

- 覆盖 Java 2 应用程序、小程序、JCA、JCE、SSL、JSSE、JAAS、网络、数据库、CORBA、EJB、servlet 及 JSP 安全性
- 构建安全的 Java 服务器
- 学习网络、数据库和 Web 编程的安全技术
- 开发可扩展的企业安全解决方案

Java Security Handbook



Java

安全手册

[美] Jamie Jaworski 等著
邱仲潘 等译



SAMS



电子工业出版社
Publishing House of Electronics Industry
URL: <http://www.phei.com.cn>

Java 安全手册

Java Security Handbook

[美] Jamie Jaworski 等著

邱仲潘 等译

電子工業出版社

Publishing House of Electronics Industry

北京 · Beijing

内 容 简 介

本书是一本全面介绍 Java 安全性的工具书, 共分为四个部分。第一部分介绍了 Java 安全的基本概念, 包括如何建立安全应用程序的基本模型、如何建立 Java 小程序和应用程序, 还概述了 Java 安全策略和 Java 应用程序中常见的安全问题。第二部分介绍了 Java 2 API JCE 和 JSSE 的加密功能及 Sun 之外的供应商提供的加密软件包。第三部分介绍了分布式系统的安全性, 包括与网络安全、数据库、JAAS、CORBA、EJB、JSP 和 Java 小程序相关的安全问题。可满足企业开发人员的特定需求。最后一部分为附录, 包括基本算法和安装 JEC 等内容。

Authorized translation from the English language edition published by Sams Publishing, Copyright © 2000. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the publisher. Simplified Chinese language edition published by Publishing House of Electronics Industry, Copyright © 2001.

本书中文简体版专有翻译出版权由 Pearson 教育集团所属的 Sams Publishing 授予电子工业出版社。其原文版权及中文翻译出版权受法律保护。未经许可, 不得以任何形式或手段复制或抄袭本书内容。

图书在版编目 (CIP) 数据

Java 安全手册 / (美) 贾沃斯基 (Jaworski, J.) 等著; 邱仲潘等译. - 北京: 电子工业出版社, 2001.8
书名原文: Java Security Handbook
ISBN 7-5053-6938-5

I. J… II. ①贾… ②邱… III. JAVA 语言 - 安全技术 - 手册 IV. TP312-62

中国版本图书馆 CIP 数据核字 (2001) 第 055749 号

书 名: Java 安全手册
原 书 名: Java Security Handbook
著 者: [美] Jamie Jaworski 等
译 者: 邱仲潘 等
责任编辑: 赵宏英
排版制作: 今日电子公司制作部
印 刷 者: 北京东光印刷厂
装 订 者: 三河司庄装订厂
出版发行: 电子工业出版社 URL: <http://www.phei.com.cn>
北京市海淀区万寿路 173 信箱 邮编: 100036
经 销: 各地新华书店
开 本: 787 × 1092 1/16 印张: 24.25 字数: 605 千字
版 次: 2001 年 8 月第 1 版 2001 年 8 月第 1 次印刷
书 号: ISBN 7-5053-6938-5
TP · 3954
定 价: 38.00 元
版权贸易合同登记号 图字: 01-2000-4355

凡购买电子工业出版社的图书, 如有缺页、倒页、脱页、所附磁盘或光盘有问题者, 请向购买书店调换。若书店售缺, 请与本社发行部联系。电话: 88211980 68279077

关于作者

Jamie Jaworski 是 JSPWare.com 公司总裁，为 100 强公司建立安全的基于 Java 的 Web 应用程序。他也是专业 Java 开发人员、Sun 认证的编程人员、开发人员和结构设计师。Jamie Jaworski 编写了 Java 与 JavaScript 方面的多本畅销书，包括《Java 2 Platform Unleashed》和《Mastering JavaScript and JScript》。他还负责为 CNET 的著名 Web 开发人员站点 Builder.com 编写 SuperScripter 栏目。

Paul J. Perrone 是 Assured Technologies 公司的创始人、总裁和高级软件顾问。Paul 通过 Assured Technologies (<http://www.assuredtech.com>) 对公司提供软件咨询、培训、产品和研究，帮助其实现高度安全、高度智能、经济实用、可伸缩、支持 Internet 的分布式企业系统，用于电子商务、公司对公司 (B2B) 事务和一般企业级应用程序。Paul 在 Assured Technologies 公司的业务实践中建立了高智能、高可靠性的 (例如安全性) 系统，具有这方面的丰富知识。Paul 是许多 500 强和中型公司大型 n 层分布式系统与产品的主要构造、设计和开发者。Paul 主攻的技术和培训领域包括企业 Java 和 J2EE、EJB、嵌入式企业系统连接、CORBA、XML、UML 和面向对象与基于组件的软件。除了本书之外，Paul 还编写了《Building Java Enterprise Systems with J2EE》，在 JavaOne 会议上发言，并在多种行业杂志中发表作品。Paul 从弗吉尼亚大学取得电子工程硕士学位，从鲁格大学取得电子工程学士学位，是 IEEE 和 ACM 会员，在北弗吉尼亚技术社区中非常活跃。可以通过 pperrone@assuredtech.com 或 (703) 728-0115 与 Paul 联系。

Venkata S.R. Krishna Chaganti 开发了本书第 3 章、第 9 章和第 13 章的许多代码。Krishna 是高级软件工程顾问，过去七年一直用 Java 和 C++ 编程环境开发分布式计算软件。Krishna 为 500 强公司开发分布式计算所需的 EJB、CORBA 与 DCE 软件。Krishna 还有过两年的 Java 与相关技术的教学经验。他是阿拉巴马大学汉特维尔分校电子工程硕士和计算机工程硕士，并在印度纳加京纳大学取得电子与通信工程学士学位，可以通过 chaganti@erols.com 访问。

献 辞

谨献给 Fred Neal、Ralph Seay 和 HQ USAFE INSA 的所有朋友们，感谢你们的帮助。

Jamie Jaworski

献给我的妻子和双亲。

Paul Perrone

致 谢

感谢每一位帮助本书完成的人，特别要感谢 Waterside Productions 公司的 Margot Maley

Hutchison 使本书的出版成为可能，感谢 Paul Perrone 接受并推出了这本书，感谢 Steve Anglin、Dawn Pearson、Tiffany Taylor、Mary Lagu 和整个 Machmillan 工作组的大量宝贵建议，感谢 Tim Ryan 带我入门，感谢 Krishna Sankar 的大量技术建议使本书质量大大提高。最后，感谢 Lisa、Emily 与 Jason 的耐心、爱心与理解。

—— Jamie Jaworski

家庭式和朋友式的文化塑造了我们，帮助我们解决问题。感谢我的大家族在我开发软件和写书过程中对我一如既往的支持。感谢妻子 Janie Perrone 的爱、理解与支持。当然，特别感谢我的双亲 Don 与 Judy Perrone，我的兄弟和亲属 Don、Denise、Allison 和 Julia Perrone、Catherine Stiles、Vances 一家、Heilmanns 一家、Izzos 一家、Lawlesses 一家。我们的家族很大。还要感谢 Anthony Perrone 与 Louis Perrone 给我的生活带来的一切。

除了亲人外，我的朋友和同事也帮助我形成了良好的判断力和洞察力，感谢 Anup Ghosh、Andy Stauffer、Jim Wamsley、Paul Kirkitelos、Jeff Ebert、Charles Choi、Doug Szajda、Geoff Hoekstra、Rick Hatch、Steve Wynne、Mike Carr、Catherine Longo 和 Ben Cappy。最后感谢 Krishna Chaganti 帮助开发了第 7 章、第 9 章、第 13 章的许多代码示例。

—— Paul Perrone

欢迎来信

作为本书的读者，你是我们的主要批评者和建议者。我们很重视你的意见，希望知道你的满意度，我们有哪些需要改进之处，以及你对我们的任何有益的见解。

作为 Sams 出版商，欢迎你提出宝贵意见，可以通过传真、E-mail 或信件与我们联系，告诉我们如何把图书做得更好。

注意，我无法帮你解决与本书的主题相关的技术问题，由于来信太多，也很难一一答复。

写信时请包括书名、作者名和你的姓名、电话或传真。我将认真分析你的建议，并转给作者和编辑。

传真： 317-581-4770

E-mail: java@mcp.com

邮件： Michael Stephens

Sams Publishing

201 West 103rd Street

Indianapolis, IN 46290 USA

前 言

对许多编程人员而言, Java 是开发 Web 应用程序和企业服务的首选语言。Java 的吸引力源自其支持小程序和 Java Development Kit (JDK) 1.0 提供的大量 API。Netscape 公司的 LiveConnect 扩展了这种吸引力, 可以用 JavaScript、JDK 1.1 中的语言改进和 API 1.1 增加的各种特性对小程序编写脚本。这些改进包括 JavaBeans (提供开发 GUI 与非 GUI 组件的机制)、Java 远程方法调用 (RMI, 提供分布式对象通信的基础) 和 JDBC (在 Java 小程序与应用程序中增加数据库连接)。

JDK 1.2 进一步增加了 Java 的功能和吸引力, 改进了 JDK 1.1 特性并增加了新特性, 如 Swing, Java 2D、Drag and Drop、Collections 和 CORBA 支持。JDK 1.2 更名为 Java 2 Platform。开发企业应用程序的软件平台 Java 2 Platform, Enterprise Edition (J2EE) 增加了对 servlet、Java Server Pages (JSP)、Enterprise JavaBeans、命名与目录服务、事务处理、邮件和其他特性的支持。J2EE 提供的特性使 Java 2 Platform 成为开发 Web 应用程序和分布式企业服务的首选平台。

尽管 Java 2 API 本身提供的大量功能足以使 Java 成为首选语言, 但 Java 还是开发安全应用程序的优秀语言和运行环境。自从 Java 的开发之初, 安全便成为设计 Java 编程语言、运行系统、API 与工具集的主要考虑。JDK 1.0 引入了 “sandbox” (沙袋) 方法, 用于保护移动代码。这是其作为 Web 编程语言最初取得成功的主要因素。JDK 1.1 增加了对签名小程序的支持, 可在信任沙袋之外而不会破坏小程序安全性。JDK 1.1 还增加了使用消息摘要、数字签名和数字证书的功能。

Java 2 Platform 的 Security API 对 JDK 1.1 API 进行了一些修改, 增加了可配置应用程序和小程序安全策略、X.509 版本 3 数字证书以及证书处理支持。Java 2 Security API 还提供了新工具, 可以指定安全策略、代码签名和管理证书。

Java 2 Platform 的安全功能中还增加了几个面向安全的扩展:

- Java Cryptography Extension (JCE) 1.2 提供了开发加密、密钥产生、密钥协议与验证算法的基础, 并提供了几种常用加密算法的实现方法。
- Java Secure Socket Extension (JSSE) 提供 Secure Sockets Layer (SSL) 版本 3 与 Transport Layer Security (TLS) 版本 1 协议的 Java 实现。这些协议可以在现有 Internet 协议 (如 HTTP, telnet 与 POP3) 中增加安全性。
- Java Authentication and Authorization Service (JAAS) 支持用户验证与访问控制。提供了 Pluggable Authentication Module (PAM) 的 Java 版本和控制哪些用户能运行安全敏感软件的种类和接口。

Java 2 Security API、JCE 1.2、JSSE 与 JAAS 一起提供了开发安全的基于 Web 的分布式应用程序的综合框架。再加上 J2EE API 的功能和灵活性, 就可以对 Web 和企业 Intranet 开发高级应用程序了。

Java 安全的重要性

对许多公众与商业性公司, Internet 已成为进行商务工作的主要渠道, Internet 是广告、促

销、销售和客户支持的主要媒介，可帮助新公司以指数级增长，帮助大公司扩大市场占有率。相反，不及时利用 Internet 的公司则可能蒙受损失。

Internet 提供了巨大的机会，但也带来了不小的风险。Web 服务器可能被攻破，Web 页面可能被涂改，专用客户数据可能被公开披露，财务事务可能被伪装，企业防火墙可能被攻破，企业网可能被盗用。公司利用 Internet 的功能很重要，而保证安全则更加重要。

作为 Web 编程语言，Java 是开发安全 Web 应用程序的核心。Java 小程序可以将可执行程序的内容传递到 Web 浏览器中，JSP 和 servlet 可以安全地处理浏览器请求，JDBC 提供了让 Web 应用程序安全访问企业数据库的功能，EJB 提供了安全地部署应用程序业务逻辑的框架，Java RMI 与 CORBA 提供了部署分布式对象的基础，Java Security API 及其安全相关扩展使完全分布式 Web 应用程序可以安全地实现和执行。如果要开发安全 Web 应用程序，则 Java 非常合适。

尽管我想说 Java 在安全方面大大超过竞争对手，但这不妥当，因为它没有对手。Microsoft 公司的 Authenticode 方法可以加密移动代码，但要求以 Web 开发人员编写善意的代码作为安全的基础，验证代码无法阻止人们开发破坏性代码，只是要求代码正确地签名，就像在邮件炸弹中要求回信地址一样。

Java 安全性在客户端编程中至关重要，而在服务器方编程中则更加重要。Java servlet 和 JSP 是惟一自我限制的服务器方编程技术。如果 ColdFusion 脚本中有严重的安全缺陷，则优秀的黑客可以利用它攻破服务器。servlet 和 Java 服务器页面可以配置成实现最低权限，即用户只有完成工作所需的权限，而没有更多权限。如果安全地配置包含安全缺陷的 servlet，则黑客攻破服务器时，只能得到 servlet 的权限，而没有更多权限。

包含破坏的功能比防止破坏的功能更加重要。Java 编程语言的安全设计、它的面向对象性能和 Java 运行系统的安全特性，使软件开发人员可以开发简单、可靠而不易出现安全错误的软件。

Java 的安全功能从客户机和 Web 服务器扩展到数据库、应用程序逻辑和基于 Web 的应用程序使用的企业对象。JDBC 与 JSSE 提供了客户机和 Web 服务器安全连接后台数据库的功能，EJB 提供了安全地部署应用程序业务逻辑的框架，Java RMI 与 CORBA 提供了部署分布式对象的基础，可以和 JSSE 一起支持分布式对象之间的安全通信。

Java 的大量 API 和集成安全特性使它成为实现外联网与内联网安全的关键技术。尽管可以用非 Java 技术保护关键 Web 应用程序，但通常会得到更昂贵、更难移植和更难扩展的解决方案。比较在客户端使用 ActiveX、Perl CGI 脚本、Oracle 数据库驱动器和专属应用程序服务器的应用程序，与基于小程序、JSP、JDBC 和 EJB 的 Web 应用程序，哪个更安全、更方便、更廉价、更易移植和维护呢？

大多数 Web 应用程序中要达到高度安全性很不容易，否则就不会每周都看到网站被攻破的新闻了。良好的安全性要求认真的规划、良好的结构、合理的设计和几乎无缺陷的实施方法，还要求使用面向安全性的开发与执行环境。Java 2 Platform 提供了开发工具与执行环境。本书介绍如何用 Java 2 Platform 开发具有良好的结构、合理的设计并集成安全特性的优秀应用程序。

本书的读者

本书适合任何要设计和建立安全 Java 小程序或应用程序的读者。如果你是中高级 Java 编程

人员，需要保护 Java 程序，则可以阅读这本书。本书能填补在 Java 运行系统与 Security API 方面的空白，并介绍 JCE 1.2、JSSE 与 JAAS，把这些知识放进实践中，利用这些 API 的安全策略、代码签名、加密、验证、授权和访问控制特性编写 Java 应用程序。

我们介绍如何用 Java 安全特性开发签名小程序、安全 servlet、安全地连接企业数据库；介绍如何在现有 Java 应用程序中增加 SSL，对用户进行强验证，并执行个人和小组的访问控制；还将介绍如何在电子商务应用程序中增加安全性，利用 RMI 与 CORBA 安全访问分布式对象，以及利用企业 JavaBeans 提供的安全特性。

除了提供开发安全 Java 应用程序所需的知识和练习外，本书还帮助用户建立安全专家的思维习惯。通过全面了解 Java 安全特性的思路，可以学习如何充分利用这些特性，避免危险陷阱，建立相当安全的 Java 应用程序。

本书的组织

本书分为四个部分共 15 章，7 个附录提供与书中内容有关的其他细节和支持信息。

第一部分“Java 安全基础”介绍 Java 安全的基本概念，包括下面 4 章：

- 第 1 章——安全性基础：介绍安全的基本概念，描述建立安全应用程序的基本模型。
- 第 2 章——Java 安全概述：提供 Java 安全特性概述及这些特性如何建立安全 Java 小程序或应用程序。
- 第 3 章——Java 应用程序安全访问控制：描述 Java 2 平台的基于策略的访问控制机制如何在 Java 应用程序中应用。
- 第 4 章——小程序安全性：介绍默认小程序安全策略和用签名小程序代码扩展这个策略。

第二部分“加密安全”介绍 Java 2 API Java Cryptography Extension (JCE) 1.2 和 Java Secure Socket Extension (JSSE) 的加密功能，还介绍 Sun 之外的提供商提供的加密软件包。第二部分包括下面几章：

- 第 5 章——加密简介：提供加密基本概念的简介，并介绍 Java 2/JCE 1.2 如何支持加密。
- 第 6 章——密钥管理与数字证书：介绍密钥管理概念和 Java 2 的密钥管理支持。
- 第 7 章——消息摘要与数字签名：介绍如何与消息摘要、数字证书与数字签名一起使用 Java 2 的特性。
- 第 8 章——Java 加密扩展：提供 JCE 1.2 概述，介绍其提供的功能及如何使用 JCE 与其他安全提供者。
- 第 9 章——SSL 与 JSSE：介绍 SSL 与 JSSE 并举例说明如何用其保护客户 - 服务器通信。

第三部分“分布式系统安全”介绍分布式系统的安全性，包括与网络安全、数据库、Java Authentication and Authorization Service (JAAS)、CORBA、EJB、Java Server Pages (JSP) 和 Java 小程序相关的安全问题，包括下列章节：

- 第 10 章——分布式企业安全概述：概述基本分布式 Java 企业 API 和利用这些 API 进行加密的方法。
- 第 11 章——数据库与数据库安全：介绍数据库安全问题和利用 JDBC 实现数据库安全的

方法。

- 第 12 章——Java 验证与授权服务：介绍 Java 验证与授权服务（JAAS）及其如何在 Java 应用程序中使用。
- 第 13 章——CORBA 安全性：介绍如何开发安全的 Java CORBA 应用程序，使用标准 CORBA Security 服务。
- 第 14 章——企业 JavaBeans 安全：介绍与企业 JavaBeans 安全（EJB）相关的安全问题和如何开发安全的 EJB。
- 第 15 章——JSP 与 Java servlet 安全：介绍与 Common Gateway Interface（CGI）相关的安全问题，并提供加密用 servlet 与 Java Server Pages 开发的 Web 应用程序的方法。

附录包括基本算法和安装 JCE 的信息等内容，包括：

- 附录 A —— Java 安全缺陷：汇总了所有已公布的 Java 安全缺陷。
- 附录 B —— RSA 算法：提供 RSA 加密系统的算法基础。
- 附录 C ——下载与安装 JCE：提供下载与安装 JCE 的步骤。
- 附录 D —— Java 2 Security API：汇总 Java 2 Security API 的类与接口。
- 附录 E ——下载与安装 Cryptix JCE 1.2：提供下载与安装 Cryptix JCE 1.2 的步骤。
- 附录 F ——使用 keytool：介绍如何使用 Java keytool。
- 附录 G ——使用 jarsigner 工具：介绍如何使用 jarsigner 工具。

除了本书的章节和附录外，本书所附 Web 站点 <http://www.courseone.com/support/books/java/security> 提供了更新、纠正和与 Java 安全有关的及时信息。其他针对 Java 分布式企业安全问题和方案的信息资源可以从 <http://www.assuredtech.com/books/jsh> 访问。

开始

要使用这本书，就要有一台计算机和支持 Java 2 Platform 的操作系统。支持 Java 2 Platform 的操作系统很多，包括 Windows 2000、NT、98 与 95，Linux 和 Solaris。Java 2 Platform 正在移植到许多其他操作系统。本书的例子是在 Windows 98、Windows NT 与 Linux 中开发的，但是它们都是纯粹的 Java，能在任何 Java 2 Platform 版本中运行。代码清单的更新见本书的 Web 站点。

如何使用本书

本书详尽介绍了 Java 安全性，可以直接翻阅感兴趣的章节。但建议从第一部分“Java 安全基础”开始，了解 Java 安全基础，Java 运行系统的操作，Java 安全策略和 Java 应用程序中常见的安全问题。这样就可以建立理解 Java API 安全机制的坚实基础。

阅读第一部分之后，建议阅读第二部分“加密安全”，特别是第 5 章“加密简介”。许多高级 Java 安全特性都需要理解加密、消息摘要、数字证书与数字签名。此外，附录提供了与第二部分的概念和工具有关的大量背景知识。

阅读第二部分之后，就能更好地理解第三部分“分布式系统安全”。本书介绍的许多分布式企业系统使用的高级安全选择特性都放在第三部分讲述，可以满足企业开发人员的特定 Java 企业开发需求。

目 录

第一部分 Java 安全基础

第 1 章 安全性基础	2
1.1 基本安全模型	2
1.2 加密	3
1.2.1 加密类	3
1.2.2 消息摘要	5
1.2.3 对称密钥	5
1.2.4 非对称密钥	5
1.3 验证与非否认	6
1.3.1 验证类型	6
1.3.2 非否认	8
1.4 访问控制	8
1.4.1 自由选择访问控制	9
1.4.2 基于角色的访问控制	9
1.4.3 强制访问控制	9
1.4.4 防火墙访问控制	9
1.5 域	9
1.6 审计	10
1.7 策略与管理	10
1.8 小结	11
第 2 章 Java 安全概述	12
2.1 Java 安全历史	12
2.2 Java 安全体系结构	14
2.2.1 Java 2 安全体系结构的核心	14
2.2.2 Java 加密体系结构	15
2.2.3 Java 加密扩展	15
2.2.4 Java 安全套接扩展	16
2.2.5 Java 验证与授权服务	16
2.3 字节码验证器	16
2.4 类装入器	17
2.4.1 类装入器体系结构与安全性	17
2.4.2 类装入器接口	18

2.5 安全管理器	21
2.5.1 安全管理器接口	21
2.5.2 定制安全管理器	22
2.6 Java 加密体系结构	24
2.6.1 JCA 体系结构	24
2.6.2 加密引擎	25
2.6.3 加密服务提供者	27
2.7 小结	28
第3章 Java 应用程序安全访问控制	29
3.1 权限	29
3.1.1 权限体系结构	29
3.1.2 权限类型	30
3.1.3 定制权限类型	34
3.2 安全策略	35
3.2.1 安全策略文件格式	35
3.2.2 在策略文件中引用属性	36
3.2.3 使用安全策略文件	36
3.2.4 安全策略工具	37
3.2.5 安全策略 API	38
3.3 Java 访问控制	38
3.3.1 访问控制体系结构	39
3.3.2 保护对象	41
3.3.3 SecurityManager 访问控制映射	42
3.3.4 微调与可配置访问控制举例	45
3.4 小结	47
第4章 小程序安全性	48
4.1 扩展沙袋	48
4.1.1 JDK1.0 沙袋	48
4.1.2 JDK 1.1 沙袋	50
4.1.3 JDK 1.2 最低权限	51
4.2 指定小程序安全策略	51
4.2.1 安全策略文件内容	52
4.2.2 提供项目语法	52
4.3 使用签名小程序	53
4.3.1 生成 JAR 文件	53
4.3.2 签名 JAR 文件	54
4.3.3 指定签名小程序策略	54
4.4 取得签名证书	55
4.5 使用不同的浏览器	55

4.6 小结	55
--------------	----

第二部分 加密安全

第 5 章 加密简介	58
5.1 密写简史	58
5.2 加密技术与密码分析	60
5.3 密码	60
5.3.1 凯撒密码	60
5.3.2 简单替换密码	65
5.4 秘密密钥加密	77
5.4.1 数据加密标准	77
5.4.2 DESede	90
5.4.3 Blowfish	90
5.4.4 Rivest 密码	94
5.5 公开密钥加密法	94
5.5.1 Rivest、Shamir、Adleman(RSA)算法	95
5.5.2 ElGamal 算法	97
5.6 消息摘要	98
5.6.1 MD5	99
5.6.2 SHA-1	101
5.6.3 Base 64 编码	102
5.7 数字签名	110
5.7.1 数字签名算法	111
5.8 数字证书	111
5.9 小结	113
第 6 章 密钥管理与数字证书	114
6.1 密钥管理的重要性	114
6.2 密钥表示	115
6.3 密钥产生	116
6.3.1 KeyPairGenerator 类	116
6.3.2 KeyGenerator 类	117
6.3.3 KeyGeneratorApp 程序	118
6.3.4 安全随机数与密钥生成	121
6.3.5 密钥转换	123
6.4 密钥协商	125
6.4.1 Internet 简单密钥管理协议	127
6.4.2 密钥协商的 JCE 支持	127
6.5 密钥存储与基于口令加密	132

6.6	JDK 1.1 与 JDK 1.2 密钥管理的差别	141
6.6.1	JDK 1.1 密钥管理	141
6.6.2	JDK 1.2 密钥管理	142
6.7	keytool	145
6.8	小结	146
第 7 章	消息摘要与数字签名	147
7.1	消息摘要类与接口	147
7.1.1	MessageDigestSpi	147
7.1.2	MessageDigest	148
7.1.3	DigestInputStream 与 DigestOutputStream	150
7.1.4	使用摘要流	152
7.1.5	DigestException	153
7.2	消息验证代码	153
7.2.1	MacSpi	154
7.2.2	Mac	155
7.2.3	MAC 操作	156
7.3	签名类与接口	157
7.3.1	SignatureSpi	157
7.3.2	Signature	157
7.3.3	SignedObject	161
7.3.4	Signer	163
7.3.5	SignatureException	163
7.4	小结	164
第 8 章	Java 加密扩展	165
8.1	JCE 内幕	165
8.2	Cryptix JCE	166
8.3	安全提供者与算法独立性	167
8.4	如何组织安全提供者	167
8.4.1	引擎类	167
8.4.2	SPI 类	168
8.4.3	提供者类	168
8.5	生成新提供者	168
8.5.1	扩展 SPI 类	169
8.5.2	扩展 Provider 类	171
8.5.3	安装 Provider 类	172
8.6	使用提供者	172
8.7	小结	174

第 9 章 SSL 与 JSSE	175
9.1 SSL 概述	175
9.2 Java 安全套接扩展概述	176
9.2.1 JSSE 包与类概述	177
9.3 JSSE 提供者	178
9.4 JSSE SSL 服务器套接	179
9.4.1 取得 SSL 服务器套接工厂	179
9.4.2 生成 SSL 服务器套接	182
9.4.3 SSL 服务器套接听取	183
9.4.4 客户机验证	184
9.5 JSSE SSL 客户机套接	185
9.5.1 取得 SSL 套接工厂	185
9.5.2 生成 SSL 客户机套接	185
9.6 JSSE SSL 对话	186
9.7 小结	187

第三部分 分布式系统安全

第 10 章 分布式企业安全概述	190
10.1 分布式企业系统技术	190
10.1.1 企业数据库连接	191
10.1.2 企业通信	191
10.1.3 企业通信服务	192
10.1.4 基于容器的企业组件	192
10.2 企业数据库连接安全性	193
10.3 企业通信安全	193
10.3.1 基本网络安全	194
10.3.2 RMI 安全性	195
10.3.3 CORBA 安全性	196
10.4 企业通信服务安全	196
10.4.1 JNDI 安全	196
10.4.2 Jini 安全性	197
10.4.3 JMS 安全性	198
10.4.4 JavaMail 安全性	199
10.5 基于容器的企业组件安全性	199
10.5.1 Web 组件安全	199
10.5.2 EJB 安全性	200
10.6 小结	200
第 11 章 数据库与数据库安全	201
11.1 何谓数据库	201

11.2	关系型数据库	201
11.2.1	使用关键字	202
11.3	结构化查询语言	202
11.4	远程数据库访问	202
11.4.1	CDBC 与 JDBC 驱动器	203
11.5	用 java.sql 包连接数据库	205
11.5.1	建立数据库连接	205
11.5.2	执行 SQL 语句	206
11.5.3	StatementApp 程序	207
11.6	数据库安全问题	211
11.6.1	保护数据库连接	212
11.6.2	保护用户连接	217
11.6.3	审计	220
11.6.4	数据库扫描	221
11.7	小结	221
第 12 章	Java 验证与授权服务	222
12.1	JAAS 概述	222
12.2	JAAS 主题	223
12.2.1	主题关系	223
12.2.2	生成主题	224
12.2.3	操纵主题属性	225
12.2.4	专门主题证书	226
12.3	用 JAAS 验证	227
12.3.1	登录模块配置与初始化	228
12.3.2	验证过程	231
12.3.3	回拨处理	233
12.4	用 JAAS 授权	236
12.4.1	JAAS 安全策略文件格式	236
12.4.2	使用 JAAS 安全策略文件	237
12.4.3	进行安全关键操作	238
12.4.4	JAAS 安全授权抽象	239
12.4.5	标准 Java 安全策略与 JAAS 权限	241
12.5	小结	242
第 13 章	CORBA 安全性	243
13.1	CORBA Security 概述	243
13.1.1	CORBA Security 包	244
13.1.2	CORBA 安全体系结构	245
13.1.3	核心 CORBA Security 接口	246
13.2	验证	249

13.3 代理	253
13.4 授权	254
13.5 审计	256
13.6 非否认	257
13.7 加密	260
13.8 安全策略	261
13.9 安全管理	263
13.10 小结	263
第 14 章 企业 JavaBeans 安全	264
14.1 EJB 安全概述	264
14.2 标准编程 EJB 访问控制	265
14.3 标准声明性 EJB 访问控制	268
14.4 厂家特定 EJB 访问控制	273
14.5 厂家特定 EJB 标识与验证	274
14.6 EJB 安全通信、代理与审计	277
14.6.1 EJB 连接安全性	277
14.6.2 EJB 主体代理	277
14.6.3 EJB 安全审计	277
14.7 小结	278
第 15 章 JSP 与 Java servlet 安全	279
15.1 公用网关接口	279
15.1.1 Web 服务器与 CGI 程序通信	279
15.1.2 CGI 程序——Web 服务器通信	279
15.2 对话状态维护	280
15.2.1 cookie	280
15.2.2 URL 改写	281
15.2.3 隐藏窗体字段	281
15.3 服务器方编程安全问题	281
15.3.1 截获对话状态信息	281
15.3.2 伪造对话状态信息	282
15.3.3 缓冲区溢出	282
15.3.4 数据验证	282
15.3.5 页面序列化	282
15.3.6 对话超时	283
15.3.7 信息报表	283
15.3.8 浏览器残余	283
15.3.9 用户验证	283
15.3.10 登记敏感信息	284
15.3.11 最低权限	284

15.4	Java servlet	284
15.4.1	为什么使用 servlet	284
15.4.2	Servlet API	285
15.4.3	servlet 如何工作	288
15.4.4	servlet 举例	298
15.4.5	servlet 安全性	301
15.5	JavaServer Pages	307
15.6	小结	307

第四部分 附 录

附录 A	Java 安全缺陷	310
附录 B	RSA 算法	316
附录 C	下载与安装 JCE	325
附录 D	Java 2 Security API	327
附录 E	下载与安装 Cryptix JCE 1.2	342
附录 F	使用 Keytool	346
附录 G	使用 jarsigner 工具	361