网络安全系列

Windows 安全性编程

Programming Windows Security

[美] Keith Brown 著
刘涛 李一舟 译

"Keith Brown 详细地说明了 Win32 安全机制及其在 Windows 2000 和 Windows NT 上的使用，并明晰地解释了认证、授权、审核、COM+ 安全机制、登录会话等等的工作机理。"

—— George V. Reilly，微软 IIS 项目经理

Addison Wesley

中国电力出版社
www.infopower.com.cn

网络安全系列

Windows 安全性编程

Programming Windows Security

[美] Keith Brown 著
刘涛 李一舟 译

中国电力出版社

Programming Windows Security (ISBN 0-201-60442-6)
Keith Brown

图书在版编目（CIP）数据
Windows 安全性编程 /（美）布朗编著；刘涛，李一舟译. —北京：中国电力出版社，2004
（网络安全系列）
ISBN 7-5083-1825-0
Ⅰ.W... Ⅱ.①布...②刘...③李... Ⅲ.窗口软件，Windows—安全性—程序设计 Ⅳ.TP316.7
中国版本图书馆 CIP 数据核字（2003）第 110218 号

丛 书 名：网络安全系列
书　　名：Windows安全性编程
编　　著：（美）Keith Brown
翻　　译：刘涛　李一舟
责任编辑：姚贵胜
出版发行：中国电力出版社
　　地址：北京市三里河路6号　　邮政编码：100044
　　电话：（010）88515918　　传　　真：（010）88518169
印　　刷：汇鑫印务有限公司
开　　本：787×1092　1/16　　印　　张：22.5　　字　　数：508 千字
书　　号：ISBN 7-5083-1825-0
版　　次：2004 年 2 月北京第 1 版　　2004 年 2 月第 1 次印刷
定　　价：39.50 元

序

像我大多数的朋友一样，我是通过 Charles Petzold 的经典著作——《Programming Windows》而学会 Windows 编程的；然后，我转向 Jefferey Richter 的面向系统开发人员的精品《Advanced Windows NT》[1]；最后，通过学习 Kraig Brockschmidt 的《Inside OLE 2》[2]，我进入了面向对象领域。Windows NT 4.0 发布后，作为创建分布式应用的一个途径，我开始使用（并最终讲授）COM。直到这个时候，我确实一直能够忽视安全性问题，长久以来我都能抑制我过去经常有的、在需要 LPSECURITY_ATTRIBUTES 而传递 NULL 时的犯罪感。我根本就不知道我的生活即将永远地改变。

那是贝尔维尤，华盛顿的一个美丽的晴天，我正在驾车赶往我在萨罗斯（一家软件开发公司）的办公室。按计划，我将在那里第一次讲授 Essential COM（DevelopMentor 的主导 COM 课程），其中包括对相对较新的 Wndows NT 4.0 特征——DCOM 的介绍。班上所有的学生都已经在他们的电脑前面蜷缩着（这些学生都是疲倦的 Windows 程序员，他们中的一些人早就将他们计算机的机箱盖丢了）。有趣的是，学生们的机器有的同时属于多个 Windows NT 域，而有的却是与任何域无关的独立的机器，有一个学生甚至在使用 Windows 95。这是一个灾难性的配置。一切都安然无事地进行着，学生们（包括我自己）都完全沉浸在这堂课中，但是，前面所说的这种极端的配置，使那天早上的 DCOM 试验作业发生了巨大的波折。事实上，所有的学生都碰到了 E_ACCESSDENIED 和各式各样不同的错误码；当然他们都看着我，等我去解决这个问题。那天，我惨败，我不得不向自己（还有学生们）承认，我确实没有很好地掌握 Windows 安全知识来解决他们的问题，我还从来没有感觉这样差劲过。

这次心灵的“创伤”后不久，我开始致力于对 Windows 安全的深刻而实用的研究。我答应为 DevelopMentor 写一本新的关于服务和安全的教材，然后不间断地用了三个月的时间来学习和试验 Windows 安全 API。我永远也想不到，我最终会爱上“她”。从此以后，我学会了很多，我在 DCOM 邮件组里回答了数以百计的有关安全性的问题，我把“安全性是一个迷人的、亲切的课题”这样一个信息传达给了数以千计的学生、讨论会参加者和《Microsoft Systems Journal》（现在改名为《MSDN Magazine》）的读者。

作为我努力的顶点，这本书将通过给程序员提供全面的关于 Windows 安全的参考来弥补 Windows 系统编程方面的缺憾，这些参考从最基本的用户实体，到管理机构、登录会话，到自始至终关于 COM+安全的 DACL，只要你是一个 Windows 程序员，就会遇到这个敏感的难题。

作为我对分布式编程偏好产生的一个副作用，这本书有点独特：我在讨论安全性时一直想着分布式系统开发人员；事实上，这本书的原名叫《Windows NT 的分布式安全》。当然，Microsoft 重命名他们的操作系统“Windows NT 5.0”为“Windows 2000”的决定，将我这本书原来的名字扼杀在摇篮中。坦白说，《Windows NT/2000 中的分布式安全》这个名字听起

---

1 至少我认为这是当时很好的方式。

2 就像许多早期的采用者一样，我是以 Kraig 的第一版的激光打印草本开始学习的，经常因为发生在我知道和喜欢的操作系统上的事而抱着酒瓶“痛哭”。

来真的是很呆板，所以，我选择了这个新名字。

不管怎么说，如果你作为一个程序员（当然不是像我几年前一样），因为被要求在一个应用中加入有关安全的特征或是调试有关安全的问题而感到肚中空虚的话，我希望这本书能满足你的需要。

哪些 Windows？

这本书涵盖了 Windows 2000 和 Windows NT 4 中的安全编程。因此，为了不至于使读者在看到“Windows 2000/NT”或类似的累累赘赘而眼花缭乱，我简单地用 Windows 指代这两种操作系统。对于我觉得有必要区分不同系统（包括 Windows 9x）的特殊问题，我将使用它们的全名。

本书适用于哪些读者？

这本书是专门为潜心于 Windows 系统编程的专业软件开发人员写的。本书的第三部分是为这些程序员中开发分布式系统的那些人写的（尤其是使用 COM）。

本书的第一部分（开始的三章）特意没有包含任何代码，介绍了可能不仅对程序员而且对技术经理和高级 Windows 用户都有用的术语和概念，而不只是笼统地介绍。如果你是一个经理并且想更好地了解 Windows 安全，你可以从开发人员手中把这本书借过来，挑出开始的三章阅读。共享一套共同的术语将有助于你和你的开发小组一起更好地工作。

开发人员必须已经知道些什么？

我假定你对 Windows 系统编程有基本的了解；也就是说，你知道进程和线程的不同，你已经写过一个 DLL，甚至可能写过一个或两个服务。我偶然会提到诸如线程本地存储之类的特征，并且假定你知道我在说什么。如果你不确定你在这个领域的能力，我推荐你看看在这方面我最喜欢的一本书：Jeffery Richter 写的《Advanced Windows》（在写我这本书时，该书的第四版刚刚出版）[3]。

在 COM 这一章（第 9 章），我假定你对 IUnknown 很了解，假定你知道代理和存根是什么。如果你不能确定，我向你推荐我最喜欢的一本关于 COM 的书：Don Box 的《COM 本质论》。

COM 这一章中后面很多材料谈到 Windows 2000 中的 COM+特征，这些在《COM 本质论》中都没有论述（本书撰写时，《COM 本质论》只有第一版）。写这本书的时候，我最喜欢的 COM+书是 Ted Pattison 的《Programming Distributed Applications with COM and Visual Basic 6.0》[4]。Tim Ewald 的《Transactional COM+: Designing Scalable Applications》可能也是非读不可的，虽然我写这本书的时候他的书还没有出版。

尽管本书经常出现 Windows API 函数的详细说明，但是如果与正在讲述的题目无关的话，我不会总是向你详细讲解每一个参数的。我希望你能认识到本书是作为对 Windows API

3 虽然第四版题目变成了《Programming Applications for Windows》。

4 在这本书出版之际，Ted 正在为新一版继续工作，因此请你随时注意。

文档的补充来使用的，而不是 Windows API 文档的替代品。

如何使用这本书

我知道，大多数的开发人员不喜欢考虑安全问题，这通常就是为什么安全考虑后来被加入现有的产品（或者在新产品即将面市的最后一刻才被加入）的原因。我的大部分学生在了解到安全实际上是一个非常有趣的话题时都很惊讶，他们确实乐于听完 Develop Mentor 的安全课程。然而，我很清楚这是一个自我挑选的队伍；这些人选择上这门课，通常是因为不管他们喜欢不喜欢，都有一批不同的问题需要他们有能力去解决。不论你对安全性先前的偏向是什么，我把这本书设计成既环环相扣，又独立成章。

许多人可能是因为本书包含（至少本书说的是这样）对 COM 安全问题详尽的讨论而买这本书的，他们将会直接翻到关于 COM 的章节。然而，如果没有对基本原理的基本了解，你是不可能了解“COM 安全”的；而不管我如何迫切要求人们读第 4 章，还是会有一大批人没有时间去看这一章。如果你正是这些人中的一员，那么在开始深入 COM 安全的本质细节前，你一定要花时间读读本书最前面的三章（非常短的三章）。这些章节将会帮助你形成一种对 Windows 安全如何工作和为什么它会以这种方式工作的更直观的感觉。

这不是一本手册

在我最近的一本书——《Effective COM》（与 Don Box、Tim Ewald 和 Chris Sells 合著）中，我特意避免把它写成一本手册，那样将提供许多的代码，以供读者剪切粘贴来解决一套特定的问题，一套你可能碰到也可能碰不到的问题。相反，这本书将会帮助你了解事情是如何运作的。我会很喜欢看到有人写一本 Windows 安全的手册。我发现，一旦我对手中的问题有了基本的了解，一本手册通常能长期提高我的生产效率。

本书中的代码段都能正确编译。然而，虽然它们中有些可以适当地剪切粘贴到你的工程中，但是你一定要明白，它们只是为了提高你的认识而存在的，因此，必然会比你在一本手册中见到的代码要抽象点。

恶作剧者

通常，当我想简要地说明一个尝试侵入别人的系统的家伙时，我总引用“恶作剧者”（Bad Guy），不管他是要进行恶毒的破坏还是为了好玩。恶作剧者是我们想要拒之门外的人，而善意者（Good Guy）是我们想要让他们进来的人。实际上，“Bad Guys”、“Good Guys”是借用于我特别喜欢的一本关于安全的书：《Network Security: Private Commnnication in a Public Word》（Kaufman、Perlman 和 Speciner 著，1995 年出版）。

示例代码习惯约定

本书中所有的代码示例都是用 Visual C++ 6（和 Windows 2000 的平台软件开发工具）建立的。每一段代码都编译通过，所有的函数例子也都通过了测试；这些编译和测试都是在拷贝进手稿前进行的，所以，你发现的任何语法错误很可能是印刷错误。你可以从 http://www.develop.com/books/pws 下载正确的源代码段。

我是用 UNICODE 宏定义建立所有的代码的，我不想使用_TEXT 宏组织这些代码，因为本书都是关于 Windows 2000 和 Windows NT 4 编程的，而在这两种系统中 Unicode 更常用。

我用一致的命名机制来命名我自己的所有函数，这样你可以将它们与系统调用区别开来。我所有的函数（和常量）都以带有下划线前缀的小写字母开头：

```
_thisIsACallToMyFunction();
ThisIsACallToASystemFunction();
```

我想提醒你的是：有时为了简单起见，我提供的代码段会忽略错误检查，当然，除了在我想要提议某种特殊的见地或者我正在提供的函数值得直接拷贝粘贴。有很多办法进行错误检查（人们已经就此付出了巨大的努力），但是，实际上所有的错误检查机制都在某种程度上忽略了系统调用的检查，我在我的代码段中正是集中在这些调用上。

最后我想说明的是，说到写“经常正确”的C++代码，我是个真正坚持己见的人；但是，我也发现要想在书本能提供的有限空间中这么做是很不现实的（很多的 Windows 安全 API 都是因为“经常不正确”而臭名昭著）。

是的，本书没有带 CD-ROM

有人告诉我，我们生活在“信息时代”；而我个人认为，我本可以通过 Web 让你得到最新的东西，却给你一张包含过时内容的光盘，实在是很不明智。因此，请你访问 http://www.develop.com/books/pws 下载真正的、通过编译和连接的例子代码（包括书中所有的代码段，还有许多别的我时不时上传的好东西）。

勘误表

我已经不厌其烦地研究过这本书中所有的主题，但是，不管如何努力，总会不可避免地存在一些问题，请你把书中的任何错误通过我的网站（http://www.develop.com/books/pws）寄给我，我将会在线公布所有确认的小错误，并且酬谢第一个发现这个问题的人。请你经常查看我的网站以了解可能已经发现的任何问题。

本书内容

第一部分　模型

写最前面几章的目的是给你一个关于 Windows 安全体系结构的导引。这些章节被设计得尽可能的简练，这样一个投入的读者能很轻松地在一两天就看完。我的目标是介绍一些基本的术语，着重点在这些条块是如何组合的，而没有深入到细节中去。使用本书这一部分的一个比较有效的方法可能是：在深入本书后面其他的章节前先通读这几章，然后，当需要返回来了解总体结构时，再重新读这些章节。这几章没有源代码，因此，有一大部分可以撕下来交给你的经理，以帮助跨越在项目中经常有的“交流鸿沟”。

第 1 章　角色

这一章关注安全系统的参与者，介绍了用户实体、管理机构、认证、域和本地安全管理机构（LSA）。本章强调了安全问题最终归结为信任，并提供了几个例子。

第 2 章　环境

这一章集中在你的程序运行的环境，介绍了登录会话、令牌、窗口工作站和描述文件。

第 3 章　执行

这一章集中在授权和访问控制，介绍了组、别名、角色、特权、安全描述符、域访问控

制表（DACL）和系统访问控制表（SACL），还有一些访问控制策略和为你的应用程序选择合适策略的方针。本章最后讨论了 Windwows 安全方面面向会话的特性。

第二部分　机制

随后的这三章深入到第一部分介绍的各个概念的细节中。除了特殊注明，你可以以任何你喜欢的顺序读这一部分。

第 4 章　登录会话

这一章研究了登录会话和令牌的细节。如果系统开发人员对登录会话有很好的把握，设计和实现应用时就会觉得容易的多。本章既讨论了 System 登录会话，又讨论了交互式登录会话和网络登录会话，还介绍了如何调用 LogonUser 来建立新的登录会话。本章还说明了如何在运行时充分利用特权和用工作对象限制特权。

第 5 章　窗口工作站和描述文件

许多 Windows 开发人员甚至从来没有听说过窗口工作站，但是，如果你不去牢牢掌握它们的话，这些看起来模糊的实体最终将会阴魂不散地缠着你。这一章讨论了窗口工作站和桌面，讨论了用户描述文件和如何管理它们。为了尽可能多地从本章获益，请你先读一下前面讲述登录会话的权限。

第 6 章　访问控制和权限

这一章告诉你如何创建和管理安全描述符，包括访问控制表（ACL）编程和审核。Windows 2000 中的访问控制表与以前版本的操作系统相比有戏剧性的变化，本章中详细介绍了这些变化。本章还讨论了如何管理和使用私有安全描述符，用来保证应用定义的对象的安全，包括处理对象层次和 ACL 继承。

第三部分　分论

第一部分和第二部分涉及到了基本的 Windows 安全编程。第三部分建立在前面的基础上，讲述了分布式是如何渗透进入安全模型的。现在，许多公司都在开发基于 Windows 的分布式系统，他们中的大部分都依赖于 COM 或者 HTTP，所以，本书最终讨论了 COM 和 IIS 的安全性。除非有特别标注，你可以以任何顺序读这几章。

第 7 章　网络认证

通过公共线路向别人证明自己的身份，这个问题最初迷住我，并成为促成我至爱的“安全事业”的首要问题。这是一个有许多解决方案的极有魔力的问题，这一章提供了在 Windows NT 和 Windows 2000 中使用的核心网络认证协议，也就是 NTLM 和 Kerberos 的介绍。在描述和对照了这两种协议后，本章通过介绍安全支持提供者接口（SSPI）进行了总结，SSPI 对各种不同的认证协议之间的区别进行了抽象。

第 8 章　文件服务器

跨网络使用 Windows 文件系统是一种很普遍的实践，这一章将致力于探讨你在这些领域很可能碰到的安全性编程问题。本章都是关于理解 SMB（Server Message Block，服务器消息块）的安全，还有如何使之按你的意愿行事。因为命名管道是建立在文件服务器基本结构之上的，所以也把它们包括进讨论中了。

第 9 章　COM（+）

这一章利用前面章节介绍的基础，提供了扎实理解 COM（+）安全的基石，COM（+）安全是 Windows 中最易被误解和最受咒骂的特征。我将讲述 COM+安全的特征，并提供对 COM+、MTS 和基础 COM 间差异的分析。如果你已经读过了本书的第一部分和第二部分（第 4 章是第二部分中最重要的），你将从本章中获得最大的受益。我还推荐你在解决本章前读一下第 7 章。

第 10 章　Internet 消息服务器

DCOM 并不是因特网上流行使用的协议。事实上，仅仅使它通过防火墙和网络地址转换层就是一项巨大的工程。因特网需要简练，HTTP 和 SSL（安套接字协议）是最合乎要求的协议。通常，一个分布式系统是使用 DCOM 作为中间层，使用 HTTP 作为客户层的网关而建立起来的。这一章首先讲述 SSL 和基于证书的认证的基础知识，然后转而集中在使用 IIS 建立 Web 的应用时需要注意的问题，特别是当用 COM+组件联结两者时要注意的事项。如果你读过了第 9 章，本章后面的部分将更有意义。

附录　告别语

我已经把一些编写设置程序（如何安装用户和组账户、配置权限、配置诸如 COM 口令的个人秘密）的小技巧放在一起；里面还有众所周知的 SID 列表，你可以用程序生成它，因为有一个简单的类可以很容易地做这件事情。我还在书中对 Windows 2000 中三种不同的组范围（全域、广域和本地域）进行了讨论；最后，我在书中包括了所有在 Windows 中定义了的权限列表，并在里面就其到底是如何工作加进了我能力所至的尽可能多的见解（它们的文档通常太含糊，没有什么用）。

术语表

重要术语在术语表中简要列出。希望这一部分能对你有所帮助。

参考书目

我所提及的任何书籍和杂志都能在参考书目中找到。

本书中没有什么？

活动目录

我用了合适的篇幅谈活动目录服务接口（ADSI），正好使你能开始安装用户和组账户。关于 Windows 目录编程，可以写一本完整的书，本书不是那样的一本书。

公钥结构

虽然我讨论了 SSL 认证和验证工作原理，但是，任何关于建立一个公钥结构需要些什么这样的细节，都不在本书的讨论范围之内。我在参考书目中为感兴趣的读者提供了几本这方面的书。

致谢

首先，我想要感谢我的妻子和孩子们，她们为这本书的出版作出了巨大的牺牲，在这个项目的最后四个月，我几乎没有见过她们。感谢 Kathy、Colin、Nathan 和 Aidan，我真的好想念你们。

我想要感谢 DevelopMentor 的 Don Box 和 Mike Abercrombie，你们为我的研究和发展提供了无与伦比的环境，当我“盘踞”下来完成这本书时，是你们悉心照顾我的家人。我与你们一起进行了万分有趣的工作，我期望我们以后会有更多的合作。

感谢 Bruce Schneier 写了关于密码系统的如此易读的一本好书，我是真的被它迷住了。读《Applied Cryptography》是我人生中的一个转折点，因为我从中发现安全实在是一个太迷人的游戏了。

感谢我过去几年安全课的所有学生们，你们听完了这一个不断发展的故事，并在其中加入了你们独特的想法。没有你们，这个故事将不会如此动人。

感谢所有在这个项目中提供给我反馈的评论家们：Saji Abraham、Richard Ward、Michael Howard、Bob Beauchemin、Lan Griffiths、George Reilly、Michael Nelson、Steve Rodgers、Tomas Deml、Henk de Koning 和 Jefferey Richter。

感谢 Addison Wesley 的职工们：Kristin Erickson 是一个很好的倡议者和朋友，Jacquelyn Doucette 的努力推动使书能按期出版，J. Carter Shanklin 首先把我带进了这个项目。

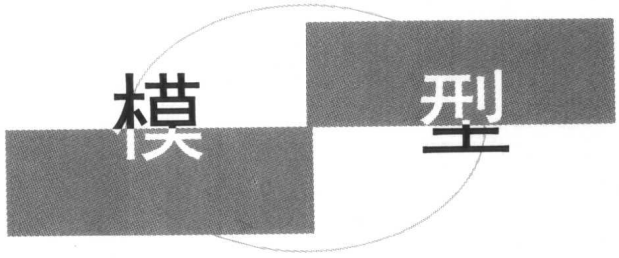
感谢我的审稿人 Cindy Kogut，他的审稿能力不断地使我惊讶：他总能在我的作品中用红笔钩出许多地方让我去考虑。Cindy 在这两年来还以各种方式使本书内容保持很好的连贯性。

最后，感谢 Alice 和 Bob。

目　录

第三部分 分 论

第一部分



第 1 章

角　　色

作为一个开发者，对我所喜爱的技术的任何本质细节我一直很感兴趣。然而，谈论一个对一些人而言十分陌生的话题，并非一个很好的想法。这一章以简单的导言部分开始，介绍一些基本的术语和机制。它拼出一幅巨大的图画，当你陷入随后技术细节的困惑时，你可以返回来阅读。本章为你提供了刚好足够的细节使你想不停地读下去，但是如果你渴望继续钻研，可以循着介绍找到后面章节，并以自己的速度来阅读。但是，不论下一步你选择读什么，都必须从本章开始，即使是有经验的 Windows 开发者也不例外。

1.1 用户实体

有一个安全系统的主要好处之一就是它也许会准许或拒绝某一实体（个人或其他的实体，如计算机或服务机构）的访问。从安全性来说，我们能安全地识别每一个实体，该实体都被认为是一个“用户实体”（principal），每个用户实体都有一个惟一的名字和以某种方式来向系统中其他的用户实体证实自己的身份。用户实体用来向其他的用户实体证明自己身份的机制被称为认证（authentication）。

一旦你在系统中识别了一些用户实体，就可以控制每个用户实体可以使用哪些资源，以及如何用，也可以在运行时刻稽核资源的使用情况，以帮助完善安全策略和侦察侵入企图。没有用户实体的概念，没有允许用户实体证明其身份的机制，大多数你能使用的安全策略将是非常有限的或者是无意义的。

在像 Windows 这样的通用操作系统中，每一个用户实体都由一个人类能识别的名字和一个机器可处理的标识符来标志。前者使人对计算机系统的使用和管理成为可能；而后者在运行时使执行有良好的效率。事实上，如果系统所选的机器可处理的标识符在位置和时间上有充分的差异，将有可能在同一个工作环境中引入两个完全不同的系统（例如，通过网络将它们联接起来，允许一个系统中的用户实体访问另一个系统中的资源），而且二者不会互相产生太多的影响[1]。这对于可扩展性有重要作用，因为网络总是开始时很小而随着机构的增长而增长。

关于用户实体的信息存储在安全数据库中（这点将在本章后面讨论）。数据库的每一个入口（entry）就是所说的账户（account），而每一个账户代表一个用户实体[2]。必须清楚了解

1　一个更加具体的例子可能是：使用一个信任关系来连接两个不同的域，这样一个域中的用户实体可以访问另一个域中的资源。我将在本章后面讨论域和信任。

2　虽然还没有讨论“组”，但每一个组也由安全数据库中的一项代表（你可能已经听过组账户这个词）。组和用户实体是很不一样的；我们可以认证用户实体，但是不能认证组。组将在第 3 章进行讨论。