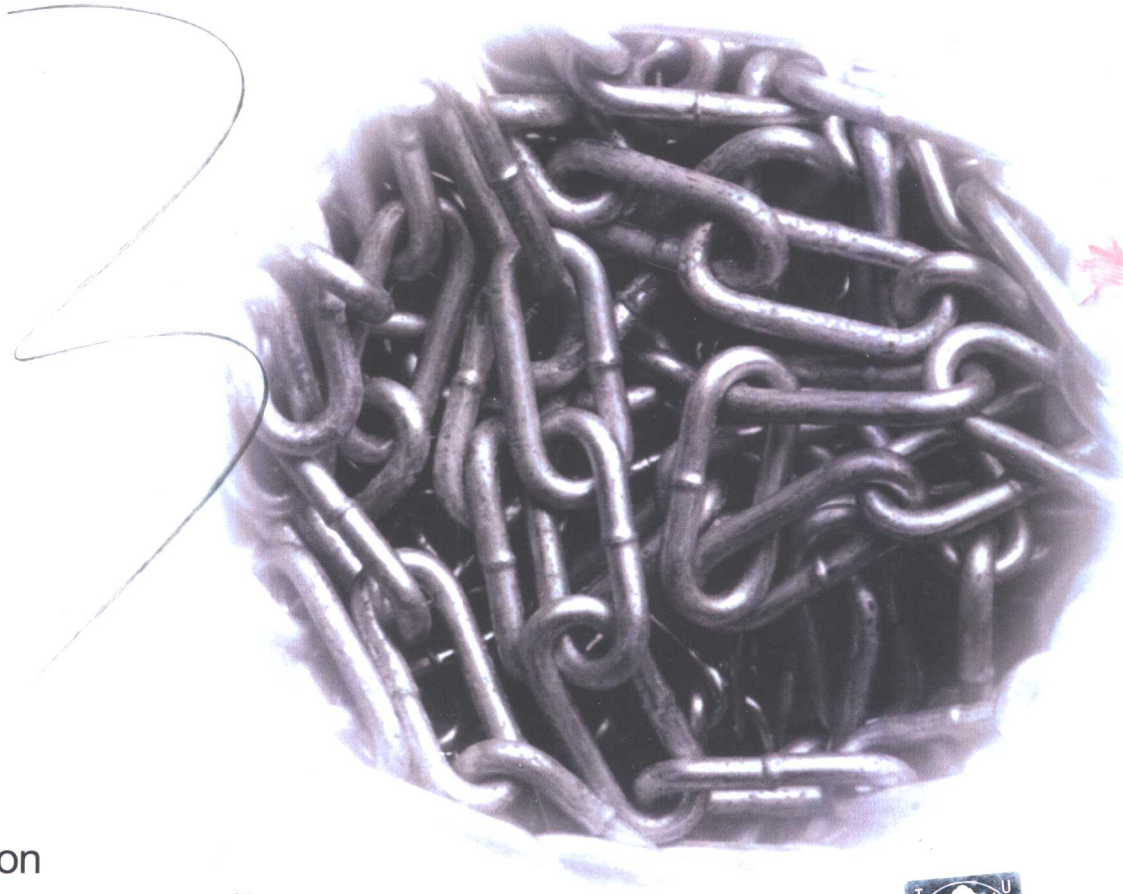
Java Security Solutions

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

Johennie Helton

著

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

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
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 遂道、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 II 部分　身份和验证

第III部分　数据完整性

第Ⅳ部分 数 据 隐 藏

第Ⅴ部分 使用 Java 的资源访问

第Ⅵ部分　企业数据安全

第Ⅶ部分　网 络 访 问

第Ⅷ部分 公钥管理

第Ⅸ部分 企业访问