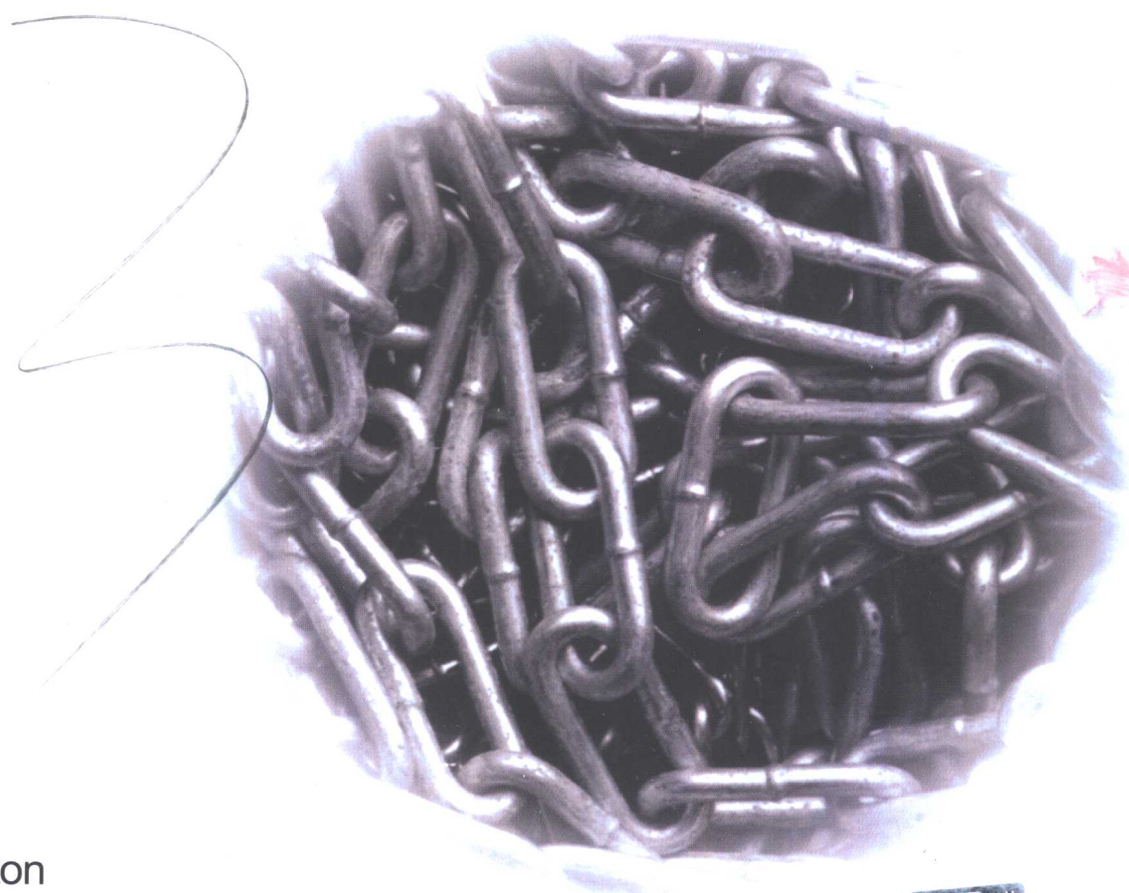


Java Security Solutions

Java

安全解决方案



Rich Helton

Johennie Helton 著

袁泉 吴静 等译



清华大学出版社

Java 安全解决方案

Rich Helton

著

Johennie Helton

袁泉 吴静 等译

清华大学出版社

北 京

北京市版权局著作权合同登记号：图字：01-2002-6317

内 容 简 介

本书全面介绍了 Java 安全及相关技术，展示了充分利用 Java 的安全解决方案(如加密、算法和体系结构等)的方法。本书首先介绍了有关安全的基础知识，然后解释了当前的 Java 安全工具、与安全有关的概念、协议及各种规范等，并通过实际的安全示例，深入阐述了用户使用各种技术的原因和时机，及其具体实现方法。

本书源代码示例丰富，并提供了许多实际的安全解决方案，非常适合于 Java 开发人员、Java 体系结构师和系统体系结构师阅读。

EISBN: 0-7645-4928-6

Java Security Solutions

Rich Helton, Johennie Helton

Copyright © 2002 by Wiley Publishing, Inc.

Original English Language Edition Published by Wiley Publishing, Inc.

All Rights Reserved.

本书中文简体字版由 Wiley Publishing 公司授权清华大学出版社出版。未经出版者书面许可，不得以任何方式复制或抄袭本书的任何部分。

版权所有，翻印必究。

本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目(CIP)数据

Java 安全解决方案/(美)海尔顿, (美)海尔顿著; 袁泉等译. —北京: 清华大学出版社, 2003

书名原文: Java Security Solutions

ISBN 7-302-06437-7

I. J... II. ①海... ②海... ③袁... III. JAVA 语言—程序设计 IV. TP312

中国版本图书馆 CIP 数据核字(2003)第 018867 号

出 版 者: 清华大学出版社(北京清华大学学研大厦, 邮编 100084)

[http:// www. tup. com. cn](http://www.tup.com.cn)

责任编辑: 陈宗斌

封面设计: 康博

版式设计: 康博

印 刷 者: 北京市清华园胶印厂

发 行 者: 新华书店总店北京发行所

开 本: 787×1092 1/16 印张: 36.25 字数: 927 千字

版 次: 2003 年 4 月第 1 版 2003 年 4 月第 1 次印刷

书 号: ISBN 7-302-06437-7/TP·4851

印 数: 0001~4000

定 价: 69.00 元

前言

欢迎阅读本书。本书将介绍一般性安全知识，并重点讲述 Java 安全，另外还将介绍加密技术、算法和体系结构。本书为安全问题提供了实用解决方案，不仅介绍了各种安全技术，还解释了这些技术的必要性和使用方法，以及如何扩充 Java 来提供更高的安全。书中的源代码是用 Java 编写的，旨在说明在 Java 中安全的实现方式。本书的内容包括：如何使用 Java 组件，如何扩充这些组件，诸如 RSA 之类的算法的重要性，以及有关基本协议的一些内容。简言之，它要回答何时、如何以及为什么在安全解决方案中使用 Java 组件。

学习目标

本书所涉及的一些规范包括 J2EE、WebServices、CORBA、JAAS、RMI、JSSE、SKIP、SASL、GSS-API、IPSec、X.509 证书、加密技术、RSA、椭圆曲线加密技术、DSS、DSA、Kerberos、LDAP、TLS、WTLS、消息摘要、密钥协定、密钥管理、Java 访问、密码、防火墙、网络安全和 PKI 等。旨在帮助您：

- 扮演成一个黑客，以找出那些可能被黑客利用的安全漏洞
- 理解安全构件块，以充分利用安全功能
- 学习如何高效充分应用 Java 安全功能
- 实际接触安全算法及其实现方式
- 了解在企业内部确保安全通信的过程
- 学习如何为企业应用程序添加安全功能
- 了解密码
- 确保消息验证和数据完整性
- 了解网络安全体系结构
- 纵览整个解决方案，并逐步找出易受攻击之处

Java 的作用

当前，Java 是开发 Web 应用程序和企业解决方案的首选语言。解决方案需要有在组件中进行分布式通信的分布式系统，支持这种分布式通信的有 CORBA、RMI 或 IIOP 之上的 RMI，这些技术和 Java 提供了一个用于开发安全解决方案的工具集。从 Java 语言出现以来，安全就一直是一个主要的设计目的。Java 提供了开发语言、运行时环境、API 以及非常适用于安全系统开发的工具。由于 Java 开发包(JDK)1.4 包含许多加密组件和支持与开发安全解决方案相关的技术，因而成为技术标准。这些技术包括 X.509 证书、密钥协定、指定安全策略的方法、身份验证、授权、代码标记和加密支持。



JDK 1.4 在它的分发版中集成了用作加密组件的 Java Cryptography Extension(Java 加密扩充, JCE), 以及 Java Authentication and Authorization Services(Java 身份验证和授权服务, JAAS)。Java 还提供了 Java Secure Socket Extension(Java 安全套接字扩充, JSSE)。尽管不使用这些技术, 您仍可以创建解决方案, 但这些解决方案和使用 JDK 1.4 创建的方案相比, 移动性差, 而且更加昂贵。毫无疑问, 花时间学习 Java 技术是非常必要的。为了理解这些技术的用法, 您需要了解各种 Java 组件出现的原因、时机、使用方式以及内容。这就是本书的目标。

读者对象

本书面向所有想了解安全问题和如何防止安全侵犯的读者。如果您想了解如何阐述安全利害关系, 以及如何用 Java 实现许多标准和协议, 那么本书就是为您所著的。本书适用于想要成为高级 Java 开发人员、Java 体系结构师和系统体系结构师的人员。学习本书前, 您应当具备基本 Java 编程知识, 了解 EJB 部署、Java 语言构造、HTML、Web 服务器和应用程序服务器技术等概念。本书将从安全角度来阐述这些概念, 而不只是停留在介绍层次。

全书结构

本书从各个角度讨论了安全性。首先介绍了安全性及其要求, 然后阐述了满足这些要求的 Java 组件, 及其用法, 最后介绍了资源、企业和网络安全。

本书共分为 9 个部分。

第 I 部分: 安全介绍

该部分介绍安全基础, 阐释安全的必要性, 并介绍黑客的思考方式、黑客可用的工具, 以及最常见的攻击形式。另外, 该部分还对安全要素和可用于安全的各种 Java 组件进行分类。如果您想从 Java 安全、它的组件和实现开始学习, 建议您直接跳转至第 3 章“Java 安全组件”。

第 II 部分: 身份和验证

该部分概述密钥管理算法、椭圆曲线加密技术(ECC)和密钥以及密钥管理的 Java 实现。内容包括: 密钥对实例、数学讨论、Diffie-Hellman、密钥生成、中间人的攻击、RSA 密钥交换、ECC、安全随机性和 DES 实例。

第 III 部分: 数据完整性

该部分介绍数据完整性、散列函数、消息摘要算法、消息验证和数字签名。内容包括 RSA、ECC、MAC、SHA-1 等。它列举了一个 MD5 实现、一个 SHA-1 算法、一个 MAC 算法和一个 DSA 签名实例。

第 IV 部分: 数据隐藏

该部分介绍密码, 以及如何实现密码(包括如何使用 CipherSpi)。还讨论了 PBE、Blowfish 和 Java Smart Cards(智能卡)。该部分包括一个 RSA 示例和一个示例实现、流加密器、PBE 和

Blowfish。

第 V 部分：使用 Java 的资源访问

该部分简要介绍了安全的通用标准。旨在帮助您理解应用程序中安全的必要性和如何使用 Java 满足这些要求。它介绍了 JAAS、Kerberos、GSS-API 和安全管理器，内容包括安全上下文、策略、配置、警戒对象、标记对象和 JAAS 等。

第 VI 部分：企业数据安全

该部分介绍了保护企业数据的必要性。重点讨论了为什么保护数据库，如何保护数据库，以及如何保护应用程序和数据存储库之间的通信。内容包括托管容器、应用程序标记和连接器 API。

第 VII 部分：网络访问

该部分介绍网络安全和体系结构，讨论 OSI 模型、DMZ、防火墙、HTTP 隧道、Java 套接字、SSL、TLS 和 JSSE。该部分列举了套接字示例(包括服务器、客户机和信道)和路由表 X.509 示例。

第 VIII 部分：公钥管理

该部分讨论 Java 数字证书，如 X.500 和 X.509，另外还讨论了 PKI 管理，内容包括“验证链、X.500、LDAP”、不可否认的验证、证书导入方法、CRL、CertPath 和 LDAP 示例。

第 IX 部分：企业访问

该部分介绍企业解决方案的必要性。前面讨论了 Java 安全模型、Java 权限、Web 层安全、Web 服务、JNDI、RMI、IIOP 和 EJB 安全。后面讨论了 BEA 的 WebLogic、IBM 的 WebSphere 及 Borland 的企业服务器的安全处理方式。

本书约定

本书用阴影突出显示代码清单和命令，以及代码中使用的其他术语。例如：

This is what a code listing looks like.

本书还使用以下的特殊段落来突出显示要点：

注释：

注释提供和讨论与主题有关的信息。通常包含和一个详细技术点相关的信息和详细描述。

提示：

提示提供一个更有效的方法，在讨论的主题上建议或给出一个指示。

注意：

注意提供一个潜在的错误使用、错误概念的警告，或是防御方法的要求。



相互参照:

相互参照把您带到对特定主题进行详细讨论的章节。

相关的 Web 站点

本书提供了一个配套的 Web 站点。该站点提供了本书的所有源代码。代码清单按章组织, 您可以直接下载所有示例。请访问 www.wiley.com/extras。

Web 站点 www.richware.com/JavaSecuritySolutions 包含一个链接表, 您可以通过它们访问相关的 RFC、文档以及与本书所涉及主题相关的站点。

资源

本书所用的源代码都已在 Windows 2000 下, 通过了 Java 2 平台标准版本 JDK 1.4, 以及 Java 2 软件开发包(企业版)的测试。

<http://Java.sun.com/Java2/> 提供了指向所需的 Java 2 技术的链接(<http://Java.sun.com/j2ee/download.html>, <http://Java.sun.com/j2se/1.4/download.html>)。

相关站点为本书各章提供所有源代码和测试脚本(run.bat)。一些示例代码需要 Sun 证书(Sun 证书随源代码提供)。指向其他重要资源的链接在相关章节中提供。

联系作者

我们希望能收到您的来信, 欢迎您对本书提出宝贵意见。如果您需要更多解释, 或有其他改进意见, 请及时与我们联系。

您可以通过邮箱 jssbook@richware.com, 直接将信寄给本书作者。

目 录

第 I 部分 安全介绍

第 1 章 安全基础	1
1.1 简介	1
1.2 保护信息	1
1.2.1 保护资源不受黑客侵犯	2
1.2.2 黑客的攻击方式	2
1.2.3 防御攻击的武器	3
1.3 保证安全的四个支柱	3
1.3.1 验证：用证书证明身份	3
1.3.2 授权：提供对系统资源的访问权限	4
1.3.3 机密性：使信息免遭未授权者访问	5
1.3.4 完整性：确认数据	6
1.4 把安全特征映射到数字世界	6
1.5 小结	8
第 2 章 黑客和他们的工具	9
2.1 简介	9
2.2 寻找黑客	9
2.2.1 截取和传输按键	9
2.2.2 键盘嗅探器	10
2.3 各种攻击类型及作用方式	11
2.3.1 社交工程	11
2.3.2 入侵系统	11
2.3.3 消极黑客攻击	12
2.3.4 积极攻击	13
2.4 了解网络攻击	14
2.4.1 网络监视术语	14
2.4.2 嗅探网络查找主机	14
2.4.3 黑客的实用程序库	15
2.4.4 嗅探系统计算机	19
2.4.5 模拟主机	21
2.4.6 IP 欺骗攻击	22
2.4.7 操作系统主动攻击	23



2.4.8 病毒攻击	24
2.5 防御黑客	26
2.6 小结	27
第 3 章 Java 安全组件	28
3.1 简介	28
3.2 安全元素分类	28
3.2.1 用主体和证书元素定义验证	29
3.2.2 用主体和权限元素定义授权	30
3.2.3 用密钥元素定义机密性	30
3.2.4 用安全散列元素定义完整性	32
3.3 Java 安全组件分类	33
3.3.1 提供验证的组件	34
3.3.2 提供授权的组件	36
3.3.3 提供机密性的组件	37
3.3.4 提供完整性的组件	39
3.4 组合各种组件	41
3.5 小结	42

第 II 部分 身份和验证

第 4 章 密钥管理算法	43
4.1 简介	43
4.2 了解密钥的用途	44
4.3 了解数学	47
4.3.1 对数	47
4.3.2 素数和随机数	51
4.4 对称和非对称密钥的比较	51
4.5 Diffie-Hellman 密钥交换	51
4.5.1 Diffie-Hellman 密钥交换	51
4.5.2 实现 Diffie-Hellman 密钥交换	53
4.5.3 了解中间人的攻击	61
4.6 Rivest、Shamir 和 Adleman 密钥交换	73
4.6.1 了解 RSA 密钥交换	73
4.6.2 实现 RSA 密钥交换	75
4.6.3 使用对称密钥	84
4.6.4 了解数据加密标准(DES)密钥	84
4.6.5 了解 Triple-DES 密钥	85

4.7 密钥交换的前景	86
4.8 小结	87
第 5 章 椭圆曲线加密技术	88
5.1 简介	88
5.2 了解 ECC 的数学原理	89
5.3 ECCDH 密钥交换	91
5.3.1 了解 ECC 密钥交换	91
5.3.2 了解服务提供者接口(SPI)	92
5.3.3 实现 ECC 密钥交换为一个 SPI	92
5.4 小结	104
第 6 章 通过 Internet 协议的密钥管理	105
6.1 简介	105
6.2 Internet 协议中的安全协议	105
6.2.1 传输和隧道模式	106
6.2.2 安全联系	107
6.2.3 确定安全级别	108
6.2.4 密钥交换的两个阶段	108
6.3 简单验证和安全层	110
6.3.1 定义 SASL	110
6.3.2 服务器询问和响应	111
6.4 小结	111
第 7 章 用 Java 实现密钥	113
7.1 简介	113
7.2 了解 DSA: 数字签名算法	114
7.3 用 Java 生成密钥对	115
7.3.1 实现	116
7.3.2 查找服务提供者	117
7.3.3 用密钥资料初始化密钥	119
7.4 用 Java 生成保密密钥	127
7.5 小结	131
第 8 章 密钥管理的 Java 实现	132
8.1 简介	132
8.2 KeyStore	133
8.3 PKCS#12 KeyStore	135
8.4 Truststore	136
8.5 TrustManager	136



8.5.1	Keytool	137
8.5.2	Jarsinger	141
8.6	策略文件	145
8.7	Policytool	147
8.8	小结	150

第III部分 数据完整性

第 9 章	保证数据完整性	151
9.1	简介	151
9.2	了解散列函数	151
9.3	了解消息摘要	152
9.3.1	加密和摘要	153
9.3.2	区分 MD	153
9.3.3	划分算法	153
9.4	了解不同的消息摘要算法	155
9.4.1	MD 算法	155
9.4.2	SHA-1 算法	166
9.4.3	RIPEMD-160	178
9.5	在 Java 中实现不同的消息摘要算法	178
9.6	小结	179
第 10 章	保证消息验证	180
10.1	简介	180
10.2	了解 MAC	180
10.3	实现 MAC	181
10.4	小结	191
第 11 章	签名完整性	192
11.1	简介	192
11.2	了解数字签名算法(DSA)	193
11.3	了解 RSA 数字签名算法	196
11.4	了解椭圆曲线数字签名算法	197
11.5	实现数字签名算法(DSA)	198
11.6	小结	214

第IV部分 数 据 隐 藏

第 12 章 了解密码	215
12.1 简介	215
12.2 了解对称密码	216
12.3 实现 RSA 公钥加密	222
12.4 一些安全建议	241
12.5 小结	242
第 13 章 用 JDK 扩充新密码	243
13.1 简介	243
13.2 实现 CipherSpi	243
13.3 实现 RC4 流密码	252
13.4 小结	256
第 14 章 应用密码	257
14.1 简介	257
14.2 了解 PBE	257
14.3 了解 Blowfish	262
14.3.1 块密码	262
14.3.2 生成子密钥和置换盒	263
14.3.3 读取明文文件	264
14.4 密码的一些实现	268
14.4.1 专利信息和安全	268
14.4.2 X.509 的思想	268
14.5 Java 智能卡基础	270
14.5.1 钱包里的计算机	271
14.5.2 卡外检验器	272
14.6 小结	274

第 V 部分 使用 Java 的资源访问

第 15 章 保护企业资源	275
15.1 安全系统的通用标准	275
15.1.1 通用标准的由来	275
15.1.2 通用标准构建块	275
15.2 了解安全需要	277
15.2.1 表明安全风险	278
15.2.2 声明安全目标	278



15.3	采取措施满足安全需要	279
15.3.1	考虑通信和可信路径或信道	279
15.3.2	考虑组件访问	280
15.3.3	考虑加密支持	280
15.3.4	考虑身份识别和验证	281
15.3.5	考虑安全审核	281
15.3.6	考虑用户隐私和用户数据保护	282
15.4	小结	282
第 16 章	通过 Kerberos 的 Java 验证和授权	283
16.1	Kerberos 简介	283
16.2	主名和密钥分配中心	284
16.2.1	Kerberos v4 和 v5 之间的区别	284
16.2.2	加密支持中的修改	284
16.2.3	对 TGS 的修改	284
16.2.4	对主名表示的修改	285
16.2.5	对 TGS 票据请求处理的修改	285
16.2.6	在 v4 中请求 TGS 票据	285
16.2.7	对服务票据请求处理的修改	287
16.2.8	对客户/服务器验证处理的修改	288
16.2.9	对票据的修改	288
16.3	Kerberos 验证器	289
16.4	Kerberos 主体数据库	290
16.4.1	命令	291
16.4.2	配置文件	292
16.5	Java Kerberos	293
16.6	小结	294
第 17 章	用 Java GSS-API 保护消息安全	295
17.1	简介	295
17.1.1	GSS-API 概述	296
17.1.2	GSS API 组件模型	298
17.2	用起始器和接受器实现 GSS	315
17.3	用 JAAS 验证	316
17.4	小结	319
第 18 章	Java 访问：安全管理器	320
18.1	简介	320
18.2	类加载器	321

18.3	安全管理器	322
18.4	访问控制器	323
18.4.1	警戒对象	325
18.4.2	签署对象	327
18.5	策略	329
18.6	权限集	334
18.6.1	设置权限	334
18.6.2	执行权限	335
18.7	小结	335
第 19 章	Java 验证和授权服务	336
19.1	JAAS 的定义	336
19.2	使用验证	337
19.2.1	了解基于主体的访问控制	337
19.2.2	了解可插入的验证模块标准	339
19.3	了解 JAAS 授权	351
19.3.1	了解主题	354
19.3.2	了解 ACL	358
19.4	小结	359

第VI部分 企业数据安全

第 20 章	处理数据库安全	360
20.1	简介	360
20.2	通过 JDBC 连接数据库	361
20.3	通过连接器体系结构连接数据库	363
20.4	保护数据库中的企业数据	365
20.5	小结	365

第VII部分 网络访问

第 21 章	网络安全体系结构	366
21.1	了解网络安全	366
21.2	网络概念简介	367
21.2.1	IP 地址	367
21.2.2	TCP 和 UDP	370
21.2.3	路由基础	378
21.3	防火墙	383
21.3.1	电路级网关	385



21.3.2	应用程序级的网关	385
21.3.3	包过滤	386
21.4	非军事区(DMZ)	387
21.5	了解代理防火墙	388
21.6	HTTP 隧道	390
21.7	Java 套接字	391
21.8	Java SOCKS	397
21.9	小结	400
第 22 章	SSL 和 TLS	401
22.1	安全套接字层(SSL)	401
22.1.1	历史	401
22.1.2	数字签名	402
22.1.3	消息摘要	403
22.2	SSL 层	403
22.2.1	握手协议	404
22.2.2	SSL 记录	406
22.3	SSL 会话和连接	407
22.3.1	SSL/TLS 模式	408
22.3.2	SSL 和验证	409
22.4	安全性和攻击	409
22.5	HTTPS: SSL 之上的 HTTP	410
22.6	WLS	411
22.6.1	WAP	411
22.6.2	改变物理介质	411
22.6.3	WSP	412
22.6.4	WTLS	412
22.7	小结	412
第 23 章	Java 安全套接字扩展	413
23.1	JSSE 体系结构	413
23.1.1	JSSE 提供者	417
23.1.2	SSLContext	418
23.1.3	SSLSession	421
23.1.4	JSSE SSLServerSockets	422
23.1.5	JSSE SSL 客户机套接字	429
23.1.6	客户机和服务器	438
23.1.7	HTTPSURLConnection	438
23.2	小结	439

第VIII部分 公 钥 管 理

第 24 章	Java 数字证书	440
24.1	数字证书简介	440
24.2	X.500 概述	441
24.3	X.509 规范	442
24.3.1	LDAP 服务	442
24.3.2	自签发证书	443
24.3.3	版本 2 惟一标识符字段	451
24.3.4	版本 3 公钥扩展	451
24.4	证书撤销	456
24.4.1	CRL 扩展	458
24.4.2	CRL 项	469
24.5	小结	471
第 25 章	PKI 管理	473
25.1	简介	473
25.2	证书链	474
25.3	X.500	475
25.3.1	识别名	475
25.3.2	目录信息基础	476
25.4	LDAP	477
25.5	证书组件	480
25.6	证书路径验证	480
25.7	不可否认	490
25.8	小结	491

第IX部分 企 业 访 问

第 26 章	Java 企业安全和 Web 服务安全	492
26.1	简介	492
26.2	Java 安全模型	493
26.2.1	沙箱模型	493
26.2.2	J2SDK v 1.4 中的安全	494
26.2.3	J2EE 安全	495
26.2.4	策略文件	495
26.3	Java 权限	496
26.4	企业组件模型	496



26.5	理解 Web 服务	497
26.5.1	处理 Web 服务安全	498
26.5.2	利用 XML 数字签名	499
26.5.3	理解 XML 加密	503
26.5.4	使用 UDDI 注册 Web 服务	503
26.5.5	使用 WSDL 定义 Web 服务接口	504
26.5.6	使用 SOAP 编码 Web 服务	506
26.6	小结	507
第 27 章	保护客户端组件	508
27.1	简介	508
27.2	分析 Java 目录服务	509
27.2.1	JNDI 体系结构概述	509
27.2.2	理解使用 JNDI 的安全	510
27.3	使用验证	511
27.3.1	配置进行验证的 Web 层	512
27.3.2	分析 Web 层的验证问题	513
27.4	使用访问控制	513
27.5	处理客户端安全	514
27.5.1	应用程序安全	515
27.5.2	Applet 安全	515
27.5.3	理解 web.xml 文件	516
27.6	使用 Servlet	517
27.7	使用 Java 服务器页面	517
27.8	客户端代码示例	519
27.8.1	理解设计	520
27.8.2	处理用户验证	521
27.8.3	处理 web.xml 文件	522
27.9	小结	532
第 28 章	保护服务器端组件	533
28.1	简介	533
28.2	用 CORBA 保证企业安全	534
28.2.1	回顾 CORBA	534
28.2.2	CORBA 安全概述	535
28.2.3	CORBA 主体	537
28.3	RMI	537
28.3.1	RMI 安全概述	538
28.3.2	IIOP 上的 RMI	539