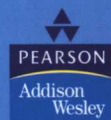
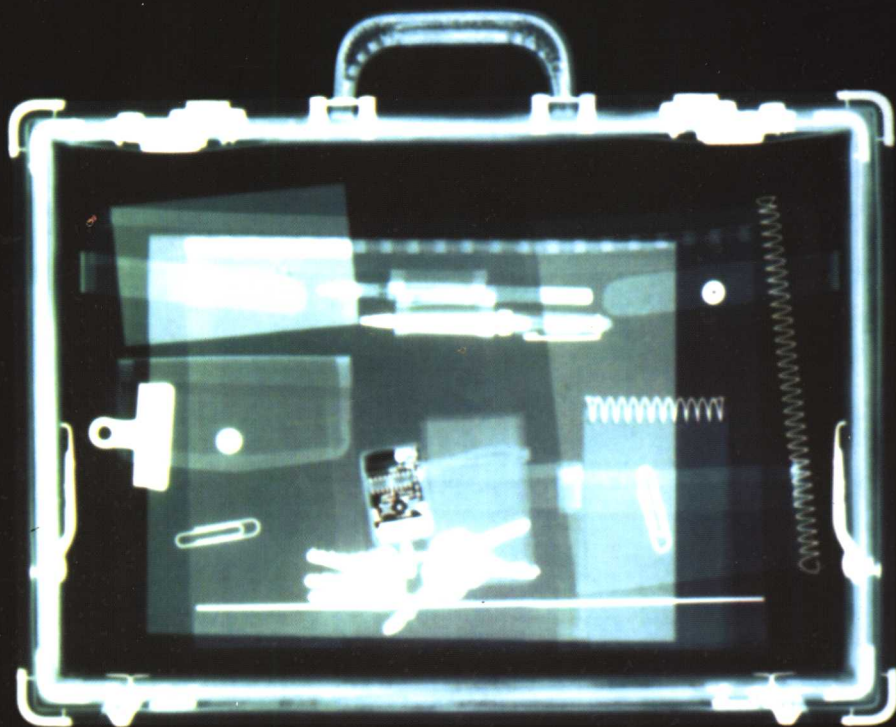


Enterprise Java Security
Building Secure J2EE Applications



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



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

Simplified Chinese edition copyright © 2005 by PEARSON EDUCATION ASIA LIMITED and Tsinghua University Press.

Original English language title : Enterprise Java Security:Building Secure J2EE Applications by Marco Pistoia,Nataraj Nagaratnam et al, Copyright © 2004

EISBN: 0-321-11889-8

All Rights Reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Addison-Wesley.

This edition is authorized for sale only in the People's Republic of China (excluding the Special Administrative Region of Hong Kong and Macao).

本书中文简体翻译版由 Pearson Education, Inc.授权给清华大学出版社在中国境内(不包括中国香港、澳门特别行政区)出版发行。

北京市版权局著作权合同登记号 图字: 01-2004-5002

版权所有,翻印必究。举报电话: 010-62782989 13501256678 13801310933

本书封面贴有 Pearson Education (培生教育出版集团)激光防伪标签,无标签者不得销售。

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

<http://www.tup.com.cn>

社总机: 010-62770175

组稿编辑: 曹康

封面设计: 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

地址: 北京清华大学学研大厦

邮编: 100084

客户服务: 010-62776969

文稿编辑: 于平

版式设计: 康博

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，它们在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 安全技术在建构包含基于 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 I 部分和 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 III 和 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

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員之一，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*

目 录

第 I 部分 企业安全与 Java

第 1 章	Java 技术与安全概述	3
1.1	为什么企业应用要采用 Java 技术.....	3
1.1.1	Java 2 平台标准版(Java 2 Platform Standard Edition, J2SE).....	4
1.1.2	Java 2 平台企业版(Java 2 Platform Enterprise Edition, J2EE).....	4
1.1.3	Java 组件.....	4
1.1.4	完整的、发展的和可互操作的 Java 安全技术.....	6
1.1.5	异类环境中的可移植性.....	7
1.2	企业级 Java 技术.....	8
1.2.1	中间层: Servlets、JSP 和 EJB.....	9
1.2.2	组件软件: 向正确方向迈出的一步.....	11
1.2.3	企业内部的安全通信.....	12
1.3	作为安全一部分的 Java 技术.....	12
1.4	企业安全集成的概述.....	13
1.4.1	身份认证与授权服务.....	13
1.4.2	密码服务.....	14
1.4.3	防火墙.....	14
1.5	上市的时间.....	14
1.5.1	对基本技术标准的支持.....	14
1.5.2	不同环境中的工程软件.....	15
1.5.3	时间是关键.....	16
第 2 章	企业网络安全与 Java 技术	17
2.1	网络体系结构.....	17
2.1.1	两层体系结构.....	17
2.1.2	三层体系结构.....	18
2.2	网络安全.....	21
2.3	服务器端的 Java 技术.....	23
2.3.1	WAS 组件.....	24
2.3.2	WAS 安全环境.....	25
2.4	Java 与防火墙.....	26
2.4.1	TCP/IP 报文.....	27
2.4.2	通过防火墙的程序间通信.....	28

2.4.3 防火墙对 Java 程序的影响	32
2.5 小结	37

第 II 部分 Enterprise Java 组件安全

第 3 章 Enterprise Java 安全基础	41
3.1 企业系统	41
3.2 J2EE 应用	42
3.2.1 EJB 模块	43
3.2.2 Web 模块	44
3.2.3 应用客户端模块	44
3.3 ORB 间的安全互操作	44
3.4 连接器	45
3.5 Java 消息传送服务(JMS)	45
3.6 一个简单的电子商务请求流程	46
3.7 J2EE 平台角色	47
3.7.1 应用组件提供者	48
3.7.2 应用组装者	49
3.7.3 部署者	50
3.7.4 系统管理员	51
3.7.5 J2EE 产品提供者	52
3.8 J2EE 安全角色	53
3.9 声明性安全策略	55
3.9.1 登录配置策略	55
3.9.2 认证策略	59
3.9.3 委托策略	61
3.9.4 连接策略	62
3.10 程序性安全	64
3.10.1 获取身份信息	65
3.10.2 预应授权	66
3.10.3 对 EIS 的应用管理式登录	67
3.11 WAS 环境内部的安全通信	68
3.12 安全电子商务请求流程	70
第 4 章 Servlet 和 JSP 安全	72
4.1 介绍	72
4.1.1 Java Servlet	73
4.1.2 JSP 技术	74
4.2 Servlet 的优点	75
4.3 Servlet 生命周期	76
4.4 Web 模块的部署描述符	79

4.5	认证	80
4.5.1	登录配置策略	80
4.5.2	一次登录, 资源尽享	86
4.6	授权	88
4.6.1	调用链	88
4.6.2	保护指定的 URL	89
4.6.3	保护 URL 模式	90
4.6.4	完全保护	91
4.6.5	理解优先级规则	92
4.6.6	数据约束——只能通过 SSL 传送	93
4.7	主体委托	94
4.8	程序性安全	95
4.8.1	主体信息	95
4.8.2	授权信息	96
4.8.3	SSL 属性信息: 证书和密码组	99
4.8.4	程序性的登录	101
4.9	Web 组件的运行时约束	101
4.10	使用方式	102
4.10.1	使用 HTTPS 连接到外部 HTTP 服务器	103
4.10.2	安全地维持状态	104
4.10.3	pre-servlet 与 post-servlet 处理	106
4.11	分割 Web 应用	109
第 5 章	EJB 安全	111
5.1	引言	111
5.2	EJB 角色和安全	112
5.2.1	EJB 提供者	113
5.2.2	应用组装者	124
5.2.3	部署者	128
5.2.4	系统管理员	128
5.2.5	EJB 容器提供者	129
5.3	认证	129
5.4	授权	130
5.5	委托	130
5.6	安全考虑事项	131
第 6 章	Enterprise Java Security 部署实例	132
6.1	规划组件安全系统	132
6.1.1	客户端访问	133
6.1.2	表示层	133
6.1.3	业务逻辑	134

6.1.4	资源适配器和遗留应用	134
6.2	部署拓扑结构	135
6.2.1	入门级	135
6.2.2	集群环境	136
6.2.3	加另一个防御等级	137
6.2.4	使用安全缓存反向代理服务器进行防御	137
6.3	安全通信信道	139
6.3.1	HTTP 连接	139
6.3.2	IIOP 连接	139
6.3.3	JMS 连接	139
6.3.4	连接到非 J2EE 系统	140
6.3.5	关于其他主题	140
6.4	安全性考虑	140

第III部分 Java 2 安全基础

第 7 章	J2SE 安全基本原理	143
7.1	访问类、接口、域和方法	144
7.2	类加载器	145
7.2.1	类加载机制的安全责任	145
7.2.2	被加载类的可靠性级别	146
7.2.3	类加载过程	150
7.2.4	构建定制的 ClassLoader	153
7.3	类文件验证器	156
7.3.1	类文件验证器的责任	158
7.3.2	类文件验证器的四个关口	159
7.3.3	字节码验证器的详细细节	162
7.3.4	类文件验证器的一个例子	164
7.4	安全管理器	166
7.4.1	安全管理器的职责	166
7.4.2	安全管理器的操作	168
7.4.3	攻击类型	169
7.4.4	恶意代码	170
7.4.5	安全管理器扩展	172
7.5	三个 Java 安全支柱之间的互相依赖	177
7.6	小结	177
第 8 章	Java 2 许可模型	178
8.1	Java 2 访问控制模型总览	178
8.1.1	特权修改的词法范围	179

8.1.2	Java 2 安全工具	180
8.1.3	JAAS	181
8.2	Java 许可	181
8.2.1	许可目标和操作	182
8.2.2	PermissionCollection 类和 Permission 类	182
8.2.3	Permission 类中的 implies() 方法	182
8.2.4	PermissionCollection 类和 Permission 类中的 implies() 方法	183
8.2.5	Permission 隐式地等同于 AllPermission	183
8.3	Java 安全策略	184
8.3.1	联合多个签名者	185
8.3.2	多个策略文件, 一个激活的策略	185
8.4	CodeSource 的概念	185
8.5	ProtectionDomain	186
8.5.1	在 ProtectionDomain 类中的 implies() 方法	187
8.5.2	系统域和应用域	187
8.5.3	Class、ProtectionDomain 和 Permission 之间的关系	187
8.6	基本的 Java 2 访问控制模型	188
8.6.1	场景: 当前线程的简单检测	190
8.6.2	SecurityManager 和 AccessController	192
8.7	Java 2 特权代码	193
8.7.1	构造特权代码的安全建议	194
8.7.2	如何编写特权代码	194
8.7.3	特权代码场景	196
8.8	ProtectionDomain 继承	201
8.9	Java 2 访问控制模型中的性能问题	202
8.9.1	去除复制 ProtectionDomain 的操作	202
8.9.2	在系统域之外过滤	202
8.9.3	在第一个特权栈帧处停止验证	202
8.10	小结	202
第 9 章	Java 认证与授权服务(JAAS)	203
9.1	JAAS 概述和 JAAS 术语	203
9.2	认证	205
9.2.1	通过 LoginModule 实现可插的认证	205
9.2.2	JAAS 的 LoginModule 模块的示例	208
9.3	授权概述	224
9.3.1	基于 J2SE 保护域的授权概述	225
9.3.2	向线程添加 Subject	226
9.3.3	安全授权策略文件	230
9.3.4	基于 Subject 的授权算法示例	233

9.3.5 对 JAAS 的其他观察	243
9.4 JAAS 与 J2EE	244
9.4.1 在不同 JVM 中执行的 Web 应用服务器	245
9.4.2 J2EE 环境中的 JAAS Subject	245
9.4.3 跨越鸿沟	245
9.4.4 企业级安全策略管理	246
9.5 可插入认证的其他技术支持	246

第IV部分 企业级 Java 与密码学

第 10 章 密码学理论	249
10.1 密码学的目标	249
10.2 秘密密钥密码学	251
10.2.1 算法与技术	251
10.2.2 秘密密钥安全属性	257
10.3 公开密钥密码学	260
10.3.1 算法与技术	260
10.3.2 公开密钥安全属性	265
10.3.3 数字签名	267
10.3.4 数字证书	268
10.3.5 秘密密钥分发	270
第 11 章 Java 2 平台与加密技术	272
11.1 JCA 和 JCE 框架	272
11.1.1 术语和定义	272
11.1.2 JCA 和 JCE 工作原理	273
11.1.3 JCA 和 JCE 提供者	275
11.1.4 引擎类和 SPI 类	280
11.2 JCA API	282
11.2.1 java.security.SecureRandom 类	282
11.2.2 java.security.Key 接口	283
11.2.3 java.security 包的 PublicKey 接口和 PrivateKey 接口	283
11.2.4 java.security.KeyFactory 类	283
11.2.5 java.security.KeyPair 类	283
11.2.6 java.security.KeyPairGenerator 类	283
11.2.7 java.security.KeyStore 类	284
11.2.8 java.security.MessageDigest 类	286
11.2.9 java.security.Signature 类	288
11.2.10 java.security 包中的 AlgorithmParameters 和 AlgorithmParameterGenerator 类	298
11.2.11 java.security.SignedObject 类	298

11.2.12	java.security.spec 包	299
11.2.13	java.security.cert 包	300
11.2.14	java.security.interfaces 包	300
11.3	JCE API	300
11.3.1	javax.crypto.Cipher 类	301
11.3.2	javax.crypto 包的 CipherInputStream 类和 CipherOutputStream 类	302
11.3.3	javax.crypto.SecretKey 接口	304
11.3.4	javax.crypto.spec.SecretKeySpec 类	304
11.3.5	javax.crypto.KeyGenerator 类	305
11.3.6	javax.crypto.SecretKeyFactory 类	305
11.3.7	javax.crypto.SealedObject 类	305
11.3.8	javax.crypto.KeyAgreement 类	306
11.3.9	javax.crypto.Mac 类	307
11.4	实践中的 JCE	308
11.4.1	Bob 的程序	308
11.4.2	Alice 的程序	310
11.5	安全考虑	312
第 12 章	J2EE 中的 PKCS 与 S/MIME	313
12.1	PKCS 概述	313
12.1.1	PKCS#1: RSA 加密标准	314
12.1.2	PKCS#5: 基于密码的加密标准	314
12.1.3	PKCS#7: 加密消息语法标准	315
12.1.4	PKCS#8: 私有密钥信息语法标准	315
12.1.5	PKCS#9: 选择属性类型	315
12.1.6	PKCS#10: 证书申请语法标准	315
12.1.7	PKCS#12: 个人信息交换语法标准	316
12.2	S/MIME 概述	317
12.3	PKCS 和 S/MIME 的签名和验证事务	317
12.3.1	有关 PKCS#7 标准的思考	319
12.3.2	使用 PKCS 和 S/MIME	320
12.4	带 PKCS 和 S/MIME 的加密事务	321
12.5	安全考虑	321
12.6	展望未来	322
第 13 章	J2EE 环境下的 SSL 和 TLS 协议	323
13.1	SSL 和 TLS 协议	323
13.1.1	record 协议	324
13.1.2	handshake(握手)协议	324
13.2	HTTPS	326
13.3	通过 SSL 支持构建 J2EE 产品	326

13.3.1	使用 SSL 保护认证期间的用户 ID 和密码	326
13.3.2	基于证书认证的 SSL	327
13.3.3	反向代理服务器和 WAS 的相互认证	328
13.3.4	SSL 中基于 Cookie 的单点登录	328
13.3.5	基于证书认证的单点登录	329
13.3.6	SSL 保护通信信道	329
13.4	在 J2EE 程序中使用 SSL	329
13.4.1	JSSE	329
13.4.2	信任管理员	330
13.4.3	信任库	330
13.5	示例	331
13.5.1	无 SSL 的基本场景	331
13.5.2	带 SSL 的场景	337
13.6	小结	361

第 V 部分 高级专题

第 14 章	Web 服务的企业级安全	365
14.1	XML	365
14.2	SOAP	366
14.3	WSDL	367
14.4	Web 服务的安全：动机	367
14.5	安全技术	368
14.5.1	XML 与加密技术	369
14.5.2	WS-Security	371
14.6	Web 服务安全模型的原则	371
14.6.1	Web 服务消息安全	374
14.6.2	WS-Policy	375
14.6.3	WS-Trust	376
14.6.4	WS-SecureConversation	376
14.6.5	WS-Privacy	377
14.6.6	WS-Federation	377
14.6.7	WS-Authorization	377
14.6.8	示例	377
14.7	应用模式	378
14.8	使用场景	379
14.9	Web 服务提供者安全	380
14.9.1	用户认证	380
14.9.2	强制授权	382
14.10	安全考虑	383