

# Inhaltsverzeichnis

Einleitung

xvii

## Kapitel 1

---

<b>Begriffe und Werkzeuge</b>	<b>1</b>
<b>Versionen des Betriebssystems Windows</b>	<b>1</b>
Windows 10 und zukünftige Windows-Versionen	3
Windows 10 und OneCore	3
<b>Grundprinzipien und -begriffe</b>	<b>4</b>
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
<b>Die internen Mechanismen von Windows untersuchen</b>	<b>39</b>
Leistungsüberwachung und Ressourcenmonitor	40
Kernel-Debugging	42
Windows Software Development Kit	48
Windows Driver Kit	49
Sysinternals-Werkzeuge	49
<b>Zusammenfassung</b>	<b>50</b>

vii

## Kapitel 2

---

<b>Systemarchitektur</b>	<b>51</b>
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

---

<b>Prozesse und Jobs</b>	<b>113</b>
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

<b>Trustlets (sichere Prozesse)</b> .....	<b>137</b>
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
<b>Der Ablauf von CreateProcess</b> .....	<b>144</b>
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
<b>Einen Prozess beenden</b> .....	<b>172</b>
<b>Der Abbildlader</b> .....	<b>173</b>
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
<b>Jobs</b> .....	<b>196</b>
Grenzwerte für Jobs .....	197
Umgang mit Jobs .....	199
Verschachtelte Jobs .....	199
Windows-Container (Serversilos) .....	204
<b>Zusammenfassung</b> .....	<b>213</b>

<b>Threads</b>	<b>215</b>
<b>Threads erstellen</b>	<b>215</b>
<b>Interne Strukturen von Threads</b>	<b>216</b>
Datenstrukturen	216
Geburt eines Threads	230
<b>Die Threadaktivität untersuchen</b>	<b>231</b>
Einschränkungen für Threads in geschützten Prozessen	237
<b>Threadplanung</b>	<b>238</b>
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
<b>Gruppengestützte Threadplanung</b>	<b>324</b>
Dynamische gleichmäßige Planung (DFSS)	326
Grenzwerte für die CPU-Rate	330
Dynamisches Hinzufügen und Ersetzen von Prozessoren	333
<b>Arbeitsfactories (Threadpools)</b>	<b>335</b>
Erstellen von Arbeitsfactories	337
<b>Zusammenfassung</b>	<b>339</b>

<b>Speicherverwaltung</b>	<b>341</b>
<b>Einführung in den Speicher-Manager</b> .....	<b>341</b>
Komponenten des Speicher-Managers .....	342
Große und kleine Seiten .....	343
Die Speichernutzung untersuchen .....	345
Interne Synchronisierung .....	350
<b>Vom Speicher-Manager bereitgestellte Dienste</b> .....	<b>350</b>
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
<b>Kernelmodusheaps (Systemspeicherpools)</b> .....	<b>370</b>
Poolgrößen .....	370
Die Poolnutzung überwachen .....	372
Look-Aside-Listen .....	377
<b>Der Heap-Manager</b> .....	<b>378</b>
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
<b>Layouts für virtuelle Adressräume</b> .....	<b>396</b>
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
<b>Adressübersetzung</b>	<b>422</b>
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
<b>Seitenfehler</b>	<b>435</b>
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
<b>Stacks</b>	<b>454</b>
Benutzerstacks	455
Kernelstacks	456
Der DPC-Stack	457
<b>VADs</b>	<b>457</b>
Prozess-VADs	458
Umlauf-VADs	460
<b>NUMA</b>	<b>461</b>
<b>Abschnittsobjekte</b>	<b>462</b>
<b>Arbeitssätze</b>	<b>472</b>
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
<b>Die PFN-Datenbank .....</b>	<b>487</b>
Seitenlistendynamik .....	491
Seitenpriorität .....	499
Die Schreibthreads für geänderte und für zugeordnete Seiten .....	502
PFN-Datenstrukturen .....	504
Reservierungen in der Auslagerungsdatei .....	509
<b>Grenzwerte für den physischen Speicher .....</b>	<b>512</b>
Speichergrenzwerte für Windows-Clienteditionen .....	513
<b>Speicherkomprimierung .....</b>	<b>515</b>
Ablauf der Komprimierung .....	516
Komprimierungsarchitektur .....	520
<b>Speicherpartitionen .....</b>	<b>523</b>
<b>Speicherzusammenführung .....</b>	<b>526</b>
Die Suchphase .....	528
Die Klassifizierungsphase .....	529
Die Zusammenführungsphase .....	530
Vom privaten zum gemeinsamen PTE .....	530
Freigabe von zusammengeführten Seiten .....	533
<b>Speicherenklaven .....</b>	<b>536</b>
Programmierschnittstellen .....	538
Initialisierung von Speicherenklaven .....	538
Aufbau von Enklaven .....	539
Daten in eine Enklave laden .....	541
Eine Enklave initialisieren .....	542
<b>Vorausschauende Speicherverwaltung (SuperFetch) .....</b>	<b>542</b>
Komponenten .....	543
Ablaufverfolgung und Protokollierung .....	544
Szenarien .....	545
Seitenpriorität und Rebalancing .....	546
Leistungsstabilisierung .....	549

ReadyBoost .....	550
ReadyDrive .....	551
Prozessreflexion .....	552
<b>Zusammenfassung .....</b>	<b>554</b>

## Kapitel 6

<b>Das E/A-System</b>	<b>555</b>
<b>Komponenten des E/A-Systems</b> .....	<b>555</b>
Der E/A-Manager .....	557
Typische E/A-Verarbeitung .....	558
<b>IRQ-Ebenen und verzögerte Prozeduraufrufe</b> .....	<b>560</b>
IRQ-Ebenen .....	561
Verzögerte Prozeduraufrufe .....	563
<b>Gerätetreiber</b> .....	<b>564</b>
Arten von Gerätetreibern .....	565
Aufbau eines Treibers .....	572
Treiber- und Geräteobjekte .....	574
Geräte öffnen .....	582
<b>E/A-Verarbeitung</b> .....	<b>586</b>
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
<b>Treiberüberprüfung</b> .....	<b>635</b>
E/A-Überprüfungsoptionen .....	638
Speicherüberprüfungsoptionen .....	638
<b>Der PnP-Manager</b> .....	<b>643</b>
Der Grad der Unterstützung für Plug & Play .....	644
Geräteauflistung .....	645
Gerätestacks .....	649



Treiberunterstützung für Plug & Play .....	655
Installation von Plug-&-Play-Treibern .....	656
<b>Laden und Installieren von Treibern .....</b>	<b>661</b>
Treiber laden .....	661
Treiberinstallation .....	663
<b>Windows Driver Foundation .....</b>	<b>664</b>
Kernel-Mode Driver Framework .....	665
Das E/A-Modell von KMDF .....	672
User-Mode Driver Framework .....	675
<b>Energieverwaltung .....</b>	<b>679</b>
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
<b>Zusammenfassung .....</b>	<b>694</b>

## Kapitel 7

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

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