Java Security

第二版
涵盖 JAAS & JSSE

Java™ 安全

Scott Oaks 著
林琪 译

O'REILLY®
中国电力出版社

Java™安全

第二版

Scott Oaks 著

林琪 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly & Associates, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

Java™ 安全 /（美）奥克斯（Oaks, S.）编著；林琪译 . - 北京：中国电力出版社，2002.3

书名原文：Java™ Security, Second Edition

ISBN 7-5083-0858-1

I. J... II. ①奥... ②林... 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（2002）第 014860 号

北京市版权局著作权合同登记

图字：01-2001-3296 号

书　　名 / Java™ 安全（第二版）

书　　号 / ISBN 7-5083-0858-1

责任编辑 / 夏平

封面设计 / Hanna Dyer，张健

出版发行 / 中国电力出版社（www.infopower.com.cn）

地　　址 / 北京三里河路 6 号（邮政编码 100044）

经　　销 / 全国新华书店

印　　刷 / 北京市地矿印刷厂

开　　本 / 787 毫米 × 1092 毫米　16 开本　38 印张　562 千字

版　　次 / 2002 年 4 月第一版　2002 年 4 月第一次印刷

印　　数 / 0001-5000 册

定　　价 / 69.00 元（册）

O'Reilly & Associates 公司介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly & Associates公司授权中国电力出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly & Associates 公司是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到 WebSite（第一个桌面PC的Web服务器软件），O'Reilly & Associates 一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates是最稳定的计算机图书出版商——每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly & Associates公司具有深厚的计算机专业背景，这使得O'Reilly & Associates形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly & Associates 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly & Associates 依靠他们及时地推出图书。因为O'Reilly & Associates紧密地与计算机业界联系着，所以O'Reilly & Associates 知道市场上真正需要什么图书。

Java™安全

目录

前言

当我向一个同事说起我要写一本关于Java™安全的书时，他立刻就向我询问有关防火墙和Internet DMZ（译注1）方面的问题，另一个同事听到我们的谈话后，马上提出了关于电子商务的一些问题，还有一个同事则对虚拟专用网表示了浓厚的兴趣。这个现象本身就很有趣，不过需要说明，我所要讨论的是如何让Java applet获得读取文件的权限这样的内容。

如果题目中有“安全”两字，往往就会造成以上的情形，实际上，安全是一个范围很广的研究领域，每个人对安全都有自己的理解。Java 安全和网络安全（包括Internet 安全）既有互补的一面，又有重叠的一面，这使问题显得更加复杂。例如可以用Java在网络上传送加密数据，这就需要在Java程序中设计加密策略；此外还可以建立虚拟专用网，从而对网络传送的所有信息都进行加密，这种方式就不用在Java程序中自行设计加密策略了。

这本书将从Java 程序的角度讨论安全。在书中，我们将讨论Java基本平台中有关安全的特性，主要包括类装载器、字节码校验器和安全管理器，并且还将讨论Java在安全领域的最新进展，包括数字签名、安全提供者和存取控制器等。本书的主旨

译注1：DMZ是Demilitarized Zone（非军事化区）的缩写，来源于朝鲜战争。在计算机安全中指的是企业局域网的周边网络（peripheral network）。

是帮助读者建立对Java安全模型体系结构的理解，并能充分了解如何在程序设计和管理两方面应用此安全模型。

读者对象

本书主要面向那些需要编写安全Java应用程序的程序员。书中重点介绍了Java中提供安全性的各种API。我们将讨论Java 2标准版中相关API的使用方法，包括如何在自行开发的应用程序中使用这些API，另外对于在Java Plug-in中运行的applet，本书也将介绍有关安全API的使用方法。任何一个版本的Java 2平台都支持Java Plug-in，因此applet可以对浏览器不做要求，而直接运行在虚拟机中。因此目前常用的浏览器中，如Internet Explorer（版本3及更高版本）、Netscape Navigator（版本4及更高版本）和Opera等等，都提供了对Java 2的全面支持。在Navigator和Opera的最新版本中，Plug-in是其所支持的虚拟机的惟一形式。从安全性的角度来看这一点至关重要，因为还没有任何一种内嵌在浏览器中的虚拟机能够提供对Java 2安全模型的支持。

本书的另一类读者是终端用户，以及对Java安全感兴趣的系统管理员。书中将介绍基本Java平台所提供的安全功能，同时还将说明Java应用程序和在Java Plug-in中的Java applet如何使用这些功能。我们不会过分深入地研究支持Java的浏览器本身的安全特性，但会以发展的眼光指出浏览器供应商应如何调整Java安全特性。终端用户和系统管理员通过阅读本书（可以跳过一些编程实例），将对Java平台的基本安全特性有所了解，而且对于如何管理这些安全特性将有所认识。对于那些对Java使用的安全性（更严格地说应该是风险性）很感兴趣的终端用户或系统管理员来说，这本书尤其有用：我们将详细地介绍Java安全模型的实现，使读者可以直接利用此模型进行编程（必要时也可以对之进行调整）；此外，书中还将深入阐述此安全模型的工作原理，读者可以根据实际情况判断Java是否能够满足其安全需要。

从编程的角度，我们假设读者能够熟练使用Java进行编程，尤其对Java应用程序的开发有一定经验。在讨论高级安全特性和加密算法时，我们也认为程序员只对相关API的使用感兴趣。因此，我们只对数字签名做基础性的介绍，并讨论如何创建和使用它，而对作为数字签名基础的加密理论、数字签名提供安全保障的原因等内容则不深入讨论。对于精通此道的程序员，我们还将介绍如何扩展这些API以支持新的加密算法，不过有关加密的数学知识和严格的定义必须要用另一本书来详细说明了。

所用版本

本书主要介绍Java 2标准版、版本1.3（通常简称为1.3）的有关内容。Java 2平台的安全模型与Java 1所提供的大相径庭。许多基本的安全接口如存取控制器只在Java 2中提供，此外与Java 1.1相比，Java 2版本中的一些API变化也很大。另一方面，Java 2中版本1.2和1.3之间的变化倒不明显，因此我们所介绍的许多内容对1.2也是适用的。

在书中我们还讨论了三个Java扩展包：JCE（Java加密扩展包）1.2.1版本、JSSE（Java安全套接字扩展包）1.0.2版本以及JAAS（Java鉴别与授权服务）1.0版本。这些扩展包都基于1.3版本的Java 2平台。

本书中所用的代码实例可以从O'Reilly的网站获得，其网址为：*http://www.oreilly.com/catalog/javasec2/*。

本书约定

本书中，以下内容将用等宽字体（constant width font）表示：

- 代码实例
- 类、变量和文本中出现的方法名

而以下内容则用斜体（*Italicized font*）表示：

- 文件名
- 主机和域名
- URL地址

当第一次介绍新的方法或类时，将以斜体表示它们，如：

public void checkAccess (Thread t)

这个函数的作用是检查当前线程是否能够修改参数*t*所指定线程的状态。

命令约定

在本书中许多地方都用到了命令，特别是在讨论管理的章节和附录中有大量的命令出现。为统一起见，约定将以UNIX系统平台为背景说明命令的执行情况，如：

```
piccolo% keytool -export -alias sdo -file /tmp/sdo.cer
Enter keystore password: ******
Certificate stored in file </tmp/sdo.cer>
```

在这些命令实例中，由用户或管理员输入的内容用黑体字（**bold font**）表示，其余的文本则是执行命令后所输出的结果（串piccolo% 表示命令提示）。在其他系统中，需要对文件名做必要的调整以满足系统要求（如对Microsoft Windows 系统，就应该用形如 *C:\sdo.cer* 的文件名）。但是一定要记住，命令行参数通常指定的是一个URL地址而非文件名，在URL地址中一定要用斜线而非反斜线。在这种情况下，不同系统中的参数设置是相似的，不过在Microsoft Windows 系统中需要指定驱动器，如Unix目录 *file:///files/sdo/* 在Microsoft Windows 系统中应表示为 *file:/C:/files/sdo/*。指定URL参数时，还需要设置协议以区别它并非文件名，实际上协议名仍被处理为串，而不需要对协议进行分析。

但是，注意由于Microsoft Windows 系统通常使用斜线（/）来设置命令行选项，而Java 工具（以及相应的系统中）则一般使用连字符（-）来表示选项，所以书中所举实例在不同平台上惟一的区别就在于文件名或URL名的差别。

代码约定

本书中的代码实例（以及在线实例）是按章节组织的。每个类将按照章的内容放在相应的包中。例如，第三章中的Test类就在包javasec.samples.ch03中。解开代码时，需要设置一个目录（*javasec*），所有子目录和源文件都将按照层次关系作为其下级目录或文件建立。

有两种简单的处理方法。第一种方法是解开源代码时保持原目录，不需设置类路径（classpath），在引用时直接取包的绝对路径名即可。因此要编译和执行第三章中的Test类时，需要如下命令行：

```
piccolo% javac javasec/samples/ch03/Test.java
piccolo% java javasec.samples.ch03.Test
Your account number is 0001 0002 0003 0004
```

还有一种方法，即在源代码所在的目录下工作，并设置类路径，具体命令如下：

```
piccolo% javac -classpath ../../.. Test.java
piccolo% java -classpath ../../.. javasec.samples.ch03.Test
Your account number is 0001 0002 0003 0004
```

如果命令占多行，就需要用到反斜线：

```
piccolo% java -classpath ../../.. javasec.samples.ch09.PrintCert \
              /files/sdo/foo/bar/very/long/command
```

以上命令可以在一行内输完，或者，如果需要占多行，就必须用系统所要求的转义符进行连接（如Unix 系统中的反斜线）。

全书的组织结构

本书是按自底向上的方式进行组织的：首先从最低层研究Java 的安全性，再逐步扩展到相应的高级特性。

第一章 Java 应用安全

这一章对Java 应用中所用的安全模型（Java 沙箱）做了总体介绍，从而为其他各章的介绍奠定了基础。

第二章 默认沙箱

这一章讨论默认沙箱的相关参数，以及如何利用策略来调整沙箱的状态。终端用户和管理员可以通过这一章了解建立Java安全策略的方法(包括如何使用策略工具 policytool 实现策略的调整)，还引入了实现策略的相关概念。

第三章 Java 语言安全

这一章讨论了Java 语言中的内存保护机制，以及如何利用这些保护机制提供具体的安全手段，另外还介绍了利用字节码校验器进一步增强安全性的有关内容。

第四章 安全管理器

这一章讨论的是安全管理器，这是保证Java 应用级安全的主要接口。安全管理器负责对本地资源的访问控制，包括文件、网络、打印机等等。

第五章 存取控制器

在Java 2中，存取控制器是安全管理器的基础。这一章讨论如何使用存取控制器以保证应用程序达到“细粒度的”安全性。

第六章 Java 类装载器

这一章讨论类装载器。它本身也是一个Java类，其作用是读入Java类文件并将其转化为类。从安全的角度来看，若需要区别原始类和做了数字签名的类时，类装载器的重要性就体现出来了，而且如果做了签名，还可以利用类装载器判断出相应的签名者，因此关于类装载器的介绍将贯穿于全书之中。

第七章 加密介绍

这一章对Java安全包中使用的加密算法做了概述。它将作为余下各章讨论的基础。

第八章 安全提供者

这一章讨论Java 安全包的体系结构，以及如何利用此结构扩展或替换SDK中的默认加密算法。

第九章 密钥与证书

这一章讨论构造加密密钥和证书的有关API。

第十章 密钥管理

这一章讨论如何在Java程序中管理密钥，具体包括：密钥存储方式以及存储位置，并介绍了如何查找和验证密钥。这一章中还将讨论数字密钥的传输方式。

第十一章 消息摘要

这一章讨论消息摘要计算的有关内容，包括摘要的建立、使用和实现方法。

第十二章 数字签名

这一章介绍如何创建、使用和实现数字签名。另外还讨论了签名类的有关内容。

第十三章 基于密码的加密

这一章讨论JCE（Java 加密扩展包）中使用的加密方法，开发人员可以利用这些方法对数据进行加密和解密。

第十四章 SSL 和 HTTPS

这一章讨论JSSE（Java 安全套接字扩展包）提供SSL 加密的方法，利用此方法可以通过TCP 套接字实现数据加密。这里还介绍了HTTPS Internet 协议的实现方法。

第十五章 鉴别与授权

这一章讨论JAAS（Java 鉴别与授权服务）的有关内容，它允许在应用中实现对用户的认证、基于用户的登录标识符ID或信任状设置相应的权限。

附录一 java.security 文件

此附录提供了*java.security*文件及必要的注解，这是Java安全体系结构的标准配置文件。

附录二 安全资源

此附录的内容是Java 安全实现的有关资源信息，可以帮助读者及时跟踪最新发展动向，具体包括Java 安全漏洞（bug）和其他相关信息的资源。

附录三 基于身份的密钥管理

Java 1.1中的密钥管理与我们在书中所介绍的存在很大差异。在此附录中将讨论Java 1.1中实现密钥管理的做法；在Java 2中这些类虽然还保留着，但是并不建议使用。

附录四 安全 Java 容器

在该附录中详细介绍了面向Java 1.1的安全管理器（在1.1中，还没有提供存取控制器），并介绍了如何充分利用1.1的安全模型编写应用程序。尽管此附录中的大部分技术在Java 2中都得到了升级，但也有例外，此附录中将给出相关提示。

附录五 实现 JCE 安全提供者

在书中我们介绍了如何实现标准安全提供者。JCE安全提供者的建立需要增加一些步骤，在此附录中将对此详细说明。

附录六 速查手册

此附录是本书中所讨论的类的一个简单索引。

第二版中新增的内容

因为JSSE和JAAS最近才发布，因此在本书第二版中专门针对这两个扩展包增加了相应的章节加以介绍。此外还介绍了JCE 1.2.1所补充的内容，并包括了调整后的代码实例。