Table of Contents

Foreword xix

Acknowledgments xxi

Introduction xxiii

1 Concepts and Tools 1

Windows Operating System Versions 1

Foundation Concepts and Terms 2

Windows API 2

Services, Functions, and Routines 4

Processes, Threads, and Jobs 5

Virtual Memory 14

Kernel Mode vs. User Mode 16

Terminal Services and Multiple Sessions 19

Objects and Handles 21

Security 22

Registry 23

Unicode 23

Digging into Windows Internals 24

Reliability and Performance Monitor 25

Kernel Debugging 26

Windows Software Development Kit 31

Windows Driver Kit 31

Sysinternals Tools 32

Conclusion 32

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

2 System Architecture 33

Requirements and Design Goals 33
Operating System Model 34
Architecture Overview 35
Portability 38
Symmetric Multiprocessing 39
Scalability 43
Differences Between Client and Server Versions 43
Checked Build 47
Key System Components 49
Environment Subsystems and Subsystem DLLs 50
Ntdll.dll 57
Executive 58
Kernel 61
Hardware Abstraction Layer 65
Device Drivers 68
System Processes 74
Conclusion 83

3 System Mechanisms 85

Trap Dispatching 85
Interrupt Dispatching 87
Exception Dispatching 114
System Service Dispatching 125
Object Manager 133
Executive Objects 136
Object Structure 138
Synchronization 170
High-IRQL Synchronization 172
Low-IRQL Synchronization 177
System Worker Threads 198
Windows Global Flags 200
Advanced Local Procedure Calls (ALPCs) 202
Kernel Event Tracing 207
Wow64 211
Wow64 Process Address Space Layout 211
System Calls 212
Exception Dispatching 212

User Callbacks 212
File System Redirection 212
Registry Redirection and Reflection 213
I/O Control Requests 214
16-Bit Installer Applications 215
Printing 215
Restrictions 215
User-Mode Debugging 216
Kernel Support 216
Native Support 217
Windows Subsystem Support 219
Image Loader 220
Early Process Initialization 222
Loaded Module Database 223
Import Parsing 226
Post Import Process Initialization 227
Hypervisor (Hyper-V) 228
Partitions 230
Root Partition 230
Child Partitions 232
Hardware Emulation and Support 234
Kernel Transaction Manager 240
Hotpatch Support 242
Kernel Patch Protection 244
Code Integrity 246
Conclusion 248

4 Management Mechanisms 249

The Registry 249
Viewing and Changing the Registry 249
Registry Usage 250
Registry Data Types 251
Registry Logical Structure 252
Transactional Registry (TxR) 260
Monitoring Registry Activity 262
Registry Internals 266
Services 281
Service Applications 282
The Service Control Manager 300

Service Startup 303
Startup Errors 307
Accepting the Boot and Last Known Good 308
Service Failures 310
Service Shutdown 311
Shared Service Processes 313
Service Tags 316
Service Control Programs 317
Windows Management Instrumentation 318
Providers 319
The Common Information Model and the Managed Object Format Language 320
Class Association 325
WMI Implementation 327
WMI Security 329
Windows Diagnostic Infrastructure 329
WDI Instrumentation 330
Diagnostic Policy Service 330
Diagnostic Functionality 332
Conclusion 333

5 Processes, Threads, and Jobs 335

Process Internals 335
Data Structures 335
Kernel Variables 342
Performance Counters 343
Relevant Functions 344
Protected Processes 346
Flow of *CreateProcess* 348
Stage 1: Converting and Validating Parameters and Flags 350
Stage 2: Opening the Image to Be Executed 351
Stage 3: Creating the Windows Executive Process Object (*PspAllocateProcess*) 354
Stage 4: Creating the Initial Thread and Its Stack and Context 359
Stage 5: Performing Windows Subsystem–Specific Post-Initialization 360
Stage 6: Starting Execution of the Initial Thread 362
Stage 7: Performing Process Initialization in the Context of the New Process 363

Thread Internals 370
Data Structures 370
Kernel Variables 379
Performance Counters 379
Relevant Functions 380
Birth of a Thread 380
Examining Thread Activity 381
Limitations on Protected Process Threads 384
Worker Factories (Thread Pools) 386
Thread Scheduling 391
Overview of Windows Scheduling 391
Priority Levels 393
Windows Scheduling APIs 395
Relevant Tools 396
Real-Time Priorities 399
Thread States 400
Dispatcher Database 404
Quantum 406
Scheduling Scenarios 413
Context Switching 418
Idle Thread 418
Priority Boosts 419
Multiprocessor Systems 434
Multiprocessor Thread-Scheduling Algorithms 442
CPU Rate Limits 444
Job Objects 445
Conclusion 450

6 Security 451

Security Ratings 451
Trusted Computer System Evaluation Criteria 451
The Common Criteria 453
Security System Components 454
Protecting Objects 458
Access Checks 459
Security Descriptors and Access Control 484
Account Rights and Privileges 501
Account Rights 502

Privileges . . . 503
Super Privileges . . . 509
Security Auditing . . . 511
Logon . . . 513
Winlogon Initialization . . . 515
User Logon Steps . . . 516
User Account Control . . . 520
Virtualization . . . 521
Elevation . . . 528
Software Restriction Policies . . . 533
Conclusion . . . 535

7 I/O System . . . 537

I/O System Components . . . 537
The I/O Manager . . . 539
Typical I/O Processing . . . 540
Device Drivers . . . 541
Types of Device Drivers . . . 541
Structure of a Driver . . . 547
Driver Objects and Device Objects . . . 550
Opening Devices . . . 555
I/O Processing . . . 562
Types of I/O . . . 563
I/O Request to a Single-Layered Driver . . . 572
I/O Requests to Layered Drivers . . . 578
I/O Cancellation . . . 587
I/O Completion Ports . . . 592
I/O Prioritization . . . 598
Driver Verifier . . . 604
Kernel-Mode Driver Framework (KMDF) . . . 606
Structure and Operation of a KMDF Driver . . . 607
KMDF Data Model . . . 608
KMDF I/O Model . . . 612
User-Mode Driver Framework (UMDF) . . . 616
The Plug and Play (PnP) Manager . . . 619
Level of Plug and Play Support . . . 620
Driver Support for Plug and Play . . . 621

Driver Loading, Initialization, and Installation 623
Driver Installation 632
The Power Manager 636
Power Manager Operation 638
Driver Power Operation 639
Driver and Application Control of Device Power 643
Conclusion 644

8 Storage Management 645

Storage Terminology 645
Disk Drivers 646
Winload 646
Disk Class, Port, and Miniport Drivers 647
Disk Device Objects 650
Partition Manager 651
Volume Management 652
Basic Disks 653
Dynamic Disks 656
Multipartition Volume Management 661
The Volume Namespace 667
Volume I/O Operations 674
Virtual Disk Service 675
BitLocker Drive Encryption 677
BitLocker Architecture 677
Encryption Keys 679
Trusted Platform Module (TPM) 681
BitLocker Boot Process 683
BitLocker Key Recovery 684
Full Volume Encryption Driver 686
BitLocker Management 687
Volume Shadow Copy Service 688
Shadow Copies 688
VSS Architecture 688
VSS Operation 689
Uses in Windows 692
Conclusion 698

9 Memory Management 699
Introduction to the Memory Manager 699
Memory Manager Components 700
Internal Synchronization 701
Examining Memory Usage 701
Services the Memory Manager Provides 704
Large and Small Pages 705
Reserving and Committing Pages 706
Locking Memory 707
Allocation Granularity 708
Shared Memory and Mapped Files 709
Protecting Memory 711
No Execute Page Protection 713
Copy-on-Write 718
Address Windowing Extensions 719
Kernel-Mode Heaps (System Memory Pools) 721
Pool Sizes 722
Monitoring Pool Usage 724
Look-Aside Lists 728
Heap Manager 729
Types of Heaps 730
Heap Manager Structure 731
Heap Synchronization 732
The Low Fragmentation Heap 732
Heap Security Features 733
Heap Debugging Features 734
Pageheap 735
Virtual Address Space Layouts 736
x86 Address Space Layouts 737
x86 System Address Space Layout 740
x86 Session Space 740
System Page Table Entries 744
64-Bit Address Space Layouts 745
64-Bit Virtual Addressing Limitations 749
Dynamic System Virtual Address Space Management 751
System Virtual Address Space Quotas 756
User Address Space Layout 757

Address Translation 761
x86 Virtual Address Translation 762
Translation Look-Aside Buffer 768
Physical Address Extension (PAE) 769
IA64 Virtual Address Translation 772
x64 Virtual Address Translation 773
Page Fault Handling 774
Invalid PTEs 775
Prototype PTEs 776
In-Paging I/O 778
Collided Page Faults 779
Clustered Page Faults 779
Page Files 780
Stacks 784
User Stacks 785
Kernel Stacks 786
DPC Stack 787
Virtual Address Descriptors 787
Process VADs 788
Rotate VADs 790
NUMA 791
Section Objects 792
Driver Verifier 799
Page Frame Number Database 803
Page List Dynamics 807
Page Priority 809
Modified Page Writer 812
PFN Data Structures 814
Physical Memory Limits 818
Windows Client Memory Limits 819
Working Sets 822
Demand Paging 823
Logical Prefetcher 823
Placement Policy 827
Working Set Management 828
Balance Set Manager and Swapper 831
System Working Set 832
Memory Notification Events 833

Proactive Memory Management (SuperFetch) 836
Components 836
Tracing and Logging 838
Scenarios 840
Page Priority and Rebalancing 840
Robust Performance 843
ReadyBoost 844
ReadyDrive 845
Conclusion 847

10 Cache Manager 849

Key Features of the Cache Manager 849
Single, Centralized System Cache 850
The Memory Manager 850
Cache Coherency 850
Virtual Block Caching 852
Stream-Based Caching 852
Recoverable File System Support 853
Cache Virtual Memory Management 854
Cache Size 855
Cache Virtual Size 855
Cache Working Set Size 856
Cache Physical Size 858
Cache Data Structures 859
Systemwide Cache Data Structures 860
Per-File Cache Data Structures 862
File System Interfaces 868
Copying to and from the Cache 869
Caching with the Mapping and Pinning Interfaces 870
Caching with the Direct Memory Access Interfaces 872
Fast I/O 873
Read Ahead and Write Behind 875
Intelligent Read-Ahead 875
Write-Back Caching and Lazy Writing 877
Write Throttling 885
System Threads 886
Conclusion 887

11 File Systems 889
Windows File System Formats 890
CDFS 890
UDF 891
FAT12, FAT16, and FAT32 891
exFAT 894
NTFS 895
File System Driver Architecture 895
Local FSDs 896
Remote FSDs 897
File System Operation 901
File System Filter Drivers 907
Troubleshooting File System Problems 908
Process Monitor Basic vs. Advanced Modes 908
Process Monitor Troubleshooting Techniques 909
Common Log File System 910
NTFS Design Goals and Features 918
High-End File System Requirements 918
Advanced Features of NTFS 920
NTFS File System Driver 934
NTFS On-Disk Structure 937
Volumes 937
Clusters 937
Master File Table 938
File Reference Numbers 942
File Records 942
File Names 945
Resident and Nonresident Attributes 948
Data Compression and Sparse Files 951
The Change Journal File 956
Indexing 960
Object IDs 961
Quota Tracking 962
Consolidated Security 963
Reparse Points 965
Transaction Support 965

NTFS Recovery Support 974
Design 975
Metadata Logging 976
Recovery 981
NTFS Bad-Cluster Recovery 985
Self-Healing 989
Encrypting File System Security 990
Encrypting a File for the First Time 993
The Decryption Process 998
Backing Up Encrypted Files 999
Conclusion 1000

12 Networking 1001

Windows Networking Architecture 1001
The OSI Reference Model 1001
Windows Networking Components 1003
Networking APIs 1006
Windows Sockets 1006
Winsock Kernel (WSK) 1012
Remote Procedure Call 1014
Web Access APIs 1018
Named Pipes and Mailslots 1021
NetBIOS 1027
Other Networking APIs 1030
Multiple Redirector Support 1033
Multiple Provider Router 1034
Multiple UNC Provider 1037
Name Resolution 1039
Domain Name System 1039
Windows Internet Name Service 1039
Peer Name Resolution Protocol 1039
Location and Topology 1042
Network Location Awareness (NLA) 1042
Link-Layer Topology Discovery (LLTD) 1043
Protocol Drivers 1044
Windows Filtering Platform (WFP) 1047
NDIS Drivers 1053
Variations on the NDIS Miniport 1057
Connection-Oriented NDIS 1057

Remote NDIS 1060
QoS 1062
Binding 1064
Layered Network Services 1066
Remote Access 1066
Active Directory 1066
Network Load Balancing 1068
Distributed File System and DFS Replication 1069
Conclusion 1071

13 Startup and Shutdown 1073
Boot Process 1073
BIOS Preboot 1073
The BIOS Boot Sector and Bootmgr 1077
The EFI Boot Process 1086
Initializing the Kernel and Executive Subsystems 1088
Smss, Csrss, and Wininit 1094
ReadyBoot 1099
Images That Start Automatically 1100
Troubleshooting Boot and Startup Problems 1101
Last Known Good 1101
Safe Mode 1101
Windows Recovery Environment (WinRE) 1106
Solving Common Boot Problems 1109
Shutdown 1115
Conclusion 1118

14 Crash Dump Analysis 1119
Why Does Windows Crash? 1119
The Blue Screen 1120
Troubleshooting Crashes 1124
Crash Dump Files 1125
Crash Dump Generation 1130
Windows Error Reporting 1131
Online Crash Analysis 1133
Basic Crash Dump Analysis 1134
Notmyfault 1134
Basic Crash Dump Analysis 1135
Verbose Analysis 1137

Using Crash Troubleshooting Tools 1139
Buffer Overrun, Memory Corruptions, and Special Pool 1140
Code Overwrite and System Code Write Protection 1143
Advanced Crash Dump Analysis 1144
Stack Trashes 1145
Hung or Unresponsive Systems 1147
When There Is No Crash Dump 1150
Conclusion 1152

Glossary 1153

Index 1185

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/