Mc Graw Hill Education

“关注实际代码及设计和编码决策中的优缺点，是 Java 开发团体和安全专家的必备参考。”

——Dave Fautheree, CISSP,
系统安全分析师，西南航空

Developing Secure Applications with Java Technology

Hacking Exposed™ J2EE & Java

J2EE&Java黑客大曝光

开发安全的 Java 应用程序

【美】Art Taylor, Randy Layman,
Brian Buege 著

张伟　张华平　赵金东　译

Mc Graw Hill

清华大学出版社

J2EE & Java 黑客大曝光

开发安全的 Java 应用程序

Hacking Exposed™ J2EE&Java

Developing Secure Applications with Java Technology

【美】 Art Taylor
Randy Layman
Brian Buege 著

张伟 张华平 赵金东 译

清 华 大 学 出 版 社

北 京

Art Taylor, Randy Layman, Brian Buege
Hacking Exposed™ J2EE&Java: Developing Secure Applications With Java Technology
EISBN 0-07-222565-3

图书在版编目（CIP）数据

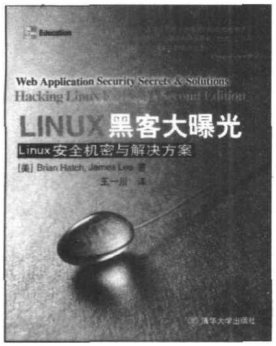
J2EE&Java 黑客大曝光：开发安全的 Java 应用程序/（美）泰勒（Taylor, A.），（美）莱曼（Layman, R.），（美）布格（Buege, B.）编著；张伟，张华平，赵金东译.
—北京：清华大学出版社，2003
书名原文：Hacking Exposed™ J2EE&Java: Developing Secure Applications with Java Technology
ISBN 7-302-07649-9

Ⅰ.J… Ⅱ.①泰… ②莱… ③布… ④张… ⑤张… ⑥赵… Ⅲ.JAVA 语言—程序设计 Ⅳ.TP312

中国版本图书馆 CIP 数据核字（2003）第 103785 号

出 版 者：清华大学出版社　　地　　址：北京清华大学学研大厦
http://www.tup.com.cn　　邮　　编：100084
社总机：010-62770175　　客户服务：010-62776969

组稿编辑：科海
文稿编辑：何武
封面设计：曹映红
版式设计：吴文娟
印 刷 者：北京科普瑞印刷有限责任公司
发 行 者：新华书店总店北京发行所
开　　本：异 16　　印张：24.75　　字数：541 千字
版　　次：2003 年 12 月第 1 版　　2003 年 12 月第 1 次印刷
书　　号：ISBN 7-302-07649-9/TP・5611
印　　数：1～5000
定　　价：43.00 元



Linux 黑客大曝光（第 2 版）

原书名：Hacking Linux Exposed，Second Edition

作者：（美）Brian Hatch，James Lee

译者：王一川

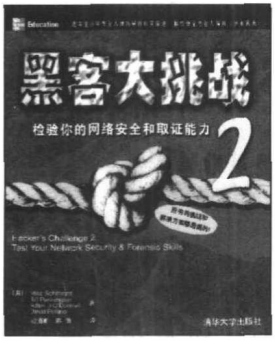
ISBN：7-302-07655-3

定价：59.00 元

Linux 操作系统正在以惊人的速度发展，用户遍及全球众多知名大学到财富 500 强企业。数以百万计的人们每天在基于 Linux 的数据库、电子商务和关键系统上工作，但却丝毫察觉不到这些系统的潜在危险。于是，一本完整的保护 Linux 安全的手册应运而生。

本书建立在《Linux 黑客大曝光》（第 1 版）的成功要素之上，保留了上一版的风格，专注于掌握入侵者收集信息、确定目标、搜寻漏洞和获得控制的方法，并给出相应的解决方案。新版除了引入新的工具和攻击方法之外，还囊括了那些众所周知或迄今仍鲜为人知的入侵案例。

本书将揭开 Linux 黑客的神秘面纱，也使攻击者试图获得系统 root 权限的各种诡计大白于天下，使广大用户可以安全地使用 Linux 的强大功能。



黑客大挑战 2

原书名：Hacker's Challenge 2

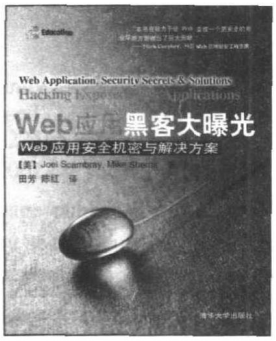
作者：（美）Mike Schiffman 等

译者：段海新，陈俏

ISBN：7-302-07207-8

定价：39.00 元

本书以一种生动惊悚的记事手法讲述了 19 个真实的网络安全入侵案例——覆盖当今世界常见的攻击类型，包括拒绝服务攻击、恶意代码、Web 应用攻击、内部攻击和外部攻击等，并涉及无线网络安全等当前热点技术。全书内容分为“挑战”和“解决方案”两部分。“挑战”详述了每一起安全事件的所有证据和取证信息（日志文件、网络拓扑图等），并提出一些问题；“解决方案”透析入侵的来龙去脉，并回应了“挑战”部分的问题，另外还提供相应的预防手段和补救措施，以降低风险并减少损失。



Web 应用黑客大曝光

原书名：Hacking Exposed Web Applications

作者：（美）Joel Scambray，Mike Shema

译者：田芳，陈红

ISBN：7-302-07486-0

定价：39.00 元

揭开黑客的秘密武器库，保护你的 Web 应用程序！

在 Internet 大众化及 Web 技术飞速演变的今天，在线安全所面临的挑战日益严峻。所幸的是，本书的作者站在技术演变的风口浪尖向我们展示了针对 Web 脆弱点的当前策略及最新见解，并且，一如既往的‘黑客大曝光’风格让人一目了然。书中揭示了入侵者收集信息、锁定目标、标识脆弱点、获取控制及掩盖踪迹的全过程。您将目睹真实世界中的黑客事件（从简单到复杂一应俱全）并学习相应的对策。配书 Web 站点 www.webhackingexposed.com 包含书中所有的代码示例。此书诚如微软安全专家 Erik Oison 所言“为 Web 架构师和操作员的必读之作。”

无线安全与保密

原书名：Wireless Security and Privacy

作者：（美）Tara M. Swaminatha，Charles R. Elden

译者：王超

ISBN：7-302-07165-9

定价：32.00 元

本书为理解现在和将来的无线安全问题建立了一个框架，并提供了在瞬息万变的市场条件下取得成功所需的特定安全战略和方法。全书围绕几个案例研究，解释建立和开发安全无线系统所需的基础知识，提出开发无线设备和应用程序时将面临的主要问题，并给出用以解决这些问题的技术和工具，演示了重要的观念、技巧、战略和模型的应用。书中还提供了一种经过验证的用于设计复杂无线风险管理解决方案的方法学，即 I-ADD 过程，该过程是一种系统化的标准方法，在无线系统的整个开发周期，用于识别目标、分析脆弱性、定义战略、设计安全。

内 容 提 要

随着 Java 应用程序的广泛应用，Java 安全问题日益错综复杂。本书作者通过来自现实世界的攻击案例，暴露黑客攻击 Java 应用程序的方法和手段，提出防御措施与方案，使您未雨绸缪，先人一步。

本书首先从 Java 及 J2EE 体系结构和基本安全机制入手，阐述 Java 认证和授权服务（JAAS）、Java 密码系统扩展（JCE）和 Java 安全套接字扩展（JSSE）等安全包，书中引用一个完整清晰的示例项目，通过研究它的不同版本，包括独立应用版本、二层应用版本、基于 Web 的版本和基于 EJB 的版本，展示 Java 及 J2EE 应用在不同环境下可能遭遇的各种安全问题，并及时提出应对策略。

本书是开发 Java 安全应用的宝典，关注的是与应用开发者息息相关的问题。本书面向熟悉 Java 语言的应用开发人员，对于网络管理员和想了解如何保持 J2EE 和 Java Web 应用安全的专业人员也不失为一本难觅的参考书。

"本书通过真实的范例很好地分析了 J2EE 的安全因素及有关解决方案。"

—John Ranta, Customer Training Instructor, Sun Services, Sun Microsystems

"本书使用一个完整清晰的示例项目，讨论了设计和编码决策的长处和弱点，注重于实际代码，为 Java 开发团体和安全专业人员提供了颇有价值的参考。"

—Dave Fautheree, CISSP, Systems Security Analyst, Southwest Airlines

"本书为不同水平的应用开发者提供了基本指南，涉及 Java、J2EE 和 Web 服务技术等的安全性。很好地讲解了常见的安全攻击及防御方法，所有示例的工作代码都基于现实生活中的案例研究。"

—Tim Seltzer, Enterprise Java Architect, Java Center, Sun Microsystems

关于作者

Brian Buege

Brian Buege 是一位具有十多年软件开发经验的信息系统专家。作为一个应用程序开发者和设计者，他的梦想是使 Java 应用安全对于每个开发者都很容易理解和实现，而不仅仅是“安全”专家才能涉足。通过 15 个软件工程项目的开发经验，他认识到，应用安全技术不但要有用、有效，还要容易实现。

在使用 Java 的 5 年中，他设计和开发了各种各样的商业系统，使用了各种技术，从金融服务系统到健康保健系统，从独立结构到 N 层结构。

除了担任财富 500 强客户的独立顾问和应用安全分析专家，Brian 还是 Sun Microsystems 授权的 Java 讲师、开发者和程序员。他在大学里教授计算机科学和数学，并在全国范围内为商业客户讲解与 Java 相关的课题。Brian 曾获得明尼苏达大学计算机科学专业的硕士学位。

——可通过 brian@hackingexposedjava.com 与 Brian Buege 取得联系。

Randy Layman

Randy Layman 是一位拥有超过 5 年开发经验的软件工程师。他曾参与设计、开发和部署关键的金融系统和 Web 发布系统等。他一直致力于开发尽可能优秀的系统，努力防卫计算机系统免受外部的攻击，同时提供高可用性且能快速响应的有效系统。Randy 获得了乔治亚技术学院计算机科学的学士学位。

——可通过 randy@hackingexposedjava.com 与 Randy Layman 取得联系。

Art Taylor

Art Taylor 在计算机工业领域工作了 17 年，并能时常回忆起当年把用 1200 波特连接的绿色屏幕字符终端作为先进技术的事。在 1996 年开始研究 Java 技术之前，他致力于数据库方面的开发，多年为 Informix 软件公司工作。

Art 写了几本关于 Java API 和技术方面的书，并为 Sun Microsystems 讲授 Java 课程。他担任过各种工程角色，包括技术设计者、项目管理者、数据库设计者等。

Art 喜欢写作，这些年出版了一些技术书籍并发表了一些文章。现在，他主要从事写作，并在 Rider 大学作为助教讲授计算机课程，也做一些咨询工作。

——可通过 taylorart@blast.net 与 Art Taylor 取得联系。

前　言

善攻者，敌不知其所守；善守者，敌不知其所攻。

—— 孙子

在 Java 短短几年的发展历程中，它从一个被硬件公司感兴趣的项目，成长为面向服务器端、中间件编程的流行语言。这个成功不是偶然的。Java 具有的很多特性，使它可以胜任从服务器到掌上电脑的各种编程任务。它是平台独立、类型安全和紧凑的语言，有一个丰富的开发库，Java 开发工具箱（JDK）和开放源码项目（像 Apache 的 Jakarta 项目）里提供了这些资源。但最重要的是，Java 语言具有较好的健壮性、一致性和可扩展的安全性，这种能力在其他语言和运行环境里非常缺乏。

Java 的安全性是开发这个语言的关键考虑。开发者知道，Java 程序将暴露给广大的未知用户，会遭遇明显的安全风险。一开始，这个语言就内置了很多安全特性，随着每个新版本的发布，这些特性会被增强和扩展。不幸的是，尽管它是内置于平台结构中的技术，仍有很多应用开发者和系统设计者忽略了 Java 和 J2EE 的安全性。在很多实例中，作者看到很多企业（和销售商）建立起自己的安全解决方案，但它们几乎完全镜像 Java 平台自身的性能——因为他们不知道已经存在于 Java 中的那些特殊安全特性。

了解可用的 Java 安全工具并一致地使用它们，是好的 Java 安全策略的基础。本书的目的是帮助读者选择恰当的安全工具，并正确地使用它们，以保护应用程序。

了解你的敌人

究竟是谁想要攻击我们的应用程序？是那些在卧室里使用高速因特网连接的 14 岁孩子么？他们都位于我们公司的防火墙之外么？有可能，但实情并非如此。目前，很多实际商业应用程序不是基于 Web 的，从公司内部网之外不能轻易访问它们，我们对于应用程序攻击者的估计与很多人通常考虑的略有不同。事实上，在组织之外，对于不基于 Web 的商业应用程序，并没有很多厉害的黑客。

尽管有很多人从外部攻击系统应用，但他们大都是业余的（在这里我们使用“业余”这个术语，是因为其中有一些人非常有技巧，但通常他们并没有因为他们的服务而获得报酬。）在很多情况下，这些系统黑客并不关注盗窃或修改信息（在公司应用程序的领域）。通常，他们感兴趣的是通过攻破系统、毁坏数据、改动公共可用信息（如公共 Web 页）或使用一个系统作为攻击另一个系统的跳板等来获得个人的满足感。

很多经验丰富的专业黑客知道全世界的政府机构数百年来就知道的事实（和其在间谍领域的所做所为）：说服具有访问权限的人为你工作比你亲自闯入来完成它要容易得多。比较过去 15 年中在美国情报活动中发生的对“不可能完成任务”的突破数量（极少），与那些在相同机构中为了较少的钱而泄漏敏感信息的员工数量，你可以领悟到这一点。相同的原理可应用在商业间谍中：当你能够花钱请在那里工作的人为你获取信息，为什么还要闯入并冒着被抓住的危险呢？最初，这个格言被用来击败物理的安全防卫，现在，同样的原理可以应用在信息系统安全防卫上。我们必须意识到，对应用程序的攻击不但会来自外部，还可能来源于组织内部。

我们通常将黑客分为 3 类：外部黑客、蓄意的内部黑客和无意的内部黑客。外部黑客包括固执的黑客和公司间谍专家（竞争者）。蓄意的内部黑客可能是伪装的、恶意的或不道德的雇员、签约人、非常有耐心地想办法渗入组织的执着的间谍专家。然后是无意的内部黑客，他们能造成许多无关痛痒的损害。这种黑客包括新手或未经培训的应用或系统用户、在按 ENTER 键之前不总是查看命令行的系统管理员以及未经恰当的回归测试就匆忙将维护版本发布出去的软件开发者。

理想情况下，应用程序可以防御所有这 3 类攻击。在目前的公司计算体系中，对不是基于 Web 的应用程序的内部攻击（偶然或蓄意的）比外部攻击更常见。

因而，除了 Web 应用章节外，本书特别关注的黑客是使用应用程序的组织成员，以及最安全的系统级措施对其都作用不大的人员（这个黑客已经获取一定程度的系统访问权限）。我们将请操作系统专家和网络安全专家帮助我们的应用程序防御外部黑客。我们不能忽视外部黑客，但是对于不是基于 Web 的应用程序，我们的重点是防范掌握系统和当前安全知识的内部成员的攻击。我们也关注掌握技术、系统或企业中所用商业软件知识的外部人员。

本书的特点

本书蕴含的哲学与市场上很多关于 Java 安全的书有着根本的不同。下面是本书的独特之处：

- ▼ **关注整体应用，而不只是一个操作系统或一项技术。**不是关注一项技术，比如 EJB，而是关注应用安全，从客户/服务器到基于 Web、从独立应用到 Web 服务，从 Java Web Start 客户端到中间件的 EJB，本书包含了广泛的 J2SE 和 J2EE 应用体系结构。我们希望这将有助于读者建立起一个综合的、集成的、可跨越体系结构和平台的应用安全策略。
- ■ **为应用开发者和系统设计者提供一个工具箱。**本书关注在 Java/J2EE 应用程序的上下文（context）中对安全技术的使用。不是向你展现相关的代码片段，而是邀请你访问我们的网站（www.hackingexposedjava.com），从这个网站可

以下载实际可用的应用示例，但要使用安装指令完成安装，它们包含了本书概述的各种技术。在很多情况下，本书使用了多种技术来实现相同的安全目标。

- **关注与应用开发者息息相关的问题，而不是针对安全理论家。**我们没有重写API规范和文档，没有讨论各种加密的细微差别，因为我们认为通过阅读随系统发布的文档，你自己可以发现这些信息。相反，我们给出了当你试图在一个实际应用中使用这些特性时，将遇到的问题和挑战。
- **能够良好实现的安全机制优于完美但未能实现的安全机制。**能够在实际中使用的安全性是最好的安全性。因而，我们介绍可被有经验的开发者容易实现的机制，而不是“接近完美”的过于复杂的机制。尽管设计了一个目前非常完善的应用安全系统，但如果因为项目管理者没有时间实现而将它砍掉（我们不止一次看到这种情况），这等于白忙一场。

谁应当阅读这本书

本书是面向熟悉Java语言及其主要概念（比如对象设计、类的继承和接口的使用等）的Java开发人员。本书也可作为网络管理员和想了解如何保持J2EE和Java Web应用安全的安全专家的参考书。

本书并不要求读者对密码学和神秘的密码数学有深刻理解。实际上，加密只是J2EE安全的一部分。流行的Java密码系统扩展（JCE）和Java安全套接字扩展（JSSE）已经使这些加密机制成为相对透明的简单处理。

对J2EE的深入理解也不是必需的。这本书并没有详细解释J2EE，它只给出了对servlet和EJB基本原理的解释。经验丰富的Java程序员能够理解和掌握这些例子。

基本的构建块：攻击和对策

秉承“黑客大曝光”系列图书的一贯风格，本书的基本构建块是在每一章中讨论的攻击和对策。并且，攻击在这里被特别强调。

这是一个攻击标志

本书中使用这个标志来强调攻击。我们的焦点是应用程序的安全性，所以本书涵盖的很多攻击与常用的攻击策略或技术有关，而不是黑客进行攻击时常用的工具。因为每个应用程序都是惟一的，所以几乎没有为入侵某一应用程序而建立特定的“工具箱”；但是建立了许多工具箱用来入侵某一操作系统的薄弱点，或者某一Web容器、应用服务器、数据库的缺陷。因为Java是平台无关的，这些工具箱或多或少可以应用到一个特定环境下的Java商业应用程序。

基于这个原因，我们的攻击不是关注系统、容器或服务器级的弱点，而是关注由应用开发者产生（和可修改）的弱点。这通常是被攻击的最薄弱部分，但是需要与传统的系统级黑客不同的技巧：应用级黑客要能像应用开发者那样思考问题。

每一种攻击也伴随着风险率，如同“黑客大曝光”系列的其他图书一样，本书也对其准确地打分。

流行度：针对运行系统的使用频率，1 为最少用，10 为广泛地使用。

容易度：执行攻击需要的技巧难度，10 为很小或没有技巧，1 为经验丰富的 Java 程序员。

影响力：成功攻击产生的毁坏影响，1 为价值不大的商业信息泄漏，10 为关键商业信息的完全损害，或应用程序可用性的丧失。

风险率：综合上面 3 个值，产生总的风险率。在有些情况下，如果我们感到某些额外因素也能够对某个特定攻击的风险产生影响，我们可以主观地调整风险率，而不是完全按照上面 3 个标准的平均值。

我们也遵循“黑客大曝光”系列图书的路线，提出对策，它们将出现在每个攻击或一系列相关攻击的后面。

这是一个对策标志

这个标志将使我们注意到这是一个关键的修补信息。因为应用安全性的很多对策需要开发和编程，所以很多对策广泛且详细地介绍了在应用程序的上下文中实现对策所需的每一个准确步骤。

其他可视的帮助信息

我们也使用了很多可视的增强标志，来强调经常被忽略的一些细节。它们是：

注意　　提示　　警告

在线资源和工具

Java 和 J2EE 应用的安全性是一个大题目。正因如此，很多信息和示例代码由于篇幅原因没有包含在本书中。

为了弥补这一点，我们建立了一个网站，用来跟踪本书中相关主题的最新信息，并提供书中非常重要的、功能完整的示例代码的下载。在此网站上，读者还可以找到关于 Java 技术的几个附录。这个站点的网址为：

```
http://www.hackingexposedjava.com
```

建议读者经常访问这个网站，以获得更新的信息，下载本书提到的代码，并获取

Java 和 J2EE 安全的有关开发信息。

另外，可以直接通过下列电子邮件地址与作者取得联系：

art@hackingexposedjava.com

brian@hackingexposedjava.com

randy@hackingexposedjava.com

快速起步引导：读者指南

在开始阅读本书之前，建议读者首先熟悉书中的案例研究。该案例第一个版本（一个简单的独立应用程序）的简要综述包含在本书第4章中。随后，在各种常用的J2EE体系结构下，案例研究被改进和重新实现。如果从开始读者就熟悉它的设计，就会更好地理解我们讨论的各种应用安全技术的应用程序上下文。例如，当我们说："……为解决这个问题，我们将在LocalPersistenceService类中加入下列几行代码……"，你会明白我们谈论的内容。

同样，我们也建议读者从网站www.hackingexposedjava.com下载一些例子的工作代码。那里大约有示例应用的20个不同版本的应用程序，每个含有不同的应用安全技术和在各种体系结构下实现的常用语句。如果你想自己实现这些策略，完整的源代码将有很大的帮助。

本书的结构

本书的划分如下所示：

- 第 1 章回顾了总的 Java 体系结构和基本的安全机制。
- 第 2 章的重点是 J2SE 1.4 中几个重要的新的安全包：Java 认证和授权服务（JAAS）、Java 密码系统扩展（JCE）和 Java 安全套接字扩展（JSSE）。
- 第 3 章集中讨论 J2EE 体系结构和安全机制。
- 第 4 章到第 6 章使用案例研究的独立应用版本，研究与任何 Java 应用相关的基本应用的安全性问题。
- 第 7 章和第 8 章使用案例研究的二层应用版本，探索了开发一个需要使用 JDBC 连接一个数据库或者使用 RMI 连接一个对象服务器的系统时通常面对的问题。
- 第 9 章和第 10 章使用基于 Web 版本的案例研究，关注部署使用 servlet 和 JSP 技术的应用程序时通常遇到的安全性问题。
- 第 11、12 章使用 Web 服务和基于 EJB 版本的案例研究，描述了应用程序中间件的安全防卫问题。

案例研究：退休应用程序，401(K)虚拟应用

Lester Goodwin，一个虚构的人物，是一个虚构公司的所有者，他计划使用Java来实现退休系统的管理。Lester要求他的退休应用管理有一些自动支持，所以他编写了一个小的应用程序来追踪客户的401K账户余额。本书中，我们将用这个程序作为案例研究。如前面提到的，本书中所有范例的完整文档代码存放在网站www.hackingexposed-java.com上。

Lester试图尽最大努力创建一个安全的应用程序，尽管他是一个Java专家，但是他对Java/J2EE的安全性支持并不是太熟悉，所以未能完全正确地使用这些特性。因而，Lester的应用程序有一点不成熟，并很容易遭受攻击。Lester非常有兴趣探索各种应用体系结构（而不注意安全问题），所以，出现了不同版本的退休账户401K应用程序，包括基于Web的、客户/服务器结构的、Java WebStart、具有servlet和JSP的J2EE Model 2，等等。为了理解Lester的应用程序，我们只需要调查简单的独立应用程序版本。当需要更细致地探索Java安全性的时候，再研究与它们相关的特定体系结构和安全性问题。

这个应用程序的独立版本可运行在一个单独的、无网络连接的计算机上。这个应用程序作为一组Java类文件分布，用户可以将它们解压到它们的Java系统类路径内的某个位置。

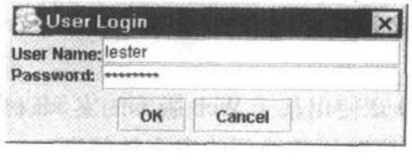
用户接口

为了运行这个应用程序，用户需要在命令行中敲入下列命令：

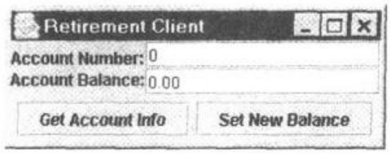
```
C:\sec\book>java book.standalone.original.ClientFrame local orig.txt
```

第一个参数是local，指明这个应用程序运行在独立模式下，使用本地系统上的数据文件。第二个参数为存储数据的文件名——本例中为orig.txt。如果它不存在，系统将使用一些示例数据自动地创建这个文件。两个示例账号将增加到这个文件中：账号12345和账号54321。

在命令行敲入这个信息后，将提供给用户一个用户登录对话框。用户输入登录信息，在本例中，用户名为lester，密码为password，如下所示。



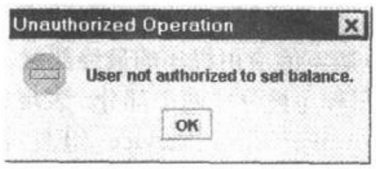
系统然后进行登录处理。在认证这个用户后（核查Lester身份的真实性），系统将显示下面非常直观的应用主界面。



为了使用这个系统，在Account Number（账号）区域输入一个账号，点击Get Account Info（获取账户信息）按钮。这个账户的余额将被显示在Account Balance（账户余额）区域。为了设定或改变一个账户的余额，用户在Account Number区域填写相关的账号，在Account Balance区域输入余额，然后点击Set New Balance（设置新余额）按钮即可。

当前，Lester执行的是程序化授权来实施商业规则，只有他可以设置任何账户的余额（尽管所有用户可察看任何账户的余额）。目前系统没有提供增加账户的功能（Lester只有2个客户）。

下面是用户brian（他的口令为password）试图设定账户12345的余额时发生的情况：



关闭这个应用主窗口，退出这个应用程序，并关闭数据文件。

这个系统的数据以文本格式存储在用户在命令行指定的文件中。下面是用户运行这个应用程序一次并对数据没做改动后，这个应用数据文件（orig.txt）的内容：

```
12345                                300.33
54321                                11111.22
```

现在我们看到了这个应用程序是如何运作的，下面了解它是如何设计和构建的。

应用程序的设计和实现

为了构建这个应用程序的安全性，我们需要理解它的设计和实现情况。

图1给出了退休应用程序实现的用例。这个应用程序允许任何用户获取任意退休账户的余额，但是只有管理员可以设定账户余额。所有用户必须作为商业用例之一（获取或设定账户余额）进行认证。

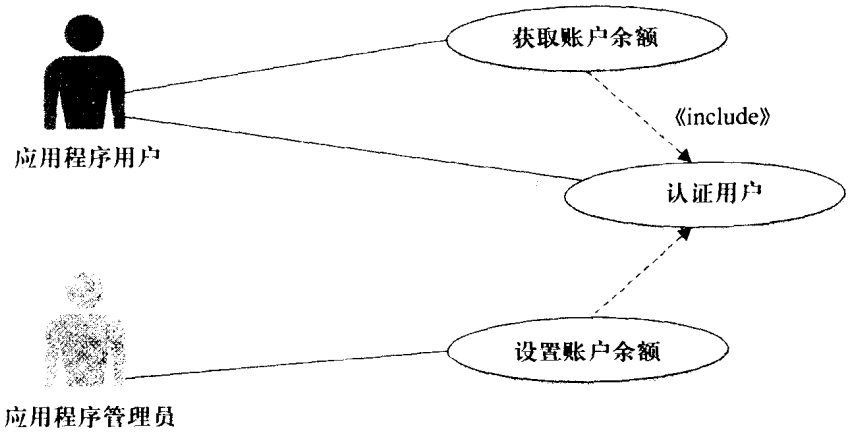


图 1　退休应用程序的用例

图2说明了这个独立版本的应用程序的最终部署。

如你所见，这个应用程序被分成两个部分：表现层（或用户接口组件）和模型（或业务和持续层，由LocalPersistenceService 组件来实现）。用户接口组件通过RetirementAccountInfo接口与模型通信。

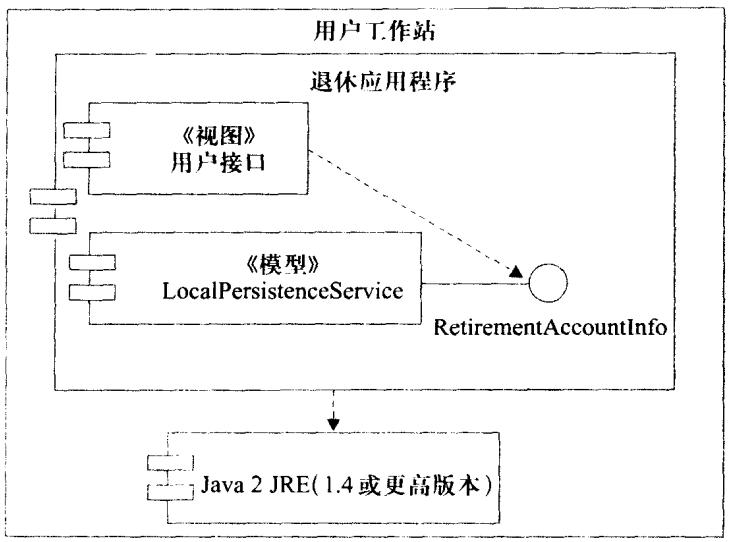


图 2　独立退休应用程序的部署

表现层

图3描述了用户接口组件中的主要类和它们之间的联系。这个应用程序的主要驱动是ClientFrame类，它含有恰当的侦听器，用来响应按钮点击，并可构建和显示一个登录对话框，来提示用户输入他们的凭证信息。

用户名和密码信息被存储在RetirementCredential对象的一个实例中，并被ClientFrame初步认证，以确信这个用户有权使用这个程序。然后，当产生一个setBalance请求的时候，将这个RetirementCredential、账户号和被请求的新余额传递到RetirementAccountInfo接口的一个实现，它将实际执行setBalance操作。

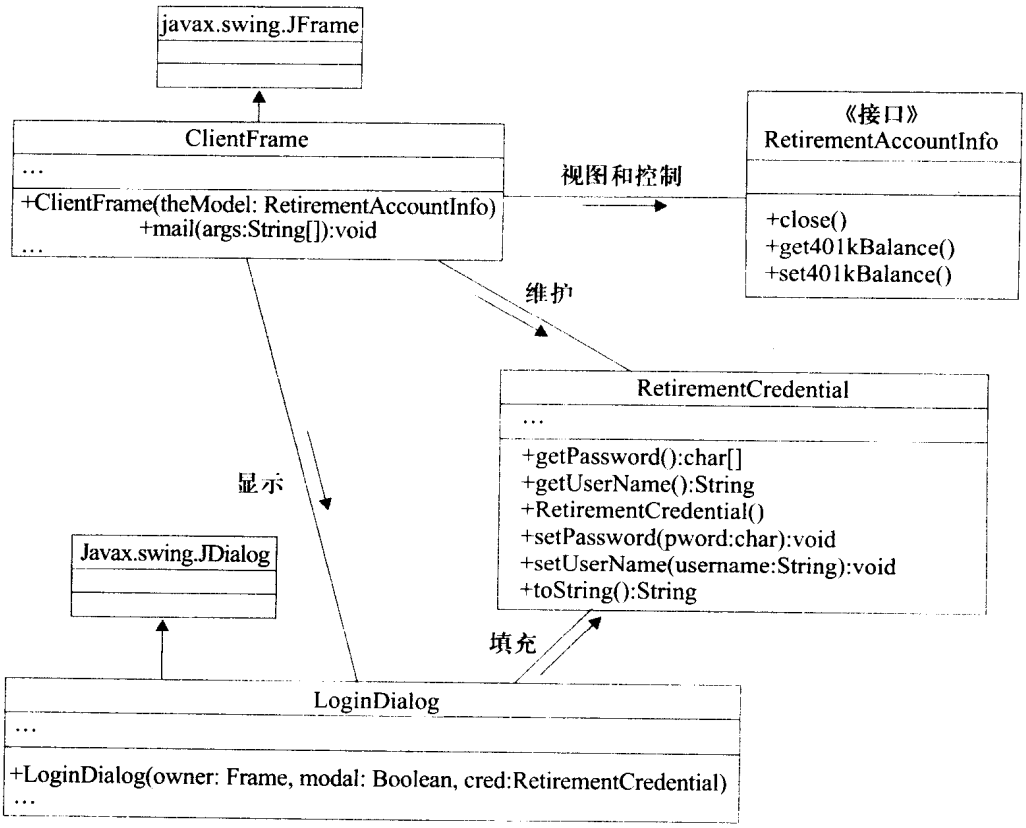


图 3　用户接口组件