

Contents

<i>Introduction</i>	<i>xi</i>
Chapter 1 Concepts and tools	1
Windows operating system versions	1
Windows 10 and future Windows versions	3
Windows 10 and OneCore	3
Foundation concepts and terms	4
Windows API	4
Services, functions, and routines	7
Processes	8
Threads	18
Jobs	20
Virtual memory	21
Kernel mode vs. user mode	23
Hypervisor	27
Firmware	29
Terminal Services and multiple sessions	29
Objects and handles	30
Security	31
Registry	32
Unicode	33
Digging into Windows internals	35
Performance Monitor and Resource Monitor	36
Kernel debugging	38
Windows Software Development Kit	43
Windows Driver Kit	43
Sysinternals tools	44
Conclusion	44
Chapter 2 System architecture	45
Requirements and design goals	45
Operating system model	46
Architecture overview	47
Portability	50
Symmetric multiprocessing	51
Scalability	53
Differences between client and server versions	54
Checked build	57
Virtualization-based security architecture overview	59

Key system components	61
Environment subsystems and subsystem DLLs	62
Other subsystems	68
Executive	72
Kernel	75
Hardware abstraction layer	79
Device drivers	82
System processes	88
Conclusion	99

Chapter 3 Processes and jobs 101

Creating a process	101
CreateProcess* functions arguments	102
Creating Windows modern processes	103
Creating other kinds of processes	104
Process internals	105
Protected processes	113
Protected Process Light (PPL)	115
Third-party PPL support	119
Minimal and Pico processes	120
Minimal processes	120
Pico processes	121
Trustlets (secure processes)	123
Trustlet structure	123
Trustlet policy metadata	124
Trustlet attributes	125
System built-in Trustlets	125
Trustlet identity	126
Isolated user-mode services	127
Trustlet-accessible system calls	128
Flow of CreateProcess	129
Stage 1: Converting and validating parameters and flags	131
Stage 2: Opening the image to be executed	135
Stage 3: Creating the Windows executive process object	138
Stage 4: Creating the initial thread and its stack and context	144
Stage 5: Performing Windows subsystem-specific initialization	146
Stage 6: Starting execution of the initial thread	148
Stage 7: Performing process initialization in the context of the new process	148
Terminating a process	154
Image loader	155
Early process initialization	157
DLL name resolution and redirection	160
Loaded module database	164
Import parsing	168
Post-import process initialization	170

SwitchBack	171
API Sets	173
Jobs	176
Job limits	177
Working with a job	178
Nested jobs	179
Windows containers (server silos)	183
Conclusion	191

Chapter 4 Threads 193

Creating threads	193
Thread internals	194
Data structures	194
Birth of a thread	206
Examining thread activity	207
Limitations on protected process threads	212
Thread scheduling	214
Overview of Windows scheduling	214
Priority levels	215
Thread states	223
Dispatcher database	228
Quantum	231
Priority boosts	238
Context switching	255
Scheduling scenarios	256
Idle threads	260
Thread suspension	264
(Deep) freeze	264
Thread selection	266
Multiprocessor systems	268
Thread selection on multiprocessor systems	283
Processor selection	284
Heterogeneous scheduling (big.LITTLE)	286
Group-based scheduling	287
Dynamic fair share scheduling	289
CPU rate limits	292
Dynamic processor addition and replacement	295
Worker factories (thread pools)	297
Worker factory creation	298
Conclusion	300

Chapter 5 Memory management 301

Introduction to the memory manager	301
Memory manager components	302
Large and small pages	303

Examining memory usage	305
Internal synchronization	308
Services provided by the memory manager	309
Page states and memory allocations	310
Commit charge and commit limit	313
Locking memory	314
Allocation granularity	314
Shared memory and mapped files	315
Protecting memory	317
Data Execution Prevention	319
Copy-on-write	321
Address Windowing Extensions	323
Kernel-mode heaps (system memory pools)	324
Pool sizes	325
Monitoring pool usage	327
Look-aside lists	331
Heap manager	332
Process heaps	333
Heap types	334
The NT heap	334
Heap synchronization	334
The low-fragmentation heap	335
The segment heap	336
Heap security features	341
Heap debugging features	342
Pageheap	343
Fault-tolerant heap	347
Virtual address space layouts	348
x86 address space layouts	349
x86 system address space layout	352
x86 session space	353
System page table entries	355
ARM address space layout	356
64-bit address space layout	357
x64 virtual addressing limitations	359
Dynamic system virtual address space management	359
System virtual address space quotas	364
User address space layout	365
Address translation	371
x86 virtual address translation	371
Translation look-aside buffer	377
x64 virtual address translation	380
ARM virtual address translation	381
Page fault handling	383
Invalid PTEs	384
Prototype PTEs	385

57A	In-paging I/O.....	386
57A	Collided page faults.....	387
57A	Clustered page faults.....	387
57A	Page files.....	389
57A	Commit charge and the system commit limit.....	394
57A	Commit charge and page file size.....	397
57A	Stacks.....	398
57A	User stacks.....	399
58A	Kernel stacks.....	400
58A	DPC stack.....	401
58A	Virtual address descriptors.....	401
	Process VADs.....	402
	Rotate VADs.....	403
58A	NUMA.....	404
58A	Section objects.....	405
58A	Working sets.....	412
58A	Demand paging.....	413
58A	Logical prefetcher and ReadyBoot.....	413
58A	Placement policy.....	416
58A	Working set management.....	417
58A	Balance set manager and swapper.....	421
58A	System working sets.....	422
58A	Memory notification events.....	423
58A	Page frame number database.....	425
58A	Page list dynamics.....	428
58A	Page priority.....	436
58A	Modified page writer and mapped page writer.....	438
58A	PFN data structures.....	440
58A	Page file reservation.....	443
58A	Physical memory limits.....	446
58A	Windows client memory limits.....	447
58A	Memory compression.....	449
58A	Compression illustration.....	450
58A	Compression architecture.....	453
58A	Memory partitions.....	456
58A	Memory combining.....	459
58A	The search phase.....	460
58A	The classification phase.....	461
58A	The page combining phase.....	462
58A	From private to shared PTE.....	462
58A	Combined pages release.....	464
58A	Memory enclaves.....	467
58A	Programmatic interface.....	468
58A	Memory enclave initializations.....	469
58A	Enclave construction.....	469
58A	Loading data into an enclave.....	471

472	Initializing an enclave	472
472	Proactive memory management (SuperFetch)	472
473	Components	473
474	Tracing and logging	474
475	Scenarios	475
476	Page priority and rebalancing	476
478	Robust performance	478
479	ReadyBoost	479
480	ReadyDrive	480
480	Process reflection	480
482	Conclusion	482
483	Chapter 6 I/O system	483
483	I/O system components	483
485	The I/O manager	485
486	Typical I/O processing	486
488	Interrupt Request Levels and Deferred Procedure Calls	488
488	Interrupt Request Levels	488
490	Deferred Procedure Calls	490
492	Device drivers	492
492	Types of device drivers	492
498	Structure of a driver	498
500	Driver objects and device objects	500
507	Opening devices	507
510	I/O processing	510
511	Types of I/O	511
513	I/O request packets	513
525	I/O request to a single-layered hardware-based driver	525
533	I/O requests to layered drivers	533
536	Thread-agnostic I/O	536
537	I/O cancellation	537
541	I/O completion ports	541
546	I/O prioritization	546
552	Container notifications	552
552	Driver Verifier	552
554	I/O-related verification options	554
555	Memory-related verification options	555
559	The Plug and Play manager	559
560	Level of Plug and Play support	560
561	Device enumeration	561
563	Device stacks	563
569	Driver support for Plug and Play	569
571	Plug-and-play driver installation	571
575	General driver loading and installation	575
575	Driver loading	575
577	Driver installation	577

The Windows Driver Foundation	578
Kernel-Mode Driver Framework	579
User-Mode Driver Framework	587
The power manager	590
Connected Standby and Modern Standby	594
Power manager operation	595
Driver power operation	596
Driver and application control of device power	599
Power management framework	600
Power availability requests	602
Conclusion	603

Chapter 7 Security 605

Security ratings	605
Trusted Computer System Evaluation Criteria	605
The Common Criteria	607
Security system components	608
Virtualization-based security	611
Credential Guard	612
Device Guard	617
Protecting objects	619
Access checks	621
Security identifiers	625
Virtual service accounts	646
Security descriptors and access control	650
Dynamic Access Control	666
The AuthZ API	666
Conditional ACEs	667
Account rights and privileges	668
Account rights	669
Privileges	670
Super privileges	675
Access tokens of processes and threads	677
Security auditing	677
Object access auditing	679
Global audit policy	682
Advanced Audit Policy settings	683
AppContainers	684
Overview of UWP apps	685
The AppContainer	687
Logon	710
Winlogon initialization	711
User logon steps	713
Assured authentication	718
Windows Biometric Framework	719
Windows Hello	721

278	User Account Control and virtualization	722
279	File system and registry virtualization	722
281	Elevation	729
282	Exploit mitigations	735
284	Process-mitigation policies	735
285	Control Flow Integrity	740
286	Security assertions	752
289	Application Identification	756
290	AppLocker	757
292	Software Restriction Policies	762
293	Kernel Patch Protection	764
294	PatchGuard	765
295	HyperGuard	768
296	Conclusion	770
297	Index	771