench 提供了建议，他欣然接受，但 Chris 和我由于时间安排紧迫而无法跟上进度。Greg 有一次问我："在 Red Sox 再次赢得世界职业棒球大赛前能够把手稿准备好吗？"由于 Chris 和我想在书中讨论更多相关主题，因此需要完成的工作范围比原计划大得多。经过几个月不断扩大范围后，Chris 和我决定邀请 Ray Lai 加入。我们的著述之旅就是这样开始的。在编写期间，我们召开了一次午夜电话会议，讨论并分享我们的想法以及解决问题，这很有趣。经过两年多的努力，工作竟然完成了，我对此确实有些吃惊。看着它远远超出了当初我们在 The Cheesecake Factory 的设想，那感觉真是棒极了。

首先，要感谢直接或间接影响我，让我有机会学习和获得安全技术使用经验的人。如果没有这些机会，我将无法获得编写本书所需的专业知识。感谢：

- Gary Lippert、Dave DiMillo、Li Gong 和 Chris Steel 给我提供使用 Java 安全技术和参与 J2EE 应用安全项目的经验；
- Sunil Mathew 和 William Olsen 推荐我参与实际的 Web 服务项目，并向我提供测试 Web 服务安全原型的机会。
- Doug Bunting 推荐我参与 Web 服务标准的制定，尤其是 OASIS WS-CAF 和 WS-Security 工作小组。
- Wayne Ashworth 和 Dan Fisher 向我提供进入 Smart Card 领域和开发 Smart Cards 应用原型的机会。
- Art Sands、Chris Sands、Tuomo Lampinen、Jeff Groves 和 Travis Hatmaker 向我提供熟悉生物特征技术和将其集成到 Sun 身份管理产品中的机会。
- Luc Wijns、Charles Andres、Sujeet Vasudevan 相信我的专业知识，给我提供为国内著名的 ID 项目建立基于 Java Card 的身份管理解决方案原型。

其次，我幸运地拥有一个优秀的审阅小组，他们的意见和建议深刻独到，极大地提高了本书的质量。

衷心感谢 Glenn Brunette、Shaheen Nasirudeen、Tommy Szeto、Sang Shin、Robert Skoczylas、Tejash Shah、Eve Maler、Rafat Alvi、Sameer Tyagi、Bruce Chapman、Tom Duell、Annie Kuo 和 Reid Williams 卓越的审阅意见，我已经将这些意见融合到各章节中。

这里要特别感谢 Patric Chang 和 Matthew MacLeod 在编写本书期间对我的鼓励和赏识。

最后，尤其需要感谢我亲爱的妻子 Joyce、儿子 Roger、小女儿 Kaitlyn 和父母，感谢他们给我的爱、灵感和持之以恒的支持。倘若没有他们的爱与支持，我将无法完成本书。

## Ray Lai

感谢我的家人，他们在我编写本书的每个夜晚和周末耐心地等待我。

另外，还要感谢以下人员的支持：

- Glen Reece 博士、Kumar Swaminathan 和 Samir Patel 在管理和精神方面的支持。
- Rafat Alvi、Glenn Brunette、Dwight Hare、Eve Maler 和 Seth Procter 严格和坦率的审阅，确保手稿在技术方面的正确性。
- Anne Anderson 对第 7 章的严格审阅和建议。

# 作者简介

Christopher Steel(CISSP、ISSAP)现任 FortMoon 咨询公司的总裁兼 CEO，目前是美国财政部 Pay.gov 项目的首席架构师。他拥有 15 年的分布式企业计算经验，主要研究应用安全、模式和方法。他的客户包括美国海军、Raytheon、Fleet、CVS Pharmacy、Nextel、Verizon、AOL、KPMG、MCI 和 GTE。他经常在本地和行业会议上发表有关安全的演讲。

Ramesh Nagappan 是 Sun Microsystems 的一名 Java 技术架构师。他拥有丰富的行业经验，擅长 Java 分布式计算和关键任务应用安全架构。编写本书之前，他参与合著了三本有关 J2EE、EAI 和 Web 服务的畅销书。他是开放源代码应用和行业标准动议的积极撰稿人，经常在有关 Java、XML 和安全的行业会议上发表演讲。目前，他研究的重点是 Web 服务安全、身份管理以及使用智能卡和生物特征的安全身份识别技术。

Ray Lai 是 Sun Microsystems 的一名高级工程师，目前在 Sun 的重点技术办公室(Chief Technology Office)工作。他在很多跨国公司的企业应用项目中担任过架构师和开发人员，包括汇丰银行、Visa、美国运通、UBS、大和证券、DHL 和国泰航空公司。他还编写了《J2EE Platform Web Services》，并经常在国际会议上发表演讲。他目前重点研究的技术包括应用安全、策略和服务供应。

# 目　录

## 第二部分 Java 安全架构与技术