

Contents

Introduction	xi
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

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

38E	Initializing an enclave	472
38F	Proactive memory management (SuperFetch)	472
38F	Components	473
38E	Tracing and logging	474
38E	Scenarios	475
38F	Page priority and rebalancing	476
38E	Robust performance	478
38E	ReadyBoost	479
38E	ReadyDrive	480
38E	Process reflection	480
38E	Conclusion	482
38E	Chapter 6 I/O system	483
38E	I/O system components	483
38E	The I/O manager	485
38E	Typical I/O processing	486
38E	Interrupt Request Levels and Deferred Procedure Calls	488
38E	Interrupt Request Levels	488
38E	Deferred Procedure Calls	490
38E	Device drivers	492
38E	Types of device drivers	492
38E	Structure of a driver	498
38E	Driver objects and device objects	500
38E	Opening devices	507
38E	I/O processing	510
38E	Types of I/O	511
38E	I/O request packets	513
38E	I/O request to a single-layered hardware-based driver	525
38E	I/O requests to layered drivers	533
38E	Thread-agnostic I/O	536
38E	I/O cancellation	537
38E	I/O completion ports	541
38E	I/O prioritization	546
38E	Container notifications	552
38E	Driver Verifier	552
38E	I/O-related verification options	554
38E	Memory-related verification options	555
38E	The Plug and Play manager	559
38E	Level of Plug and Play support	560
38E	Device enumeration	561
38E	Device stacks	563
38E	Driver support for Plug and Play	569
38E	Plug-and-play driver installation	571
38E	General driver loading and installation	575
38E	Driver loading	575
38E	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

722	User Account Control and virtualization	722
722	File system and registry virtualization	722
729	Elevation	729
735	Exploit mitigations	735
735	Process-mitigation policies	735
740	Control Flow Integrity	740
752	Security assertions	752
756	Application Identification	756
757	AppLocker	757
762	Software Restriction Policies	762
764	Kernel Patch Protection	764
765	PatchGuard	765
768	HyperGuard	768
770	Conclusion	770
771	Index	771