Windows NT 安全技巧

〔美〕 Nevin Lambert 著
李冬 吴昊 鲍敏 译

浙江科学技术出版社
ZD PRESS

Windows NT 安全技巧

Windows NT 安全技巧

[美] Nevin Lambert 著
李冬 吴昊 鲍敏 译

浙江科学技术出版社

浙江省版权局著作权合同登记号　图字：11-1997-44 号

书　名	Windows NT 安全技巧
著　者	[美]Nevin Lambert
译　者	李 冬　吴 昊　鲍 敏
出　版	浙 江 科 学 技 术 出 版 社
印　刷	杭州长命印刷厂
发　行	浙江省新华书店
制　作	浙江科学技术出版社计算机图书工作室
读者热线	0571-5157523
电子信箱	hzzjkj@mail.hz.zj.cn
开　本	787x1092 1/16
印　张	15.25
字　数	357 000
版　次	1999 年 2 月第一版
印　次	1999 年 2 月第一次印刷
书　号	ISBN 7-5341-1231-1/TP·79
定　价	27.00 元
责任编辑	熊盛新
封面设计	孙　菁

JS300/22

内 容 提 要

越来越多的企业 Intranet 正在使用 Windows NT。通过对本书的学习，你将了解 NT 的安全保护能力，以及 NT 如何将它们应用于你的操作系统，使它的安全达到最优化。本书全面而详细地介绍了 NT 操作系统的安全性和安全技术，这样，你就能集中解决 NT 网络中的安全问题，而不必为了具体的某个问题临时抱佛脚。

本书的主要内容包括：

- 配置帐户属性，控制他们对资源的访问。
- 远程访问安全管理和一些协议。
- 通过设置权限和 NT 的利用容错能力，保护 NTFS 文件系统。
- 访问对象的安全，包括如何对它们进行选择性访问控制。
- 如何决定审核对象以及如何根据审核结果进行处理。
- 集成 BackOffice 套件安全性、Microsoft Exchange 安全性和操作系统中的 Windows NT 服务器目录服务。
- 加密技术和数字签名的使用，使它只能被经验证和鉴定的用户阅读。

作 者 序

首先，感谢所有本书的读者。我们希望这是一本有价值的指南图书，指导您理解和执行 Windows NT 的安全性。

虽然 Windows NT 面世已经有许多年，但面向管理员专门介绍 Windows NT 安全性的书并不多。Windows NT 的使用越来越广泛，Windows NT 工作站也已经成为了一种可行的桌面操作系统。

如果您对本书有什么意见或建议，可按以下地址发送邮件：

NevinL@pacts.com

ManishP@pacts.com

PADTS, 5515N. 7th St., Ste. 5-441, Phoenix, AZ 85014

1. 谁是本书的读者

本书适合哪些读者呢？

- 刚刚成为网络（任何规模）管理员的人员。
- 刚刚成为 Windows NT 管理员的人员（本书是 NT 初学者的必读之物）。
- 对其他操作系统有经验的网络管理员。
- 有经验的 Windows NT 管理员，但他可能没有安全方面的经验或经验不足。
- 有经验的管理员，同时熟悉 Windows NT 安全性，但没有使用过“审核”。
- 每个想进一步学习审核的人。
- 具有 Windows NT 4.0 初级管理员知识，但还想学习更多关于其安全性的人。

上述人员都能从本书得到有用的信息，以进一步研究 Windows NT 的安全性。

2. 什么是安全性

首先，我们定义了“安全”这个概念。当事物呈现为它们应有的面貌时，你是否觉得一点都没有问题？那么，有人走近你的汽车，汽车发出警报声的时候呢？或者，有一个强壮的人时刻跟在你的后面，你会不会觉得不安全？所以我们说，“安全”是个主观的概念。

对于计算机安全，有些人可能会说，对计算机的管理操作在很大程度上影响了它的安全性，但这并不是全部。

本书所说的“安全”，是指防止潜在的不安全因素，防止非法的入侵者，包括直接的

在线行为和来自破坏性程序的入侵。

什么是“诚实的错误”？可能就是那种由于粗心大意而导致的错误。对合法用户无意或有意超越自己的权限这样的行为，NT 安全机制也提供了有效的防范措施。

3. 关于 Windows NT 安全性的一些概念

下面要介绍的是有关 Windows NT 安全性的一些概念，它们将出现在本书的各个部分。

验　证

计算机是为我们服务的，实际上，是我们在移动和创建信息，所以，我们要保护自己的安全。

最早的计算机安全规则是定义谁要求使用系统，而这正是他为什么调用验证的原因。通常，验证就是在你使用系统之前，它要求你出示用户名和密码（称为“登录”）。安全控制是基于“只有你一个人知道自己的密码”这个假设的基础之上的，因此，如果你出示了正确的密码，计算机就推断你是合法的用户，并对你进行确认。登录以后，根据安全系统的要求，Windows NT 通过你的登录名或帐号监视着你在系统上的一举一动。当你结束工作，注销登录后，任何其他用户都不能用你的帐号使用该计算机。

通过你提供的信息，系统定义了你的帐号，包括用户名和密码。这个安全帐号还包括系统赋予你的一些特殊权限。

攻击性软件和病毒

对于病毒，你一定要小心对付。许多病毒表面上看起来和其他应用程序没什么两样（屏幕保护程序看起来很“酷”，但它将渗入你的系统，并破坏数据）。通过本书的学习，你将了解如何使用安全控制，以尽量减小和避免由于病毒造成的损害。

受托/安全路径

还有一件具有潜在危险性的事是一些带有恶意的程序，如特洛伊木马程序，它们会伪装成合法程序的样子，骗你向它输入密码等敏感资料。委托路径就是使你免受这些程序破坏的传统方法。

“委托路径”就像“安全路径”，因为它是一个特殊的窗口，名为“Windows NT 安全”。你可按下组合键 Alt+Ctrl+Delete 调用委托路径，这时，Windows NT 就能确保它的窗口是合法窗口，你可以安全地输入任何信息。如果你要进行一些可能带来安全隐患的操作，如登录、更改密码，你最好使用委托路径。

除非你按下组合键 Alt+Ctrl+Delete，否则，Windows NT 安全窗口（委托路径）不会显示。但作为管理员，你应告诫用户，在按下上述组合键之前，千万不要在看起来像委托路径窗口的窗口中输入敏感信息，也不要用其他方法执行委托路径的功能，如更改密码。

网络环境和 Internet

“网络安全”有两种。第一种是由一台计算机执行的简单的安全，它必须由网络中紧密连接的计算机协调工作。它的重要特征是安全信息集中，且用户身份控制着网络中所有机器的用户的行为。Windows NT 允许网络中的计算机协调工作的基础是“域”。

第二种网络安全是保护在计算机系统之间传输的数据的安全以及保证远程通信的安全。实现上述目的的唯一方法是各种加密技术，它将给数据进行编码，这样，非法入侵者就无法偷看或篡改数据了。Internet 的发展使加密技术更为完善和重要，而 Windows NT 充分利用和发展了这项技术。

目 录

第 1 章　Windows NT 和网络安全性

今天，计算机网络已经成为人们生活、工作不可缺少的一部分。来自各种机构的无数用户都通过联网的计算机共享和访问信息与资源。而这些系统中存储的通常是机密文件或经过特殊认证后才允许使用的资料。因此，对于一个机构而言，不管是从安全性还是从有利于竞争的角度出发，如果它的网络系统具备保护信息资源（如防止未经许可的非法访问）和有效监控已认证访问的能力，这将是非常重要的。

网络安全性由对计算机网络系统的所有组成部分（包括硬件、软件和所存储的数据）的全方位保护构成，包括对破坏、窃贼及非法访问的保护措施。事实上，制定经仔细推敲并可切实实施的系统策略，加上小心谨慎的审核过程，做到这些，就能使对系统资源的合法访问变得很简单，而非法访问则变得几乎不可能。

防止丢失和暴露机密、敏感的数据是所有机构最重视的事情之一。无论大公司、SOHO（small office/home office，小型办公室或家庭办公室）还是银行、国家政府机关，主管人员都希望他们的重要数据不受恶意攻击、非法访问和由于用户失误而造成破坏。如果他们使用了 Windows NT 工作站或服务器，这些是完全可以现实的。

Windows NT 提供了全面的安全选项，且不论系统管理员还是最终用户，都非常容易做到：一个基于口令的简单的登录过程，就能使用户获得对已授权资源的访问权。当然，用户们并不知道系统级的加密过程有多么复杂，对他们而言，只是登录而已。

本章将分低级、中级和高级这三种安全类别讨论 Windows NT 安全性的基本组成部分，同时介绍美国政府对安全性的评价标准的背景材料。

1.1　对访问、操作和审核的控制

Microsoft 公司在最初开始设计 Windows NT 的时候，就把安全性作为一项重要的特性考虑了，且这项特性至始至终贯穿于整个操作系统之中。利用 Windows NT 的这种特性和其他工具软件相结合，建立符合个人需要的安全配置是非常容易的。Windows NT 的安全性模型包括以下三个部分：

- 对象（如文件和打印机）的访问控制。
- 用户级的对象操作控制（如读或写操作）。
- 指定事件的审核。

对象访问控制是 Windows NT 安全性模型的关键。该模型对所有对象提供了所有用户和组帐号的安全性信息。访问级别由所制定的权限控制。对象的所有者或经认可的使用者，可以自由改变其他用户对该对象所拥有的权限和使用情况。因此，你可允许或禁止一个用户对任意资源的访问。作为管理员，你可以赋予任何用户或组帐号对某一对象的访问权限。