

Spis treści

Wprowadzenie	13
Rozdział 1. Zagadnienia i narzędzia	19
Wersje systemu operacyjnego Windows	19
Windows 10 i przyszłe wersje systemu Windows	21
Windows 10 i platforma OneCore	22
Podstawowe pojęcia i terminy	22
Interfejs API systemu Windows	22
Usługi, funkcje i programy	26
Procesy	27
Wątki	37
Zadania	40
Pamięć wirtualna	40
Porównanie trybu jądra i trybu użytkownika	43
Hipernadzorca	47
Oprogramowanie sprzętowe	49
Usługi terminalowe i wiele sesji	49
Obiekty i dojścia	50
Zabezpieczenia	51
Rejestr	53
Unicode	53
Analizowanie wewnętrznych mechanizmów systemu Windows	55
Monitor wydajności i Monitor zasobów	56
Debugowanie jądra	58
Windows Software Development Kit	64
Windows Driver Kit	64
Narzędzia z witryny Sysinternals	65
Podsumowanie	65
Rozdział 2. Architektura systemu	67
Wymagania i cele projektowe	67
Model systemu operacyjnego	68
Opis architektury systemu	69
Przenośność	72
Wieloprosesorowość symetryczna	73
Skalowalność	75
Różnice między wersjami kliencką i serwerową	76
Wersja Checked build (kompilacja testowa)	79
Krótki opis architektury z mechanizmami bezpieczeństwa opartymi na wirtualizacji	81
Kluczowe komponenty systemu	84
Podsystemy środowiskowe i biblioteki podsystemów	84
Inne podsystemy	91

Centrum wykonawcze	96
Jądro	99
Warstwa abstrakcji sprzętowej	102
Sterowniki urządzeń	105
Procesy systemowe	112
Podsumowanie	124
Rozdział 3. Procesy i zadania	125
Tworzenie procesu	125
Argumenty funkcji CreateProcess*	127
Tworzenie nowoczesnych procesów systemu Windows	128
Tworzenie innych rodzajów procesów	128
Wewnętrzne elementy procesów	129
Chronione procesy	137
Protected Process Light (PPL)	138
Obsługa zewnętrznych procesów przez rozszerzenie PPL	143
Procesy minimalne i procesy Pico	144
Procesy minimalne	144
Procesy Pico	145
Programy Trustlet (bezpieczne procesy)	147
Struktura programu Trustlet	148
Metadane zasad programów Trustlet	149
Atrybuty programów Trustlet	150
Programy Trustlet wbudowane w system	151
Tożsamość programów Trustlet	151
Usługi izolowanego trybu użytkownika	152
Wywołania systemowe dostępne dla programów Trustlet	153
Przepływ funkcji CreateProcess	155
Etap 1. Przekształcanie i sprawdzanie poprawności parametrów i flag	157
Etap 2. Otwieranie obrazu do wykonania	162
Etap 3. Tworzenie obiektu procesu wykonawczego systemu Windows	165
Etap 4. Tworzenie początkowego wątku oraz jego stosu i kontekstu	171
Etap 5. Przeprowadzanie inicjalizacji powiązanej z podsystemem systemu Windows	174
Etap 6. Rozpoczęcie wykonywania wątku początkowego	176
Etap 7. Przeprowadzanie inicjalizacji procesu w kontekście nowego procesu	176
Kończenie procesu	183
Program ładujący obrazy	184
Wczesna inicjalizacja procesu	186
Przekierowywanie i rozwiązywanie nazw bibliotek DLL	189
Baza danych załadowanych modułów	194
Analizowanie importu	199
Inicjalizacja procesu po imporcie	200
Technologia Switch Back	201
Mechanizm API Sets	204
Zadania	206

Limity zadań	207
Obsługa zadania	209
Zadania zagnieżdżone	209
Kontenery systemu Windows (silosy serwerowe)	213
Podsumowanie	222

Rozdział 4. Wątki 223

Tworzenie wątków	223
Wewnętrzne mechanizmy wątków	224
Struktury danych	224
Powstanie wątku	236
Sprawdzanie aktywności wątków	237
Ograniczenia wątków chronionych procesów	242
Planowanie wątków	243
Przegląd planowania w systemie Windows	243
Poziomy priorytetów	245
Stany wątków	252
Baza danych dyspozytora	258
Kwant	260
Zwiększanie priorytetu	268
Przełączanie kontekstu	286
Warianty planowania	288
Wątki bezczynności	292
Wstrzymanie wątków	296
„Głębokie zamrożenie”	296
Wybór wątku	298
Systemy wieloprocessorowe	300
Wybór wątku w systemach wieloprocessorowych	316
Wybór procesora	317
Planowanie heterogeniczne (big.LITTLE)	320
Planowanie oparte na grupach	322
Planowanie dynamiczne ze sprawiedliwym udostępnianiem	323
Limity wykorzystania procesora	327
Dynamiczne dodawanie i usuwanie procesorów	330
Fabryki procesów roboczych (pule wątków)	332
Tworzenie fabryki wątków roboczych	333
Podsumowanie	336

Rozdział 5. Zarządzanie pamięcią 337

Wprowadzenie do menedżera pamięci	337
Składniki menedżera pamięci	338
Strony małe i duże	339
Sprawdzanie wykorzystania pamięci	341
Synchronizacja wewnętrzna	344
Usługi menedżera pamięci	345
Stany stron i przydzielanie pamięci	347
Ładunek deklaracji i limit deklaracji	350
Blokowanie pamięci	350

Ziarnistość alokacji	351
Pamięć współdzielona i pliki mapowane	351
Ochrona pamięci	354
Zapobieganie wykonywaniu danych	356
Kopiowanie przy zapisie	359
Okienkowe poszerzanie przestrzeni adresowej	361
Stery w trybie jądra (systemowe pule pamięci)	363
Rozmiary pul	363
Monitorowanie wykorzystania puli	365
Listy asocjacyjne	369
Menedżer sterty	370
Stery procesu	371
Typy stert	372
Serta NT	372
Synchronizacja sterty	373
Serta o małej fragmentacji	373
Serta segmentowa	374
Bezpieczeństwo stert	379
Funkcje debugowania sterty	380
Mechanizm pageheap	381
Serta odporna na błędy	385
Układy wirtualnej przestrzeni adresowej	386
Układy przestrzeni adresowej na platformie x86	388
Układ systemowej przestrzeni adresowej na platformie x86	391
Przestrzeń sesji na platformie x86	391
Systemowe wpisy tabeli stron	393
Układ przestrzeni adresowej na platformie ARM	394
Układ przestrzeni adresowej 64-bitowej	394
Ograniczenia adresowania wirtualnego na platformie x64	396
Dynamiczne zarządzanie systemową wirtualną przestrzenią adresową	397
Przydziały systemowej wirtualnej przestrzeni adresowej	402
Układ przestrzeni adresowej użytkownika	403
Tłumaczenie adresów	409
Tłumaczenie adresów wirtualnych na platformie x86	409
Asocjacyjny bufor translacji	415
Tłumaczenie adresów wirtualnych na platformie x64	418
Tłumaczenie adresów wirtualnych na platformie ARM	419
Obsługa błędów strony	420
Niewłaściwe wpisy PTE	422
Prototypowe wpisy PTE	423
Operacje wejścia-wyjścia w stronicowaniu	425
Błąd strony kolidującej	425
Błędy stron klastrowanych	426
Pliki stronicowania	427
Ładunek deklaracji i systemowy limit deklaracji	432
Ładunek deklaracji a rozmiar pliku stronicowania	435
Stosy	438

Stosy użytkownika	438
Stosy jądra	439
Stos DPC	440
Deskryptory adresów wirtualnych	440
Struktury VAD procesu	441
Rotacja deskryptorów adresów wirtualnych	443
NUMA	443
Obiekty sekcji	444
Zestawy robocze	452
Stronicowanie na żądanie	452
Logiczny prefetcher i funkcja ReadyBoot	453
Strategia rozmieszczania	456
Zarządzanie zestawami roboczymi	457
Menedżer zestawu równowagi i program wymiany	461
Systemowe zestawy robocze	462
Powiadomienia o stanie pamięci	463
Baza danych numerów stron pamięci	465
Dynamika list stron	469
Priorytet stronicowy	477
Moduł zapisujący strony zmodyfikowane i zmapowane	479
Struktury danych PFN	481
Rezerwacja pliku stronicowania	485
Ograniczenia pamięci fizycznej	488
Limity pamięci w klienckich wersjach systemu Windows	489
Kompresja pamięci	491
Ilustracja kompresji	492
Architektura kompresji	495
Partycje pamięci	498
Scalanie pamięci	501
Etap wyszukiwania	502
Etap klasyfikacji	503
Etap scalania stron	504
Konwersja wpisu PTE z prywatnego na współdzielony	505
Zwalnianie stron skalonych	506
Enklawy pamięci	510
Interfejs programowy	511
Przygotowywanie enklaw pamięci	512
Konstruowanie enklawy	512
Wczytywanie danych do enklawy	514
Inicjalizacja enklawy	515
Proaktywne zarządzanie pamięcią (mechanizm Super Fetch)	515
Komponenty	516
Śledzenie i rejestrowanie	518
Scenariusze	519
Priorytet strony oraz ponowne bilansowanie	520
Niezawodność działania	522
Funkcja Ready Boost	523

Funkcja Ready Drive	524
Dublowanie procesu	525
Podsumowanie	527

Rozdział 6. System operacji wejścia-wyjścia 529

Komponenty systemu operacji wejścia-wyjścia	529
Menedżer operacji wejścia-wyjścia	531
Typowe przetwarzanie operacji wejścia-wyjścia	532
Poziomy żądań przerwania IRQL i wywołania DPC	535
Poziomy żądań przerwania	535
Wywołania DPC	537
Sterowniki urządzeń	539
Typy sterowników urządzeń	539
Struktura sterownika	545
Obiekty sterowników i obiekty urządzeń	548
Otwieranie urządzeń	555
Przetwarzanie operacji wejścia-wyjścia	559
Typy operacji wejścia-wyjścia	560
Pakiety żądań operacji wejścia-wyjścia IRP	563
Żądanie operacji wejścia-wyjścia wysyłane do jednowarstwowego sterownika urządzenia	574
Żądania operacji wejścia-wyjścia kierowane do sterowników z warstwami	586
Operacja wejścia-wyjścia agnostyczna względem wątków	589
Anulowanie operacji wejścia-wyjścia	589
Porty ukończenia operacji wejścia-wyjścia	594
Określanie priorytetu operacji wejścia-wyjścia	599
Powiadomienia kontenerów	606
Driver Verifier	606
Opcje weryfikacji powiązane z operacjami wejścia-wyjścia	608
Opcje weryfikacji związane z pamięcią	609
Menedżer technologii PnP	614
Poziom obsługi technologii Plug and Play	615
Wyliczanie urządzeń	615
Stosy urządzeń	618
Obsługa technologii Plug and Play przez sterowniki	625
Instalacja sterownika Plug and Play	627
Ładowanie i instalowanie ogólnego sterownika	631
Ładowanie sterowników	631
Instalacja sterownika	633
Środowisko WDF	634
Środowisko KMDF	635
Środowisko UMDF	644
Menedżer zasilania	648
Stany Connected Standby i Modern Standby	652
Działanie menedżera zasilania	652
Kontrola zasilania urządzenia przez aplikację i sterownik	657
Środowisko zarządzania zasilaniem	658

Żądania dostępności zasilania	660
Podsumowanie	662
Rozdział 7. Bezpieczeństwo	663
Klasy bezpieczeństwa	663
Kryteria oceny zaufanych systemów komputerowych (TCSEC)	663
Wspólne kryteria	665
Składniki systemu zabezpieczeń	666
Bezpieczeństwo oparte na wirtualizacji	669
Ochrona poświadczeń	670
Ochrona urządzenia	676
Ochrona obiektów	678
Sprawdzanie dostępu	681
Identyfikatory zabezpieczeń	684
Wirtualne konta usług	706
Deskryptory zabezpieczeń i kontrola dostępu	711
Dynamiczna kontrola dostępu	728
Interfejs AuthZ	728
Warunkowe wpisy ACE	730
Prawa i przywileje konta	731
Prawa konta	732
Przywileje	732
Superprzywileje	739
Tokeny dostępowe procesów i wątków	740
Inspekcje zabezpieczeń	740
Inspekcje dostępu do obiektów	742
Globalne zasady inspekcji	745
Ustawienia zaawansowanych zasad inspekcji	747
Kontenery aplikacji	748
Przegląd aplikacji UWP	748
Kontener aplikacji	751
Logowanie	774
Inicjacja procesu Winlogon	776
Etapy logowania użytkownika	777
Wzmocnione uwierzytelnianie	783
Biometria w systemie Windows	784
Windows Hello	786
Kontrola konta użytkownika i wirtualizacja	787
Wirtualizacja systemu plików i rejestru	788
Podwyższanie uprawnień	794
Oslabianie exploitów	801
Zasady osłabiania procesów	803
Integralność przepływu sterowania	808
Asercje bezpieczeństwa	821
Identyfikacja aplikacji	826
AppLocker	827
Zasady ograniczeń oprogramowania	832

Ochrona przed poprawkami jądra	834
PatchGuard	835
HyperGuard	839
Podsumowanie	841
Skorowidz	842