Microsoft® Press

Microsoft® Windows® 2000 安全技术手册

（影印版）

Microsoft® Windows® 2000 Security Technical Reference

Microsoft® 公司 著

北京大学出版社
http://cbs.pku.edu.cn

Microsoft Windows 2000

安全技术手册（影印版）

Microsoft公司 著

北京大学出版社

内容简介

本书系统地讲述了 Windows 2000 安全性的设计、部署和管理，主要内容有：如何利用最新的安全配置工具，用户身份验证工具的使用，机密服务，网络资源的集中管理，Intranet 和 Internet 的安全性管理，等等。作者根据自己在实施网络安全服务方面的实际经验，向您提出了大量的建议，它将帮助您决定系统的安全级别，利用 Windows 2000 中内置的安全特性和支持，建立和维护该安全级别。

本书由微软公司组织有经验的专家编写，具有独特的技术视角和较高的权威性，是中、高级系统管理人员必备的参考书。

图书在版编目（CIP）数据
Windows 2000 安全技术手册/美国 Microsoft 公司编.
影印版.——北京：北京大学出版社，2000.11
ISBN 7-301-04848-3
Ⅰ.W… Ⅱ.美… Ⅲ.计算机网络—操作系统（软件），Windows 2000——安全技术 Ⅳ.TP393.08
中国版本图书馆 CIP 数据核字（2000）第 88458 号
著作权合同登记号：图字 01-2001-0049 号

书　　名：Microsoft Windows 2000 安全技术手册（影印版）
责任著作者：Microsoft 公司
标 准 书 号：ISBN 7-301-04848-3/TP・0509
出　版　者：北京大学出版社
地　　址：北京市海淀区中关村北京大学校内　100871
网　　址：http://cbs.pku.edu.cn
电　　话：出版部 62752015　发行部 62765128　62754140　编辑部 62765126
电 子 信 箱：wdzh@mail.263.net.cn
印　刷　者：北京大学印刷厂印刷
发　行　者：北京大学出版社
经　销　者：新华书店
787 毫米×1092 毫米　16 开本　37.75 印张　918 千字
2001 年 1 月第 1 版　2001 年 1 月第 1 次印刷
定　　价：98.00 元

出版前言

如果用一个成语来概括国内计算机图书市场的现状，当谓之“汗牛充栋”。然而，如果您是一位从事计算机应用系统开发或管理的中、高级专业人士，很可能发现这貌似种类齐全的计算机图书中，为您量身定做的并不多见。

依据多年从事计算机图书工作所积累的经验，以及与 IT 领域广泛而深入的接触所获取的信息，我们认识到，具有相当的专业深度和技术前沿性的图书，是计算机专业人员的迫切需要，当然，也是我们从事计算机图书工作、服务专业领域的一大着眼点。

基于这一点，2000 年元月，我们与微软出版社(Microsoft Press)达成合作协议，成立微软图书影印中心，独家代理微软出版社图书影印版在中国大陆的出版、发行，为 IT 业界提供及时的专业技术服务。选题和策划上的匠心独运，使得我们的影印书成为计算机图书中的标新立异者。这里，有四大特色值得读者朋友予以关注：

首先，这是微软出版社第一次授权在中国大陆影印、发行它的版权书。在选题上，可以说独辟蹊径。在内容上，立足技术广度和深度，系统推介微软产品。所有这些，都是目前国内一般计算机图书所无法比拟的。

其次，我们的理念是为国内计算机专业人员学习前沿性的微软技术提供服务。为此，我们不但与微软公司紧密协作与沟通，及时掌握微软最新技术动向，而且组织了精干的工作人员，倾力于微软影印书的出版和发行。

再者，微软影印书主要面向中、高级专业人员，印量有限。这类书的读者对象有较强的针对性，一般来说，包括 IT 决策人员，中、高级开发人员，以及中、高级系统管理人员。因而，我们将每套书的印数控制在 1000~2000 册之间。

最后，微软图书影印版几乎与原版书保持同步发行，最大限度地满足了国内读者跟踪微软最新技术的需求。软件升级越来越快，新软件令人目不暇接。作为技术载体之一的图书，只有迅速作出反应，把新软件介绍给读者，才能赢得他们的青睐。总之，兵贵神速，这是我们的目标。

正应验了前人的预言，21 世纪是一个信息时代。软件作为信息系统的神经，在我们生活的这个时代里发挥着举足轻重的作用，而微软公司和它推出的各种软件，更是令世人为之瞩目。我们将立足图书，继续并扩大与微软公司的合作，在中国信息产业的发展道路上留下自己的足迹。

出版者

2000 年 10 月

Preface

When David Clark and Anne Hamilton first asked me to undertake this project, Windows 2000 was still at beta 2. I had previously written detailed security documentation on Windows NT 4.0, and I thought I knew the scale of the work involved. I could not have been more wrong. As Windows 2000 evolved during the development process, some features were added and others changed. The interface underwent a series of changes—some fairly major, others less so. During testing we found issues, some of which were subsequently identified as bugs and fixed. Working with a product still in development was challenging. We learned a great deal the hard way, and it took more time than I had expected. Other members of the Knowledge Services team at Internet Security Systems were called in to help, and many a long evening was spent testing or trying to resolve a particular problem.

The book could not have been written without the help of two team members in particular: Ivan Phillips and Dimitris Tsapakidis. Their collective expertise and hard work were invaluable.

Thanks must also go to Tom Fronckowiak, Linda J. Locher, and Craig Zacher for their collaboration on several chapters in an effort to get us past the finishing post.

Last, but by no means least, my thanks to Maureen Zimmerman for guiding the book, and me, through the editing process to completion.

I learned a great deal during the development of this book. I hope readers find it both educational and a useful reference. Microsoft has provided a wealth of security functionality in Windows 2000. This book is intended to help readers get the most out of it.

John Hayday
Director of Knowledge Services
Internet Information Services, Inc.

Contents

List of Tables xvi
Preface xix

1 Overview of Security Changes in Windows 2000 1

Windows 2000 Versions 2
Security Features New to Windows 2000 2
Active Directory 3
Kerberos 7
Public Key Cryptography 8
Group Policy Objects 11
Internet Protocol Security 12
Encrypting File System 13
Security Configuration Tool Set 15
Summary 18

2 Windows NT 4.0 Security Review 19

Overall System Security Design 19
Secure Logon Process 19
Local Security Authority 29
Security Reference Monitor 29
Object Manager 30
Security Account Manager 30
Discretionary Access Controls 32
Security Identifiers 33
Security Access Token 35
Access Control Lists 36
Accessing an Object 38
Workgroups, Domains, and Trust Relationships 39
Workgroups 40
Joining a Domain 40
Domains 40
Trust Relationships 41

Access Control 47
File System Access Control 47
Registry Access Control 51
Printer Access Control 51
Security Event Logging 52
Users and Groups 53
User Rights and Privileges 53
Account Policy 58
Policies 58
Summary 59
3 Windows 2000 Security Model and Subsystems 61
Introducing the Security Model 61
Understanding Security Principals 62
User Accounts and Computer Accounts 62
Naming Security Principals 63
User Accounts 64
Computer Accounts 65
Group Accounts 67
Domain Trusts 73
One-Way Trusts 74
Nontransitive Trusts 74
Distributed Security Features 74
User Authentication 75
Impersonation 75
Access Token 77
Access Control 78
Public Key Infrastructure 79
Understanding Encrypting File System 80
Introducing New Local Security Features 81
NTFS 82
Secondary Logon 82
Introducing the Security Subsystem 84
User Rights 84
Local Security Policy 86
Group Policy 86
Implementing Security Functionality with System Services 86
Summary 88

4 Active Directory 89

Active Directory and Directory Services: the Basics 89
Why Do We Need a Directory Service? 89
How Does Active Directory Work? 90
What Are the Benefits of Active Directory? 91
Active Directory Architecture 93
Active Directory and Domain Name Service (DNS) 93
Active Directory and Domain Controllers 95
Active Directory Objects 98
The Schema 98
Object Naming Conventions 99
Description of Active Directory Objects 103
Object Publishing 104
Interoperability 105
Internal and External References 105
Windows 2000 Domains 106
Mixed-Mode and Native-Mode Domains 107
Sites 109
How Active Directory Uses Site Information 110
Default-First-Site-Name 111
Organizational Units 111
Active Directory Replication 113
Planning and Rollout Considerations 116
Planning for Active Directory 117
Planning the Forest Structure 118
Planning the Domain Structure 121
Planning the Organizational Unit Structure 125
Planning the Site Structure 127
Planning the DNS structure 129
Planning DNS Server Deployment 131
Optimizing Authentication with Shortcut Trusts 132
Using Active Directory 132
Active Directory Domains And Trusts Snap-In 133
The Active Directory Users and Computers Snap-In 135
The Active Directory Sites And Services Snap-In 145
Managing Active Directory 149
Delegation of Control 149
Summary 152

5 Authentication 153

Overview 153
Interactive Logon and Network Authentication 154
Interactive Logon 155
Authentication Package 157
Local Security Authority 157
Interactive Logon to Local Machine 158
Interactive Logon to a Domain Account 159
Security Support Provider 162
Network Authentication 163
Kerberos v5 164
How Does Kerberos v5 Work? 164
Enabling Kerberos v5 Authentication 167
Kerberos v5 Policies 167
Kerberos v5 Applications 168
NT LAN Manager 168
Smart Card Logon 169
What Are Smart Cards? 169
What Are the Advantages of Smart Cards? 170
Smart Card Readers 171
Enabling Smart Cards 171
Using Smart Cards 172
Secure Sockets Layer 173
Summary 174

6 Cryptography and Microsoft Public Key Infrastructure 175

An Introduction to PKI 175
Windows 2000 PKI Offerings 176
Cryptographic Background 176
Confidentiality 177
Entity Authentication 177
Data Integrity 177
Nonrepudiation 177
PKI Basics 177
Multiple CAs and Issuing Policies 178
Cryptographic Services 179
Symmetric Cryptographic Algorithms 179
Asymmetric Cryptographic Algorithms 179

Asymmetric Signing Algorithms 180
Asymmetric Key Exchange 180
Hashing 180
Cryptographic Services 180
Certification and Key Exchange 182
Microsoft PKI 185
Why Use a PKI? 186
Certificate Services 187
Certificate Lifecycles 196
Public Key Policies 199
Active Directory 199
Designing Your Public Key Infrastructure 200
Identify Your Certificate Requirements 200
Define Certificate-Issuing Practices 203
Define Your CA Trust Strategies 203
Define the CA Server Security Requirements 205
Define Certificate Lifetimes 205
Define the Enrollment and Renewal Processes 207
Define the Revocation Policy 207
Define the Maintenance and Disaster-Recovery Processes 208
Document the Design 208
Summary 208

7 Access Control Model 209

Access Control: The Basics 209
Access Control Overview 210
Permissions 211
Permission Inheritance 212
User Rights 213
Security Identifiers 213
Ownership 214
Access Tokens 215
Access Control Lists 217
Security Descriptors 219
Inheritance 221
Access Checking 223
Audit Generation 224

Editing Access Control Settings 225
Security Properties 226
Advanced Access Control Settings 227
NTFS Settings 231
Folder Sharing 232
Disk Quotas 232
Encrypting File System 234
Summary 235
8 Group Policy 237
What Is Group Policy? 238
Group Policy Infrastructure 239
Requirements for Using Group Policy 240
Group Policy MMC Snap-in Extensions 241
Windows NT 4.0 Policy vs. Windows 2000 Policy 241
Group Policy Containers and Objects 242
Local and Nonlocal Group Policy Objects 242
Organizing Group Policy Objects 243
Group Policy Containers 246
Group Policy Templates 246
Group Policy Areas 248
Computer Configuration 249
User Configuration 254
Group Policy Application 257
Policy Inheritance and Precedence 258
Security Policies Precedence 259
Startup and Logon 260
Applications and Group Policy 261
Using Group Policy Tools 264
Configuring a Domain Security Structure Using Group Policy 264
Accessing Group Policy 265
Active Directory Snap-in Extensions 266
Security Policies Tools 288
Managing Group Policy 292
Administering Group Policy in the Network 292
Securing Group Policy 294
Policy for Microsoft Management Console 295

Migration Issues 295
The Role of Administrative Templates 297
The Role of System Policy Editor 297
Windows NT 4.0 System Policies 297
Summary 298

9 Security Configuration and Monitoring 299

The Security Configuration Tool Set 300
Security Configuration Tool Set Components 301
Security Configuration Tool Set User Interfaces 302
Security Templates, Databases, and Policies 306
Security Templates 306
Predefined Security Templates 308
Security Databases 309
Security Policies 309
The Security Templates Snap-In 310
Loading the Security Templates Snap-In 311
Creating a New Template 311
Modifying an Existing Template 311
Modifying Account Policies 313
Modifying Local Policies 314
Modifying Event Log Settings 314
Creating a Restricted Group Policy 315
Setting Permissions for the System Services 316
Configuring Registry Settings 317
Configuring Permissions for a File System Directory 318
Inheriting, Overwriting, and Ignoring Policy Changes 318
Security Template Management 319
Saving the Template Console 320
Security Configuration And Analysis Snap-In 320
Installing the Security Configuration And Analysis Snap-In 321
Importing and Exporting Templates 322
Creating the Database 322
Performing the Analysis 323
Reviewing the Analysis Results 324
Modifying Baseline Analysis Settings 325
Configuring System Security 325

Viewing the Updated Settings 326

Viewing Updated Registry Settings 326

Viewing Updated File System Security Settings 327

Security Settings Extension for Group Policy Snap-In 327

Installing the Security Settings Extension 329

Editing Settings Within the Security Settings Extension 329

Secedit.exe Command-Line Tool 331

Configuring Security with Secedit.exe 332

Performing Security Analysis with Secedit.exe 333

Customizing the Security Configuration Tool Set 333

Registry Extensions 334

Editing the Registry 334

Modifying a Registry Value 335

Implementing the New Settings 338

Security Descriptor Definition Language 341

Enterprise Configuration Rollout 341

Summary 342

10 Auditing 343

Effective Auditing 344

Auditing Strategy 345

Windows 2000 Auditing Functionality 346

Audit Log File Policy 347

Configuring Audit Policy 353

Configuring Object Auditing 356

Auditing Printers 359

Auditing Local Drives 360

Auditing the Registry 362

Auditing User Account Management 363

Audit Log Categories 364

Full-Privilege Auditing 364

Setting Up Permissions for Auditing 365

Auditing and Group Policy 366

Local and Group Policy 366

Event Log Subsystem 367

Event Record 367

Event Log Properties 369

Filtering Events 369
Security Event Records 370
Finding Specific Logged Events 372
Filter Events 372
View Details about Events 373
Auditing Dynamic Host Configuration Control Protocol 373
How Audit Logging Works 374
Naming Audit Log Files 374
Starting a Daily Audit Log 374
Analyzing Server Log Files 376
DHCP Server Log File Format 376
Auditing for Message Queuing 376
Configuring Auditing 377
Audit Messages 377
IP Security Audit Log 378
Verifying IPSEC Security 378
Event Viewer and the Security Audit Log 379
TCP/IP Properties 379
Event Identifications and Descriptions 379
DHCP Server Log: Common Event Codes 388
Summary 388

11 Network Security 389

Securing IP Communications 389
Packet Capturing 390
Data Modification 390
Spoofing 390
Password Compromise 391
Denial of Service Attacks 391
Key Compromise 391
Application Layer Attack 391
IPSec Standards 394
IPSec Protocols 395
IPSec Components 401
Deploying IPSec 403
DHCP Security Issues 412
DHCP and IPSec 413
Rogue DHCP Servers 413

Securing Dynamic DNS 415
DNS Security Standards 415
The Secured Dynamic Update Procedure 416
Changing DNS Server Security Defaults 417
Changing DNS Client Security Defaults 418
Using Downlevel Clients 419
DFS Security 420
Remote Access Security 420
Extensible Authentication Protocol Support 421
EAP-MD5 421
EAP-TLS 422
Summary 422

12 Terminal Services 423
Modes of Operation 424
Application Server Mode 425
Remote Administration Mode 425
Terminal Services Integration 427
Remote Desktop Protocol 427
Preparing for Terminal Services 428
Security Auditing 428
Firewalls 428
WAN and Remote Access Considerations 428
Group Policy and Terminal Services 428
Enabling Terminal Services 431
Terminal Services Configuration Tool 433
Configuring Connections 433
Setting Connection Properties 437
Configuring Server Settings 448
Terminal Services User Configuration 451
User Permissions 451
Terminal Services Active Directory Users And Computers Extension 452
Terminal Services Client Configuration 458
Installing a Terminal Services Client 458
Connecting to a Server Running Terminal Services 459
Terminal Services Client Configuration Manager 460

Terminal Services Manager Tool 462
Console Session 463
Listener Session 463
Idle Session 463
Using Terminal Services Manager 463
Managing Sessions 468
Summary 474

13 Internet Information Services 5.0 and Internet Explorer 5.0 475

Internet Information Services 475
IIS Security Requirements 475
Connection Requirements 476
Server Security Requirements 476
What's New 476
Inherited Permissions 476
Security Templates 477
Active Directory Directory Services 477
Certificate Services 477
Kerberos Authentication 477
IPSec 477
High Encryption Pack 477
IIS Security Checklist 478
Windows Security 478
Internet Information Services Security 480
IIS Security Features 481
Resource Hierarchy and Property Inheritance 481
Authentication 481
Access Control 493
Encryption and Certificates 500
Auditing 503
Internet Explorer 5.0 505
IE Security Threats 505
Malicious Active Content 505
Executable Files and Documents 505
Confidentiality and Integrity 505
Password Confidentiality 506
Server Masquerading 506

Cookie Privacy 506

Accessing Inappropriate Content 506

Internet Explorer Security Requirements 506

Authorized Access (Execution) of Code to the Browser 506

Authorized Access to Content 506

Session Integrity and Confidentiality 507

User Privacy 507

Internet Explorer 5.0 Security Features 507

Security Zones 507

Zone Security Settings 508

Secure Client and Server Communications 520

Secure Channels 520

Authenticode 522

Content Ratings 522

Internet Explorer Administration Kit and Group Policy 524

Other Security Settings 525

Profile Assistant 525

Configuring Security Zones and Settings 526

Configuring Secure Client and Server Communications 528

Configuring Authenticode 529

Configuring Content Ratings 530

Configuring Internet Explorer Administration Kit and Group Policy 531

Configuring Other Security Settings 531

Configuring Profile Assistant 531

Summary 532

Appendixes

A Microsoft Windows 2000 Resource Kit Tools 533

Appsec.exe: Application Security 533

Auditpol.exe: Audit Policy 534

Dsstore.exe: Directory Services Store 535

Dumpel.exe: Dump Event Log 535

Efsinfo.exe: Encrypting File System Information 535

Elogdmp.exe: Event Log Dump 535