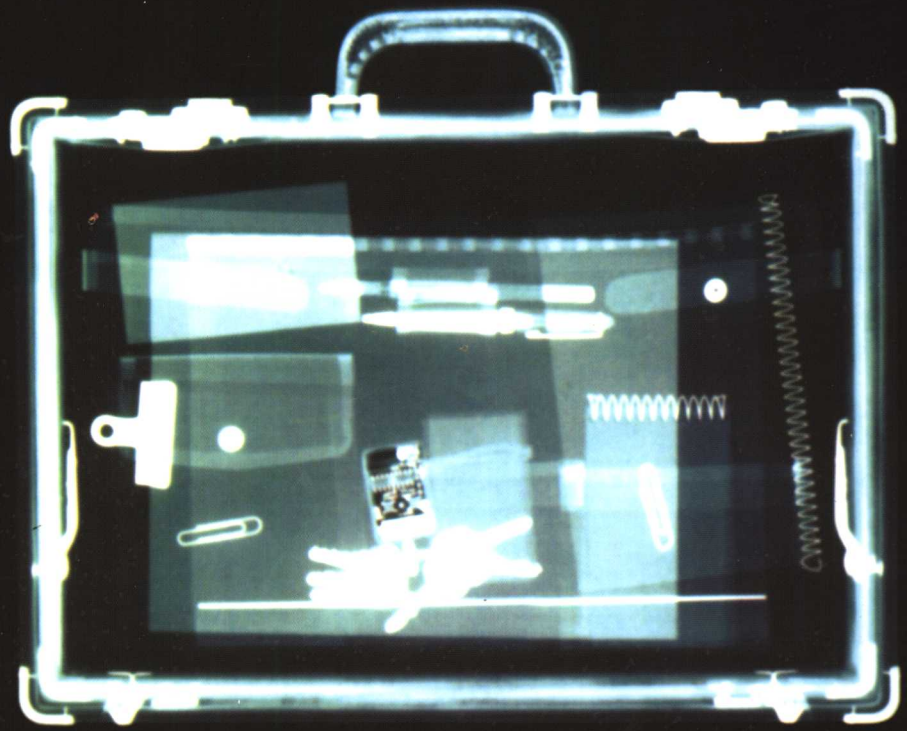
Enterprise Java Security

Building Secure J2EE Applications

PEARSON Addison Wesley

企业级 Java 安全性

——构建安全的 J2EE 应用



(美) Marco Pistoia 等著
Nataraj Nagaratnam
尹 亚 明喻卫 严进宝 译

Pearson Education

清华大学出版社

企业级Java安全性：构建安全的J2EE应用

(美) Marco Pistoia　Nataraj Nagaratnam　等著

尹　亚　明喻卫　严进宝　译

清华大学出版社

北　京

EISBN: 0-321-11889-8

北京市版权局著作权合同登记号　图字：01-2004-5002

图书在版编目(CIP)数据

企业级 Java 安全性：构建安全的 J2EE 应用/(美)彼斯特(Pistoia, M.)，(美)讷格日特纳姆(Nagaratnam,N.)等著；尹亚，明喻卫等译. —北京：清华大学出版社，2005.3

书名原文：Enterprise Java Security:Building Secure J2EE Applications

ISBN 7-302-09744-5

Ⅰ. 企… Ⅱ. ①彼… ②讷… ③尹… ④明… Ⅲ. JAVA 语言—程序设计—安全技术 Ⅳ. TP312

中国版本图书馆 CIP 数据核字(2004)第 105437 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：曹　康　　**文稿编辑**：于　平
封面设计：康　博　　**版式设计**：康　博
印 刷 者：北京通州大中印刷厂
装 订 者：三河市金元装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：27　**字数**：691 千字
版　　次：2005 年 3 月第 1 版　2005 年 3 月第 1 次印刷
书　　号：ISBN 7-302-09744-5/TP·6734
印　　数：1～3000
定　　价：58.00 元

序

电子商务作为信息技术产业中发展最快的部分之一，正在改变着商业活动的面貌。在 Web 上进行各种业务活动，正在飞速地成为企业之间、以及机构组织与它们的客户之间进行的业务活动中的基本元素。基于 Web 的系统并不是孤立的，相反，它们是许多现存的企业系统、过程和协议的整合，这个系统会被经常地重新设计和构建，以增强其固有的性能并在其中增加新的功能。系统的价值并不在于各个技术组成部分的细节，而是在于它针对新的业务解决方案的快速创建能力。

当然，所有的技术都会给业务引入风险，而挑战性就在于如何处理这些风险。其中有些风险来自于为满足公司的商业需求而设计的解决方案的复杂性；而另外一些则来自于所选择的技术的本身。为了应对这些风险，业界已经提出了许多安全技术，例如，病毒扫描仪、防火墙、入侵检测系统、虚拟专用网络(VPN)、公开密钥加密系统和安全套接字层(Secure Sockets Layer，SSL)协议。

在“风险”这个问题上，Web 也不能例外。虽然它提供了开拓销路和市场的新机遇，但是，它所引入的风险也已经迫使技术人员提出了许多相应的具有创造性的解决方案。其中包括了对系统用户的认证和授权、保护事务不受恶意用户破坏、加强的访问控制、隐私保护和提供联合身份管理。

一个企业系统通常包含了许多异构的子系统。因为大多数情况下，系统的发展并不需要推倒一切，从头构建一个全新的系统，而仅仅是让现有系统和服务可以通过 Web 访问，所以，使得这些企业系统中的子系统能够相互通信，并且可以被整合成为有用的端到端解决方案，这是非常必要的。在企业系统中，如果包括安全在内的关键元素可以基于开放标准，那么这个要求就很容易满足。开放标准的使用可以大大简化开发的成本和复杂性，但是，只有在供应商之间建立开放式的交流与合作渠道时，这才会成为可能。

众所周知，Java 2 平台下的 Enterprise Edition (J2EE)支持现有子系统整合到功能更强大的基于 Web 的企业系统中。而本书正是对基于 J2EE 的企业应用程序的开发进行了深入的讨论。本书的中心是对支持和加强了 J2EE 环境的安全标准集的研究，其中包括 SSL、Kerberos 认证和授权、私有密钥和公开密钥加密、公开密钥加密标准(PKCS)、安全/多用途 Internet 邮件扩充(Secure/Multipurpose Internet Mail Extension)和 Web 服务安全规范。本书不是一段一段孤立地讨论安全技术，而是在一个更广阔的范围内提出安全方面的观点。在行业领域，程序性安全正在向声明性安全转变，其目标就是通过策略而不是依靠在每个应用程序中散布着的安全代码来控制安全保障，显然，在发现新的威胁和风险后，后者的维护和升级的代价要高得多。

本书是 IBM 在安全、中间件和即时计算(on-demand computing)方面的技术和研究实力的结果，也是 IBM 的 Software Group 和 Research Division 团队长期协作的结晶。在此协作中汇集了该领域的世界各地的专家，他们以合作伙伴关系致力于在动态的业务和技术环境下为市场创造价值的工作。

长期以来，我们一直在呼唤 J2EE 安全方面的专业书籍的问世。我非常高兴地看到，现在有这样一本优秀的作品来解答开发人员、管理人员和研究人员在这个重要领域的技术问题。我相信，本书会对 J2EE 平台和电子商务的成功做出重要的贡献。

Steven A.Mills
副总裁和公司执行官
IBM 公司软件组

前　言

本书诠释了 J2EE 和 J2SE 安全技术在构建包含基于 Java 企业应用的安全企业基础结构中的适用性。本书结合实例，解释了为什么 Java 安全是电子商务环境中的关键因素，并介绍了应用程序开发人员应该如何使用这种技术来构建安全的企业级应用。

本书介绍了 J2EE 和 J2SE 安全体系结构，展示了这种体系结构是如何相互关联的，以及如何通过 Java 认证与授权服务（JAAS）增强以提供认证和授权机制。接着，书中深入研究了 J2EE 安全技术：servlet 的安全技术、JSP 和 EJB，因为这些技术共同构成了 J2EE 体系结构的核心。为了满足开发人员构建安全可靠的 J2EE 应用程序的需求，本书还包括了对 J2EE 和密码学技术之间联系的详细介绍。Java 加密体系结构(Java Cryptography Architecture，JCA)、Java 加密扩展(Java Cryptography Extension，JCE)、公开密钥密码学标准(Public-Key Cryptography Standard)、安全/多用途 Internet 邮件扩展(Secure/Multipurpose Internet Mail Extensions)和 Java 安全套接字扩展(Java Secure Socket Extension)在书中也有详细的描述。书中还介绍了如何在实际中使用 J2EE，并展示了前面提到的各种技术是如何协作和整合的。书中描述的情景是面向那些需要构建一个整合的、安全的和基于组件系统的 J2EE 开发人员和部署人员。然后，讨论了 Web Service 安全和其他新技术，并介绍了位于底层的中间件的工作方式。最后，本书概括了 J2EE 安全对当今电子商务环境的影响。

与其他关于 Java 安全的同类书籍不同，本书在讨论 J2SE 和 J2EE 安全体系结构的同时，提供了实用的解决方案，并在把这些体系结构完善成为企业电子商务解决方案的过程中，使用模式来解决遇到的问题。这样做的目的，就是向那些涉及到需要使基于 Java 的应用程序或 Web 站点满足工业级强度的商业要求，给出实用的指导。书中提供了许多示例，这给用户提供了清晰理解底层技术的途径。

J2EE 安全为了实现可移植性和可重用性，其设计主要采用了声明性方法。在 J2EE 平台上的绝大多数的认证、授权、整合、机密性和访问控制决策等行为，都是可以使用配置文件和部署描述符来完成的。而由于这些配置文件和部署描述符是置于应用程序之外的，这就减轻了程序员的负担，并且使得 Java 企业级程序具有可移植性、可重用性和灵活性。因此，本书的第Ⅰ部分和第Ⅱ部分重点介绍了 Java 安全的声明性方法，并通过配置文件和部署描述符的示例进行说明。另外，这些部分也说明了如何在不能单独使用声明性安全的情况下使用程序式的方法(示例程序可以在第 4 章和第 5 章中找到)。本书的样例程序大多数集中在第Ⅲ和第Ⅳ部分。

本书引用了本书作者为 *IBM Systems Journal* 和 *IBM developer Works* 撰写的一些文章。在这些文章中，描述了 Java 安全的起源和使用 J2EE 编程模型的企业级应用的安全性。虽然本书的作者在地域上分布于美国的各地，但是，他们曾于 2000 年 3 月聚集在加州的 Santa Clara,在 O'Reilly Java 会议上就一系列安全主题进行了探讨。他们发现，许多开发人员和管理人员并不熟悉 Java 安全特性、J2EE 安全和在 J2EE 环境下管理安全的措施。通过邮件，他们源源不断地接收到人们关于 Java 和 J2EE 安全方面的询问。他们已经完成了一本关于 J2SE 安全的书籍，但是看来仍然需要一本专门讨论包括那些基于服务器的应用和 Web Service 在内的关于企业级

应用安全的书籍。

本书参考了多方面的资料，包括前面提及的 J2SE 安全的书籍和文章。本书覆盖了 J2SE 1.4 版和 J2EE 1.4 版。本书中相应的 J2EE 规范包括了 J2EE 1.4 版、Java Servlet 2.4 版、EJB 2.1 版的规范和 Web Service 的规范。

作 者 简 介

本书的作者是几名 IBM 安全问题研究人员和架构设计师，他们的主要研究方向是 Java 安全体系结构的定义和相关技术。这个项目的领导人是 Marco Pistoia。

Marco Pistoia 是 Java 和 Web 服务安全部门的研究人员之一。这个部门是 IBM 在纽约 Yorktown Heights 的 IBM Thomas J.Watson 研究中心的网络安全、隐私和密码学研究部门的一部分。Marco 撰写过十本书籍，并发表过许多论文和期刊文章，其内容涉及 Java 和电子商务安全问题的各个领域。他撰著的一本书，*Java 2 Network Security, Second Edition* 在 1999 年由 Prentice 出版社出版。他曾经出席过许多全球级别的会议，例如 Sun Microsystems 的 JavaOne 会议等。他曾被邀请为研究生讲授 Java 安全问题方面的课程，并曾出席纽约 Brooklyn 的 Center for Advanced Technology in Telecommunications(CATT)。Marco 于 1995 年在意大利的罗马大学获得了数学硕士学位，现在正在纽约州 Brooklyn 的 Polytechnic 大学攻读博士学位。他的技术兴趣主要集中在可移动代码的安全问题、组件软件和面向对象语言的静态分析。

Nataraj Nagaratnam 是位于北卡罗莱纳州 Raleigh 的 IBM WebSphere software family 高级技术成员之一和首席安全架构师。他领导了 IBM WebSphere 安全体系结构和 IBM Grid 基础结构的研究。他还是 IBM Web Service 安全体系结构研究组的核心成员。他曾经与他人合著了 Web Service 安全规范和 Open Grid Services Architecture(OGSA)文档。他积极地参与研究 Java Community Process 中与 J2EE 安全问题相关的主题部分，也承担了 Java Specification Request 中关于 J2EE 安全问题的部分领导工作。Nataraj 在纽约的 Syracuse 大学获得了计算机工学博士学位。他的学术论文是关于分布式对象环境中的安全委托问题。他广泛地参与了各种关于 Java 和安全问题的会议，并且在许多的期刊、会议和杂志上发表了大量的文章。Nataraj 是 Waite Group Press 在 1996 年最早的出版的 *Java Networking and AWT API SuperBible* 的领衔作者之一，此书是关于 Java 网络的最早的书籍之一。

Larry Koved 是 Java 和 Web 服务安全部门的经理和研究人员之一，这个部门是 IBM 在纽约 Yorktown Heights 的 IBM Thomas J.Watson 研究中心的网络安全、隐私和密码学研究部门的一部分。他曾经是 IBM 的 Java 安全架构师，并曾在关于 Java 安全设计和开发合作的事宜中负责与 Sun Microsystems 联络沟通。他积极地参与了 JAAS 及其后的 EJB 1.1 版本的安全体系结构的设计。Larry 在关于用户界面技术、虚拟现实、超文本和移动计算、Java 代码的静态分析以及安全方面发表了 25 篇以上的文章和技术报告。他目前的研究兴趣包括可移动代码的安全性、组件软件和 OO 语言的静态分析。

Anthony Nadalin 是 IBM 在德克萨斯州 Austin 的 Java 和 Web Service 的首席安全架构师。作为一名资深技术成员，他负责横贯 IBM、Tivoli 和 Lotus 的安全基础结构的设计和开发。他在与 Sun Microsystems 关于 Java 安全设计和开发合作，以及与 Microsoft 关于 Web Service 安全设计和开发的合作中担任首席安全联络员。他在 20 年 IBM 的职业生涯中，曾历任以下职位：VM/SP 首席安全架构师、AS/400 安全架构师和 OS/2 安全架构师。他曾经独立以及与他人合作撰写了 30 多篇技术性期刊和会议文章，iUniverse.com 在 2000 年出版了他的 *Java and Internet*

Security 一书。他曾在三个主要的学术期刊和一个会议担任技术委员会成员，并且广泛地审阅了由当今本领域的技术先驱们发表的文章。他曾经出席过许多技术性安全问题会议并多次被邀请发言。

目　录

第Ⅰ部分　企业安全与 Java

第 II 部分 Enterprise Java 组件安全

第III部分 Java 2 安全基础

第Ⅳ部分 企业级 Java 与密码学

第Ⅴ部分 高级专题