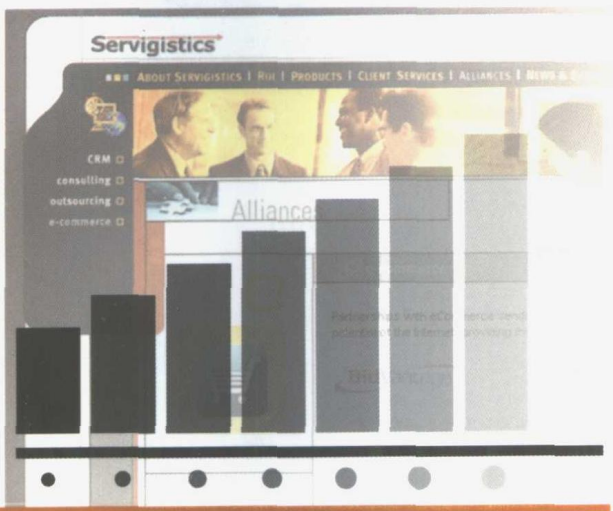
Java 编程实例系列丛书

Java安全性编程实例



徐迎晓 编著

- 全面解析Java技术
- 丰富、简洁的实例，使晦涩的概念和理论变得轻松易读
- 超凡的实战经验，帮您进入更广阔的编程空间

Jav

清华大学出版社

Java 编程实例系列丛书

Java 安全性编程实例

徐迎晓　编著

清华大学出版社
北　京

内 容 简 介

本书以大量的实例介绍了 Java 安全性编程方面的概念和技术，全书共计 9 章。

经过精心设计，每个小节的实例着重说明一个问题，又相互贯穿和联系。内容涉及 Java 加密和解密，反编译和反反编译，对类、成员变量、方法的攻击和保护，消息摘要，消息验证码，数字签名，口令保护，数字证书和证书链的生成、签发、检验和维护，SSL 和 HTTPS 客户及服务器程序、基于代码位置和签发者的授权，签名 Java Applet 以及基于身份的验证和授权(JAAS)等。

全书的实例极为精简，只保留了能够说明问题的代码，而又可真正运行，便于 Java 入门者轻松掌握安全性方面繁杂的概念。适合于初步了解 Java 语法的学习者，也适合于作安全技术的入门学习及高校 Java 教学的参考书。

图书在版编目(CIP)数据

Java 安全性编程实例/徐迎晓编著.—北京：清华大学出版社，2003
(Java 编程实例系列丛书)
ISBN 7-302-06420-2

Ⅰ.J… Ⅱ.徐… Ⅲ.JAVA 语言—程序设计 Ⅳ.TP312

中国版本图书馆 CIP 数据核字(2003)第 018513 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.tsinghua.edu.cn
策划编辑：彭 欣
责任编辑：刘 颖
印 刷 者：中国科学院印刷厂
发 行 者：新华书店总店北京发行所
开 本：787×1092 1/16 **印张**：30.5 **字数**：721 千字
版 次：2003 年 4 月第 1 版 2003 年 4 月第 1 次印刷
书 号：ISBN 7-302-06420-2/TP·4838
印 数：0001～5000
定 价：42.00 元

编委会名单

丛书序

《Java 编程实例丛书》在参与编写的作者、合作者，以及丛书编辑的共同努力下，近日即将与读者见面了，首先向付出辛勤劳动的丛书作者和编辑们致以崇高的敬意。

Java 语言是一种与平台无关的编程语言，它具有“一次编写，随处运行”的特点，所以，非常适合于分布式的网络编程。随着 Internet 网络在我国的迅速普及，参与和从事网络编程人员也在不断地增加，同时，也将有更多的网络开发者选用 Java 语言作为编程工具，而一些 C 和 C++程序员也在逐步转向应用 Java 语言编写程序，为在较短时间内学会并掌握 Java 语言的编程方法和技巧，我们从实际应用出发，编写了《Java 编程实例》丛书系列，该套丛书包括：《Java 基础编程贯通教程》、《Java Applet 编程实例》、《Java 图形与动画编程实例》、《J2EE EJB 应用编程实例》、《Java 安全性编程实例》、《Java 数据库编程实例》、《Java 网络编程实例》、《Java 服务器编程实例》等。丛书的每一个实例都是一个具体的应用，具有较强的实用性和目的性，这套丛书的实例包括了 Java 语言应用的方方面面，而且实例难易结合、应用面广，非常适合初、中、高级的学习 Java 语言编程的读者。

在这里有一点需要说明的是，如果您在阅读本套丛书之前，没有接触过 Java 语言，建议您先认真阅读一下《Java 基础编程贯通教程》这本书，该书叙述全面、重视教学方法同时将丛书实例涉及到的内容贯通起来进行讲解，不但有利于把问题说清楚，也可以减轻初学者的学习负担。从头到尾，一本书基本解决问题，读者学习之前不需要有编程基础，只要读通本书，就能立即参与编程。这也是我们之所以把《Java 基础编程贯通教程》列入该套丛书的主要原因。

如果您以前接触过 Java 语言或已经具备一定的编程基础，那么您可以直接进入实例演练的世界，相信本套丛书将会成为您学习 Java 编程的良师益友。

《Java 编程实例丛书》在编写过程中，充分体现了理论联系实际，所有参加编写的人员都是多年使用 Java 语言开发网络实际应用项目、具有丰富的实际应用经验的研究员、高级工程师、工程师以及从事 Java 教学和培训的教师等，有些参编人员已经获得了 Sun 公司的 Java 程序员的资格认证。在丛书中的多数实例都是作者从实际应用项目中提炼出来的，它们具有很强的代表性和实用性，并由浅入深地介绍给读者，通过丛书的实例能够给读者一定的启发，可以说，该系列丛书为 Java 程序员开发各种实际应用项目提供了可参考的解决方案。

《Java 编程实例丛书》的内容涉及了计算机应用的前沿技术，例如，网络应用技术、图形动画以及多媒体技术、数据库技术、大型企业级应用开发技术、网络服务器应用技术、EJB 技术、网络安全技术等，每一个实例都有明确的目标，即解决一类问题。由于 Java 代码的可移植性，读者完全可以将丛书中的实例应用到自己的项目中。

在《Java 编程实例丛书》内的每一个实例源程序代码中都添加了详细的注释，增强了程序的可读性，便于读者学习和使用。

本系列丛书体系结构分类合理、各单册层次清晰、深入浅出、通俗易懂，相信一定能够得到 Java 程序员和 Java 爱好者的欢迎。

《JAVA 编程实例丛书》编委会

2003 年 3 月

前　言

随着 Internet 的发展，安全性已经引起人们越来越大的关注。Java 自其诞生起就将安全性作为主要考虑因素之一，随着 Java 的发展，更多的安全机制被加入到 Java 中，在 Java 2 SDK 1.4 中更是集成了 JCE、JSSE 和 JAAS 等 Java 安全扩展平台。这些安全机制是开发基于企业级 Java 2 应用平台(J2EE)的安全应用程序的基础。

很多安全性方面的书籍涉及大量难以理解的理论和概念，缺乏浅显易懂的实例，使初次进入安全领域的学习者望而生畏。本书以实例为基础，从实例导入基本概念和理论，引导读者逐步进入安全领域。

本书以功能和实例为导向，每个小节列举一个实例完成一个小的功能和知识点。各个实例经过精心简化，只保留最关键部分，因此本书的程序往往数行便可实现关键功能，读者可以方便地进行扩充和加上自己的代码。

各个小节的实例像一块块积木，既有独立性又相互关联，读者可以方便地利用这一块块“积木”搭建出大型的应用。

本书共分 9 章，主要内容如下：

- 第 1 章

  解决的主要问题

  运行本书的程序需要哪些软件？

  主要内容

  介绍本书所使用的主要软件及其安装和配置。

- 第 2 章

  解决的主要问题——内容的安全性

  数据在网上传递怎样防止被黑客窃听到？

  硬盘上的文件中有敏感数据，如何防止被黑客看到？

  主要内容

  本章解决的是数据内容的安全性，介绍 Java 的加密和解密技术。学完本章可以通过 Java 编程对各种数据进行各种形式的加密。密码学也是安全机制的基础。

- 第 3 章

  解决的主要问题——和源代码相关的安全性

  编写好的程序给用户后，用户如果能反编译出源代码怎么办？

  定义类、成员变量、方法时如何防止恶意或无意的攻击？

  主要内容

  本章解决的是和源代码相关的保护，包括源代码、类、成员变量、方法的保

护。通过常用的反编译工具加强对源代码保护的认识，使用混淆器和加密等方式对源代码做出初步保护。同时演示了编写程序时如何考虑攻击者对类、成员变量、方法等方面的攻击。

- 第 4 章

解决的主要问题——确定数据的完整性和所有者

网上下载一个程序，如何确定它确实是某某公司开发的？

如何确定黑客没有将程序修改过？

某公司或人发来一个文件，后来他不承认发过这个文件怎么办？

主要内容

第 4 章起开始介绍和身份认证相关的技术。包括身份确定性、不可篡改性、不可否认性等，该章介绍的消息摘要和签名技术可解决这些问题。

- 第 5 章、第 6 章

解决的主要问题——数字化身份的凭证

实际应用中如何方便地使用摘要和签名技术？

如何确定某个签名确实是某个人或机构的？

主要内容

第 5 章和第 6 章介绍基于摘要和签名技术的数字证书。这是 Java 安全中确定身份的主要技术。其中第 5 章介绍了数字证书的创建、签发、验证和维护等，第 6 章介绍了多个证书组成的证书链(CertPath)的创建和验证。

- 第 7 章

解决的主要问题——数据安全传输，服务器和用户身份的确定

客户机和服务器之间的通信如何自动进行加密传输？

客户机和服务器之间的通信如何相互确定身份？

浏览器访问一个站点，如何确定这个站点不是黑客的服务器？

主要内容

本章介绍使用加密技术和证书机制的一个实际应用——基于 SSL 和 HTTPS 的编程。学完本章可以编写自己的 SSL 和 HTTPS 客户及服务器程序。

- 第 8 章

解决的主要问题——基于代码来源的程序的安全运行

网上下载了一个程序，运行时会不会删除本机的文件，或将某些文件泄漏给黑客？

编写了一个 Java Applet，如何使其能访问硬盘上的文件？

主要内容

本章介绍基于代码来源的程序的安全运行，可以基于运行时代码在哪个 URL、或代码是谁签名的来限制其可以访问哪些用户资源。还介绍了定义自己的权限以及签名 Java Applet。

- 第 9 章

解决的主要问题——身份验证和基于执行者身份的程序的安全运行

程序需要用户输入账号和口令到数据库登录，但以后可能需要改为智能卡验证。

程序需要访问某个用户资源，但只有用户以某些特殊身份登录时才需要该权限。

主要内容

本章介绍 Java 验证和授权服务(JAAS)，可以方便地更换验证模块，并实现基于身份的授权。

本书实例以帮助读者入门为目的，因此为了易于理解做了很多简化，如很多实例中口令以字符串保存，各个实例的异常处理都做了简化。因此，在编写实际应用系统时不可照搬。本书实例涉及的源代码可从 www.wenyuan.com.cn 网站下载。

本书的作者是 SUN 认证讲师，多年从事 Java 的培训与研究。对于本书的各种意见和建议请发送 E-mail 到 xyx@shu.edu.cn，作者提供网站 http://javabook.126.com 供读者交流。

徐迎晓

2003 年 1 月于上海大学

目　录

第1章

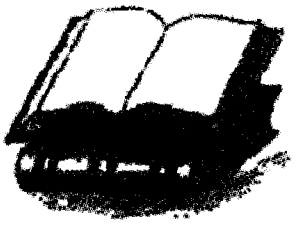
准备上手

本章要点

本章将介绍本书所使用软件的安装和设置。其中最主要的软件是J2SDK 1.4，安装好该软件后，将可以运行本书绝大部分程序。个别章节中使用的反编译器、混淆器等也在本章做了介绍。

本章主要内容

1. 安装和配置 J2SDK 1.4 环境
2. 安装反编译器
3. 安装混淆器



1.1 J2SE 的安装和设置

J2SE 的全称是 JavaTM 2 Software Development Kit，Standard Edition(Java 2 SDK，Standard Edition)。本节介绍其下载、安装、设置以及其中本书所使用的主要工具。

1.1.1 下载 J2SE

访问 http://java.sun.com，在出现的主页中显示了 Java 2 平台的 3 种不同版本：Enterprise Edition(J2EE)、Standard Edition(J2SE)和 Micro Edition(J2ME)。本节使用的是 J2SE。

单击 Standard Edition(J2SE)链接，在出现的页面中单击 J2SE Downloads 链接，进而选择版本。由于自 1.4.0 版本开始集成了各种安全机制和相关的 API，因此请选择 1.4.0 或以上的版本。本书以 1.4.0 版本为例。

单击 J2SE 1.4.0 版本的链接，在出现的下载页面(http://java.sun.com/j2se/1.4/download.html)中选择 Windows(all languages，including English)一行、SDK 一列中的 DOWNLOAD 链接，在随后出现的协议页面中单击 ACCEPT 按钮，出现最后的下载窗口，单击 Download j2sdk-1_4_0_03-windows-i586.exe，则提示保存目录并开始下载软件。该软件大小为 37,118,676 bytes。

在上述过程中同时可下载 J2SE 的文档，在文档中包含了多个教程和 API 文档。

也可在一些 FTP 搜索引擎如 http://bingle.pku.edu.cn 中输入“j2sdk-1_4”关键字搜索一些国内的下载站点。

1.1.2 安装 J2SE

J2SE 安装过程如下：

(1) 开始安装

双击下载的 J2SE 安装程序，在出现的初始安装界面中单击 Next 按钮，出现许可协议对话框，单击 Yes 按钮接受协议。

(2) 选择安装目录

接着选择安装目录。不同版本的 J2SE 默认安装目录不同，对于 j2sdk-1_4_0_03-windows-i586.exe，默认安装目录是 C:\j2sdk1.4.0_03，不妨单击 Browse 按钮，重新设置安装目录为 C:\ j2sdk1.4.0。这样，本书叙述中对不同的改进版本就可以统一使用 C:\j2sdk1.4.0 代表 J2SE 的安装目录。继续单击 Next 按钮。

(3) 选择安装的组件

在接下来的对话框中选择欲安装的组件，如图 1.1 所示，如果硬盘空间足够的话不妨安装所有组件。其中 Program Files 一项是必选的。Java Source 组件提供了组成 Java 平台的所有类的源代码。在本书有些章节中会利用部分源代码来帮助理解 Java 各种文档和教程中某些比较含糊的地方。

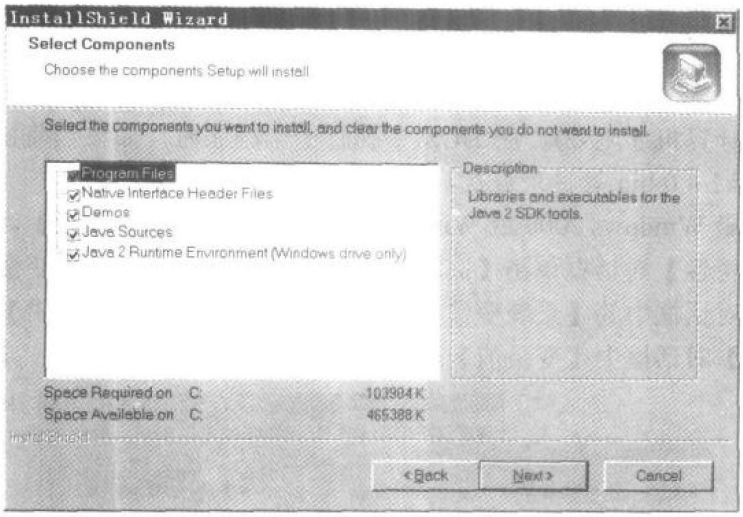


图1.1 选择所安装的组件

(4) 选择使用 Java Plug-in 的浏览器

在图 1.1 所示的对话框中单击 Next 按钮，出现图 1.2 所示的对话框。本书 8.6 节将在浏览器中使用 Java Plug-in 来运行 Java Applet。这里可选择所使用的浏览器类型。

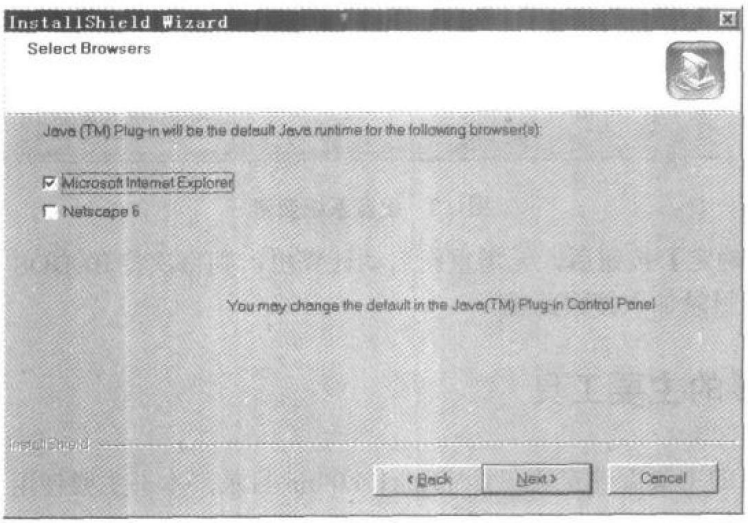


图1.2 选择使用Java Plug-in的浏览器

(5) 结束安装

继续单击图 1.2 所示对话框中的 Next 按钮将开始实际的安装过程，最后单击 Finish 按钮结束安装。

1.1.3 设置 J2SE

对 J2SE 的设置主要是设置环境变量，以方便使用安装目录下 bin 子目录中的各种工具。由于 J2SE 的编译、运行多在 DOS 环境下进行，为了能在任何目录中使用 C:\j2sdk1.4.0\bin 目录下的工具，可在 Windows 9X 操作系统 C 盘根目录的 autoexec.bat 中加入如下一行：

```
set path=C:\j2sdk1.4.0\bin;%path%
```

则以后每次打开 DOS 窗口时，会自动将 C:\j2sdk1.4.0\bin 目录加入搜索路径(第一次设置时需重新启动计算机才生效)。在 DOS 中执行一个程序时，如果当前目录没有该程序，会自动到 C:\j2sdk1.4.0\bin 等目录查找。

如果使用的是 Windows 2000 或 Windows XP，可打开【控制面板】，双击其中的【系统】，在【系统特性】对话框单击【高级】选项卡，进而单击【环境变量】按钮。在出现的【环境变量】对话框中的【系统变量】列表中选择 Path，单击【编辑】按钮，在弹出的【编辑系统变量】对话框中【变量值】最后加上“; C:\j2sdk1.4.0\bin”，如图 1.3 所示。

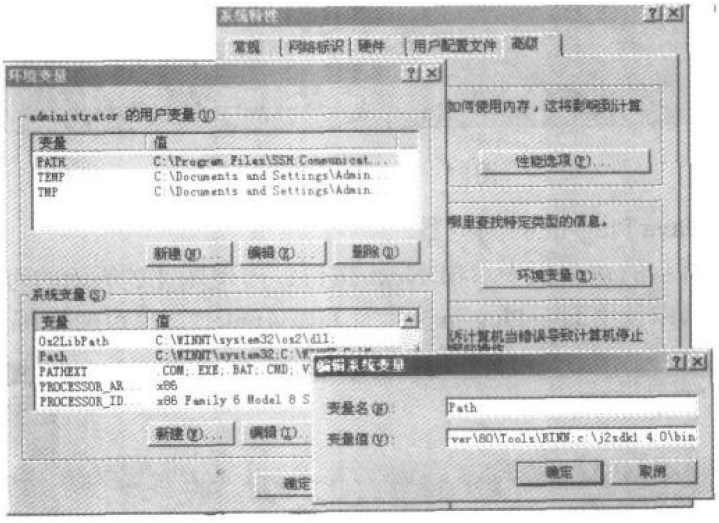


图1.3　设置系统变量

单击多次【确定】按钮后，无需重新启动计算机，则每次打开 DOS 窗口时将自动将 C:\j2sdk1.4.0\bin 目录加入搜索路径。

1.1.4　J2SE 的主要工具

Java 2 SDK 的主要工具安装在 C:\j2sdk1.4.0\bin 目录，本书主要使用了其中的 javac、java、jar、keytool、policytool、Jarsigner、HtmlConverter 和 appletviewer 等工具。这些工具主要功能如下：

1. **基本工具**

- Javac：Java 编程语言的编译器。本书各章的程序都是在 DOS 窗口中通过执行“javac 文件名”来编译 Java 程序的。文件名必须以.java 为后缀，编译以后生成.class 为后缀的字节码文件。
- Java：用于执行 Java 应用程序。本书各章的程序大都通过在 DOS 窗口输入“java 字节码文件名称”来运行 javac 编译好的程序。输入命令时，字节码文件名称的后缀不输入。
- Javadoc：用于生成 API 文档。在编写程序时将注释语句写在“/**”和“*/”之间，