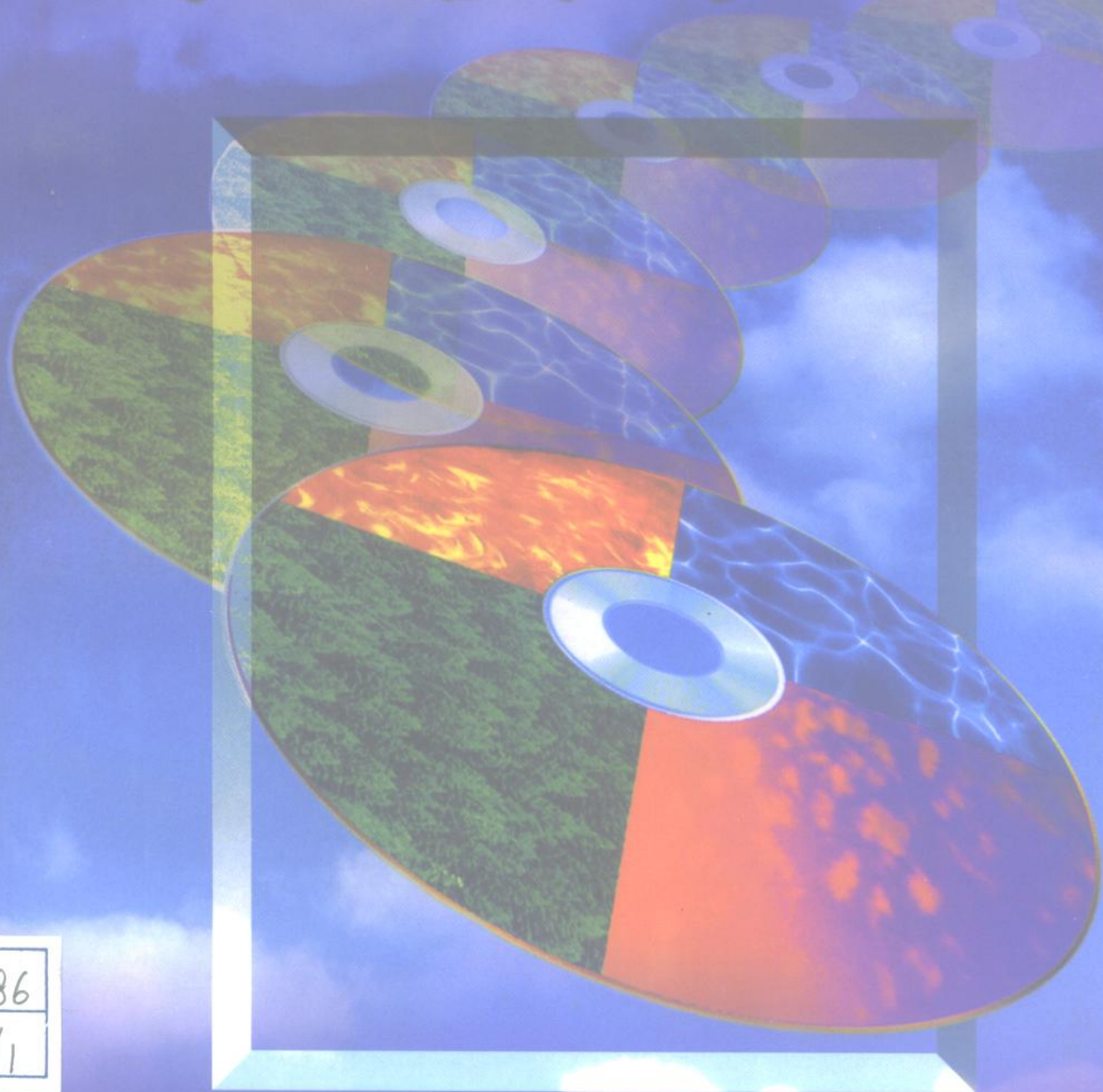


Windows NT
安全技巧

Windows NT

安全技巧

[美] Nevin Lambert 著
李冬 吴昊 鲍敏 译



浙江科

31686

31/1

社



浙江科学技术出版社

ZD
PRESS

Windows NT 安全技巧

^{N.}
[美] Nevin Lambert 著
李冬 吴昊 鲍敏 译

浙江科学技术出版社

Jim Sterne:What Make People Click:Advertising on the Web
Authorized translation from the English language edition published by
ZD Press Copyright©1997 by ZD Press
All rights reserved. For Sale in Mainland China Only

本书中文简体字版由浙江科学技术出版社和美国西蒙与舒斯特国际出版公司
合作出版, 未经出版者书面许可, 本书任何部分均不得以任何方式复制或抄袭。
本书封面贴有西蒙与舒斯特防伪标签, 无标签者不得销售。

版权所有, 翻印必究。

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	787×1092 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。
- 有经验的管理人员，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，也不要使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	1
1.1 对访问、操作和审核的控制	1
1.2 安全级别	2
1.2.1 你的网络需要多大安全性	2
1.2.2 低级安全性	3
1.2.3 中级安全性	3
1.2.4 高级安全性	5
1.3 C2 级系统安全性标准	6
1.3.1 橘皮书标准	6
1.3.2 Windows NT 是否符合 C2 级系统安全性标准	7
1.3.3 Windows NT 服务器 C2 级系统安全性标准的实现	7
1.4 小 结	7
第 2 章 操作系统与 NT	8
2.1 回 顾	8
2.2 Windows NT 的诞生	9
2.3 Windows NT 和对象	9
2.4 Windows NT 的结构	10
2.4.1 用户模式	11
2.4.2 内核模式	11
2.5 工作组和域	13
2.5.1 工作组（独立管理）	14
2.5.2 域（集中管理）	14
2.5.3 委 托	14
2.6 Windows NT 的域模式	15
2.6.1 单域	15
2.6.2 主控域	15
2.6.3 多主控域	16
2.6.4 完全委托域	16
2.7 域与安全性	16
2.8 小 结	16
第 3 章 用户与组的管理	17
3.1 域用户管理器	17
3.2 用户和用户帐号	17

3.2.1 用户和用户帐号的概念	17
3.2.2 用户权限	18
3.3 组和组帐号	20
3.3.1 本地组	20
3.3.2 全局组	21
3.4 用户帐号属性	23
3.4.1 “用户属性”对话框	23
3.4.2 复制用户帐号	26
3.4.3 重命名用户帐号	26
3.4.4 复制组帐号	26
3.4.5 特殊/系统组	26
3.5 用户与组的创建	27
3.5.1 创建用户帐号	27
3.5.2 创建全局组	28
3.5.3 创建本地组	29
3.5.4 复制用户帐号	30
3.5.5 复制组	32
3.6 发展组的策略	32
3.7 小 结	33
第4章 文件系统的安全性	34
4.1 Microsoft 的文件系统	34
4.1.1 高级文件系统的安全需要	34
4.1.2 分 区	35
4.1.3 NT 支持的文件系统	35
4.1.4 权限的类型	36
4.2 保护数据的完整性	37
4.2.1 事务日志	37
4.2.2 扇区冗余	37
4.2.3 簇的重定向	38
4.3 容 错	38
4.3.1 磁盘镜像 (RAID 1)	39
4.3.2 带奇偶校验的磁盘带区 (RAID 5)	39
4.4 容错的执行	40
4.4.1 磁盘镜像的执行过程	40
4.4.2 配置带奇偶校验的带区	41
4.5 紧急启动盘	45
4.5.1 编辑 Boot.ini 文件	45
4.5.2 启动盘的制作	46
4.6 小 结	46

第 5 章 NT 安全子系统	47
5.1 NT 4.0 的安全模式	47
5.2 NT 的登录过程	48
5.2.1 组合键 Ctrl+Alt+Del 的作用	48
5.2.2 物理登录	49
5.2.3 身份识别包	49
5.2.4 本地识别与远程识别	50
5.2.5 安全帐号管理器 (SAM)	51
5.2.6 移 交	51
5.2.7 访问标识的生成	52
5.2.8 主 题	52
5.2.9 桌 面	53
5.3 连接网络资源	53
5.3.1 连接到服务器	53
5.3.2 远程身份识别	53
5.3.3 传送身份识别信息	54
5.4 关于委托	55
5.5 小 结	55
第 6 章 本地资源的安全性	57
6.1 Windows NT 中对象的安全	57
6.2 SID 的定义与格式	58
6.2.1 SID 的创建	58
6.2.2 大家熟悉的 SID	59
6.3 选择性访问控制	59
6.3.1 访问控制列表 (ACL)	60
6.3.2 ACL 是如何工作的	62
6.4 权 限	63
6.5 NT 安全进程	64
6.5.1 对象管理器	65
6.5.2 进程管理器	65
6.5.3 对象所有权	66
6.6 管理本地资源的工具	66
6.6.1 Windows NT 资源管理器	66
6.6.2 CACLS	66
6.6.3 文件管理器	67
6.7 创建和管理文件夹与子文件夹	67
6.7.1 创建文件夹	67
6.7.2 获得文件夹所有权	68
6.8 小 结	72

第7章 网络和网络安全性	73
7.1 Windows NT 网络结构	73
7.1.1 ISO/OSI 模式	73
7.1.2 OSI 与 NT 层模式的比较	74
7.1.3 网络驱动程序接口规范 (NDIS)	75
7.1.4 传送驱动程序接口 (TDI)	75
7.2 协 议	76
7.2.1 NetBEUI	76
7.2.2 NWLink	77
7.2.3 TCP/IP	77
7.3 TCP/IP 与 NT	78
7.3.1 地 址	78
7.3.2 子网屏蔽	79
7.3.3 TCP/IP 安全	80
7.3.4 TCP/IP 的发展趋势	81
7.3.5 绑 定	82
7.3.6 注册表参数	82
7.4 网络安全	83
7.4.1 网络安全的两种类型	83
7.4.2 创建共享	84
7.5 Windows NT 如何处理网络安全问题	92
7.5.1 分配权限	93
7.5.2 远程用户的 RAS 安全机制	93
7.5.3 Internet 服务的安全性	94
7.5.4 管理共享	94
7.6 小 结	96
第8章 远程访问服务 (RAS)	97
8.1 RAS 的配置	97
8.2 远程访问客户机	98
8.2.1 Windows NT 3.5、3.51 和 Windows 95 客户机	98
8.2.2 Windows NT 3.1 客户机	99
8.2.3 工作组用 Windows、MS-DOS 和 LAN 管理器客户机	99
8.2.4 PPP 客户机	99
8.3 网络服务器	99
8.4 LAN 协议	99
8.4.1 TCP/IP 与 RAS	100
8.4.2 IPX 与 RAS	100
8.4.3 NetBEUI 与 RAS	101
8.5 RAS 服务器	101

8.6 远程访问协议	102
8.6.1 串行线路 Internet 协议	102
8.6.2 点对点协议	103
8.6.3 PPP 多连接协议	104
8.6.4 点对点通道协议	105
8.6.5 PPTP 过滤	107
8.6.6 Microsoft RAS 协议	108
8.7 广域网 (WAN) 连接	108
8.7.1 Modem 池访问	108
8.7.2 通过拨号网络访问	109
8.7.3 使用电话簿条目	110
8.7.4 ISDN 访问	110
8.7.5 X.25 访问	110
8.7.6 无 Modem RS-232C 连接	110
8.7.7 电话 API (TAPI) 连接	111
8.8 远程访问客户机的安全机制	111
8.8.1 审 核	112
8.8.2 集成域安全	112
8.8.3 加密验证和登录进程	112
8.8.4 RAS 安全	113
8.8.5 如何在连接中安全地工作	115
8.8.6 中间媒介安全主机	115
8.9 小 结	116
第 9 章 打印服务与安全性	117
9.1 打印进程	117
9.1.1 打印服务器	118
9.1.2 打印机的创建与连接	118
9.1.3 双向打印	118
9.1.4 打印作业的传送	118
9.1.5 获得打印机所有权	119
9.1.6 暂停、恢复、清除和重定向	119
9.2 打印操作的安全性设置	119
9.2.1 属性设置	119
9.2.2 设置使用权限	119
9.2.3 打印作业控制	120
9.2.4 后台打印	121
9.3 连接和创建打印机	123
9.3.1 连接打印机	123
9.3.2 连接到打印机服务器	125

9.3.3 创建打印机	125
9.3.4 打印机属性与权限	128
9.3.5 打印机重定向	131
9.4 小 结	132
第 10 章 NT 注册表	133
10.1 Windows NT 注册表	133
10.1.1 层次结构	133
10.1.2 单元与文件	134
10.1.3 注册表项的值项	134
10.1.4 Windows NT 使用的注册表	135
10.2 使用注册表编辑器	137
10.2.1 浏览注册表	138
10.2.2 其他注册表工具	139
10.3 NT 注册表文件	141
10.3.1 初始化 (.INI) 文件	141
10.3.2 MS-DOS 中的配置文件	144
10.4 注册表的安全	145
10.4.1 预防措施	145
10.4.2 注册表审核	145
10.5 备份注册表	145
10.5.1 Windows NT 备份 (NTBACKUP.EXE)	146
10.5.2 紧急修复磁盘 (RDISK.EXE)	146
10.5.3 注册表备份 (REGBACK.EXE)	146
10.5.4 使用替代操作系统	146
10.5.5 注册表编辑器 (REGEDT32.EXE)	147
10.5.6 从备份中还原注册表	147
10.6 修改注册表	147
10.6.1 注册表的访问控制	147
10.6.2 在登录前显示一个正式通告	148
10.7 注册表的最高级保护	149
10.7.1 限制远程访问	149
10.7.2 保护注册表	149
10.7.3 调度服务 (AT 命令)	150
10.7.4 隐藏最后用户名	150
10.7.5 只允许已登录用户关闭计算机	150
10.7.6 控制访问可移动媒介	151
10.8 小 结	151
第 11 章 用户配置文件和系统策略	152
11.1 配置文件的类型	152

11.1.1 本地机配置文件	155
11.1.2 服务器配置文件	155
11.2 系统策略	157
11.2.1 系统策略模板	158
11.2.2 系统策略文件	159
11.2.3 系统策略的工作原理	160
11.2.4 系统策略的缺陷	161
11.2.5 修改策略设置	161
11.3 配置文件与系统策略的创建	165
11.3.1 创建服务器用户配置文件	165
11.3.2 查看或添加策略模板	165
11.3.3 创建系统策略	165
11.4 小 结	166
第 12 章 审核与日志	167
12.1 审核的对象	167
12.2 审核的内容	167
12.3 创建审核规则	168
12.4 事件查看器安全日志	169
12.5 事 件	170
12.5.1 登录及注销	170
12.5.2 文件及对象访问事件	175
12.5.3 用户权限使用事件	180
12.5.4 用户及组管理事件	181
12.5.5 更改安全性规则	182
12.5.6 重新启动、关机及系统事件	183
12.5.7 进程追踪事件	183
12.6 小 结	184
第 13 章 Internet 安全基础	185
13.1 Windows NT Internet 服务	185
13.1.1 Internet Information Server (IIS) 与 Peer Web Server	185
13.1.2 IIS 支持的服务	186
13.2 维护 Internet 服务的安全性	186
13.3 WWW 的安全性	186
13.3.1 服务属性	187
13.3.2 目录属性	188
13.3.3 记录属性	189
13.3.4 高级属性	189
13.3.5 网络监视器的安全问题	190
13.4 小 结	190

第 14 章 BackOffice 安全集成	191
14.1 服务的安全性	191
14.2 系统管理服务	193
14.2.1 SMS 的安全性	193
14.2.2 善于解决问题的 SMS	194
14.3 SQL Server	195
14.3.1 SQL Server 的标准安全模式	195
14.3.2 SQL Server 中的 Windows NT 集成安全性	195
14.3.3 SQL Server 的复合安全模式	198
14.3.4 改变 SQL Server 的安全模式	199
14.4 MS Exchange Server	200
14.4.1 数据加密	200
14.4.2 数字签名	203
14.4.3 用户到用户的密钥交换	203
14.4.4 防火墙	204
14.4.5 帐号的安全性	204
14.5 小 结	205
第 15 章 加密技术	206
15.1 加密与解密	206
15.2 编码及其应用	206
15.2.1 对称密钥	207
15.2.2 公共/私有密钥对(P/PK)	207
15.2.3 密钥长度	207
15.2.4 导出密钥	208
15.2.5 孤立密钥	208
15.3 暗 码	208
15.3.1 块暗码的加密模式	208
15.3.2 Secure Sockets Layer	209
15.4 Hash 程序	209
15.4.1 数字签名	209
15.4.2 确认证明书凭证	209
15.5 是否要使用加密	210
15.6 Microsoft 的加密 API (CryptoAPI)	210
15.7 小 结	210
第 16 章 企业级安全策略	211
16.1 安全策略的基本要求	211
16.1.1 密 码	211
16.1.2 安全认证通道	211
16.1.3 非委托的程序	212

16.1.4 特殊的组	212
16.1.5 组的创建与管理	212
16.1.6 复合域的组	212
16.1.7 管理员帐号策略	212
16.1.8 域与网络管理员	212
16.1.9 普通用户帐号	213
16.1.10 通用的帐号设置	213
16.1.11 安全审核	213
16.1.12 磁盘格式	213
16.1.13 打印访问策略	213
16.1.14 远程访问服务	213
16.1.15 ACL	214
16.2 小 结	214
第 17 章 Windows NT 的分布式安全服务	215
17.1 什么是 NT 分布式安全服务	215
17.1.1 Windows NT Server 目录服务	215
17.1.2 目录服务帐号管理的优点	216
17.2 多重安全协议	217
17.3 域间委托关系	218
17.4 身份验证	218
17.5 平稳转换到新版本的域	219
17.6 小 结	219
附 录	220

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。