

Inhaltsverzeichnis

Einleitung

xvii

Kapitel 1

Begriffe und Werkzeuge	1
Versionen des Betriebssystems Windows	1
Windows 10 und zukünftige Windows-Versionen	3
Windows 10 und OneCore	3
Grundprinzipien und -begriffe	4
Die Windows-API	4
Dienste, Funktionen und Routinen	7
Prozesse	8
Threads	20
Jobs	23
Virtueller Arbeitsspeicher	23
Kernel- und Benutzermodus	26
Hypervisor	30
Firmware	32
Terminaldienste und mehrere Sitzungen	32
Objekte und Handles	33
Sicherheit	34
Die Registrierung	36
Unicode	37
Die internen Mechanismen von Windows untersuchen	39
Leistungsüberwachung und Ressourcenmonitor	40
Kernel-Debugging	42
Windows Software Development Kit	48
Windows Driver Kit	49
Sysinternals-Werkzeuge	49
Zusammenfassung	50

Kapitel 2

Systemarchitektur	51
Anforderungen und Designziele	51
Das Modell des Betriebssystems	52
Die Architektur im Überblick	53
Portierbarkeit	56
Symmetrisches Multiprocessing	57
Skalierbarkeit	60
Unterschiede zwischen den Client- und Serverversionen	61
Testbuild	64
Die virtualisierungsgestützte Sicherheitsarchitektur im Überblick	66
Hauptsystemkomponenten	69
Umgebungsteilsysteme und Teilsystem-DLLs	70
Weitere Teilsysteme	76
Exekutive	81
Der Kernel	84
Die Hardwareabstraktionsschicht	88
Gerätetreiber	92
Systemprozesse	98
Zusammenfassung	111

Kapitel 3

Prozesse und Jobs	113
Prozesse erstellen	113
Argumente der CreateProcess*-Funktionen	114
Moderne Windows-Prozesse erstellen	115
Andere Arten von Prozessen erstellen	116
Interne Mechanismen von Prozessen	117
Geschützte Prozesse	126
Protected Process Light (PPL)	128
Unterstützung für Drittanbieter-PPLs	133
Minimale und Pico-Prozesse	134
Minimale Prozesse	134
Pico-Prozesse	134

Trustlets (sichere Prozesse)	137
Der Aufbau von Trustlets	137
Richtlinien-Metadaten für Trustlets	138
Attribute von Trustlets	139
Integrierte System-Trustlets	140
Trustlet-Identität	140
IUM-Dienste	141
Für Trustlets zugängliche Systemaufrufe	142
Der Ablauf von CreateProcess	144
Phase 1: Parameter und Flags konvertieren und validieren	145
Phase 2: Das auszuführende Abbild öffnen	151
Phase 3: Das Windows-Exekutivprozessobjekt erstellen	154
Phase 4: Den ursprünglichen Thread mit seinem Stack und Kontext erstellen	160
Phase 5: Spezifische Prozessinitialisierung für das Windows-Teilsystem durchführen	162
Phase 6: Ausführung des ursprünglichen Threads starten	164
Phase 7: Prozessinitialisierung im Kontext des neuen Prozesses durchführen	165
Einen Prozess beenden	172
Der Abbildlader	173
Frühe Prozessinitialisierung	176
DLL-Namensauflösung und -Umleitung	179
Die Datenbank der geladenen Module	183
Importanalyse	188
Prozessinitialisierung nach dem Import	190
SwitchBack	191
API-Sets	194
Jobs	196
Grenzwerte für Jobs	197
Umgang mit Jobs	199
Verschachtelte Jobs	199
Windows-Container (Serversilos)	204
Zusammenfassung	213

Threads	215
Threads erstellen	215
Interne Strukturen von Threads	216
Datenstrukturen	216
Geburt eines Threads	230
Die Threadaktivität untersuchen	231
Einschränkungen für Threads in geschützten Prozessen	237
Threadplanung	238
Überblick über die Threadplanung in Windows	239
Prioritätsstufen	240
Threadstatus	248
Die Dispatcherdatenbank	255
Das Quantum	258
Prioritätserhöhung	266
Kontextwechsel	286
Mögliche Fälle bei der Threadplanung	288
Leerlaufthreads	292
Anhalten von Threads	296
Einfrieren und Tiefgefrieren	296
Threadauswahl	299
Mehrprozessorsysteme	301
Threadauswahl auf Mehrprozessorsystemen	319
Prozessorauswahl	320
Heterogene Threadplanung (big.LITTLE)	322
Gruppengestützte Threadplanung	324
Dynamische gleichmäßige Planung (DFSS)	326
Grenzwerte für die CPU-Rate	330
Dynamisches Hinzufügen und Ersetzen von Prozessoren	333
Arbeitsfactories (Threadpools)	335
Erstellen von Arbeitsfactories	337
Zusammenfassung	339

Speicherverwaltung	341
Einführung in den Speicher-Manager	341
Komponenten des Speicher-Managers	342
Große und kleine Seiten	343
Die Speichernutzung untersuchen	345
Interne Synchronisierung	350
Vom Speicher-Manager bereitgestellte Dienste	350
Seitenstatus und Speicherzuweisungen	352
Gesamter zugesicherter Speicher und Zusicherungsgrenzwert	356
Seiten im Arbeitsspeicher festhalten	356
Granularität der Zuweisung	357
Gemeinsam genutzter Arbeitsspeicher und zugeordnete Dateien	357
Speicherschutz	360
Datenausführungsverhinderung	362
Kopieren beim Schreiben	366
AWE (Address Windowing Extensions)	367
Kernelmodusheaps (Systemspeicherpools)	370
Poolgrößen	370
Die Poolnutzung überwachen	372
Look-Aside-Listen	377
Der Heap-Manager	378
Prozessheaps	379
Arten von Heaps	380
NT-Heaps	380
Heapsynchronisierung	381
Der Low-Fragmentation-Heap	381
Segmentheaps	383
Sicherheitseinrichtungen von Heaps	388
Debugging einrichten für Heaps	390
Der Seitenheap	391
Der fehlertolerante Heap	394
Layouts für virtuelle Adressräume	396
x86-Adressraumlayouts	397
Das Layout des x86-Systemadressraums	401

x86-Sitzungsraum	401
System-Seitentabelleneinträge	404
ARM-Adressraumlayout	405
64-Bit-Adressraumlayout	406
Einschränkungen bei der virtuellen Adressierung auf x64-Systemen	408
Dynamische Verwaltung des virtuellen Systemadressraums	408
Kontingente für den virtuellen Systemadressraum	415
Layout des Benutzeradressraums	416
Adressübersetzung	422
Übersetzung virtueller Adressen auf x86-Systemen	422
Der Look-Aside-Übersetzungspuffer für die Übersetzung	429
Übersetzung virtueller Adressen auf x64-Systemen	433
Übersetzung virtueller Adressen auf ARM-Systemen	434
Seitenfehler	435
Ungültige PTEs	436
Prototyp-PTEs	438
Einlagerungs-E/A	440
Seitenfehlerkollisionen	440
Seitencluster	441
Auslagerungsdateien	442
Gesamter zugesicherter Speicher und systemweiter Zusicherungsgrenzwert	448
Der Zusammenhang zwischen dem gesamten zugesicherten Speicher und der Größe der Auslagerungsdatei	452
Stacks	454
Benutzerstacks	455
Kernelstacks	456
Der DPC-Stack	457
VADs	457
Prozess-VADs	458
Umlauf-VADs	460
NUMA	461
Abschnittsobjekte	462
Arbeitssätze	472
Auslagerung bei Bedarf	472
Der logische Prefetcher und ReadyBoot	473

Platzierungsrichtlinien	477
Verwaltung von Arbeitssätzen	477
Der Balance-Set-Manager und der Swapper	482
Systemarbeitssätze	483
Speicherbenachrichtigungsereignisse	485
Die PFN-Datenbank	487
Seitenlistendynamik	491
Seitenpriorität	499
Die Schreibthreads für geänderte und für zugeordnete Seiten	502
PFN-Datenstrukturen	504
Reservierungen in der Auslagerungsdatei	509
Grenzwerte für den physischen Speicher	512
Speichergrenzwerte für Windows-Clienteditionen	513
Speicherkomprimierung	515
Ablauf der Komprimierung	516
Komprimierungsarchitektur	520
Speicherpartitionen	523
Speicherzusammenführung	526
Die Suchphase	528
Die Klassifizierungsphase	529
Die Zusammenführungsphase	530
Vom privaten zum gemeinsamen PTE	530
Freigabe von zusammengeführten Seiten	533
Speicherenklaven	536
Programmierschnittstellen	538
Initialisierung von Speicherenklaven	538
Aufbau von Enklaven	539
Daten in eine Enklave laden	541
Eine Enklave initialisieren	542
Vorausschauende Speicherverwaltung (SuperFetch)	542
Komponenten	543
Ablaufverfolgung und Protokollierung	544
Szenarien	545
Seitenpriorität und Rebalancing	546
Leistungsstabilisierung	549

ReadyBoost	550
ReadyDrive	551
Prozessreflexion	552
Zusammenfassung	554

Kapitel 6

Das E/A-System	555
-----------------------------	------------

Komponenten des E/A-Systems	555
Der E/A-Manager	557
Typische E/A-Verarbeitung	558
IRQ-Ebenen und verzögerte Prozeduraufrufe	560
IRQ-Ebenen	561
Verzögerte Prozeduraufrufe	563
Gerätetreiber	564
Arten von Gerätetreibern	565
Aufbau eines Treibers	572
Treiber- und Geräteobjekte	574
Geräte öffnen	582
E/A-Verarbeitung	586
Verschiedene Arten der E/A	586
E/A-Anforderungspakete	590
E/A-Anforderungen an einen einschichtigen Hardwaretreiber	603
E/A-Anforderungen an geschichtete Treiber	613
Threadagnostische E/A	616
Abbrechen der E/A	617
E/A-Vervollständigungsports	622
E/A-Priorisierung	627
Containerbenachrichtigungen	634
Treiberüberprüfung	635
E/A-Überprüfungsoptionen	638
Speicherüberprüfungsoptionen	638
Der PnP-Manager	643
Der Grad der Unterstützung für Plug & Play	644
Geräteauflistung	645
Gerätestacks	649

Treiberunterstützung für Plug & Play	655
Installation von Plug-&-Play-Treibern	656
Laden und Installieren von Treibern	661
Treiber laden	661
Treiberinstallation	663
Windows Driver Foundation	664
Kernel-Mode Driver Framework	665
Das E/A-Modell von KMDF	672
User-Mode Driver Framework	675
Energieverwaltung	679
Verbundener und moderner Standbymodus	683
Funktionsweise der Energieverwaltung	684
Energieverwaltung durch die Treiber	686
Steuerung der Geräteenergiezustände durch den Treiber und die Anwendung	689
Das Framework für die Energieverwaltung	690
Energieverfügbarkeitsanforderungen	692
Zusammenfassung	694

Kapitel 7

Sicherheit	697
Sicherheitseinstufungen	697
Trusted Computer System Evaluation Criteria	697
Common Criteria	699
Systemkomponenten für die Sicherheit	700
Virtualisierungsgestützte Sicherheit	704
Credential Guard	705
Device Guard	712
Objekte schützen	714
Zugriffsprüfungen	716
Sicherheitskennungen	720
Virtuelle Dienstkonten	745
Sicherheitsdeskriptoren und Zugriffssteuerung	751
Dynamische Zugriffssteuerung	770

Die AuthZ-API	771
Bedingte Zugriffssteuerungseinträge	772
Privilegien und Kontorechte	773
Kontorechte	775
Privilegien	776
Superprivilegien	783
Zugriffstokens von Prozessen und Threads	784
Sicherheitsüberwachung	785
Überwachung des Objektzugriffs	787
Globale Überwachungsrichtlinie	790
Erweiterte Überwachungsrichtlinienkonfiguration	792
Anwendungscontainer	793
UWP-Apps im Überblick	794
Anwendungscontainer	796
Anmeldung	824
Initialisierung durch Winlogon	826
Die einzelnen Schritte der Benutzeranmeldung	827
Sichere Authentifizierung	833
Das Windows-Biometrieframework	835
Windows Hello	837
Benutzerkontensteuerung und Virtualisierung	838
Virtualisierung des Dateisystems und der Registrierung	839
Rechteerhöhung	847
Schutz gegen Exploits	855
Abwehrmaßnahmen auf Prozessebene	856
Control Flow Integrity	861
Zusicherungen	875
Anwendungsidentifizierung	880
AppLocker	882
Richtlinien für Softwareeinschränkung	887
Kernelpatchschutz	889
PatchGuard	890
HyperGuard	894
Zusammenfassung	896
Index	897