ET PUBLISHING
今日電子

网络安全

- 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
電子工業出版社
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。

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

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执行环境。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 Sockers 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

第二部分　加密安全

第三部分　分布式系统安全

第四部分 附 录