

Spis treści

O autorach	15
Przedmowa	17
Wprowadzenie	21
Rozdział 8. Mechanizmy systemowe	27
Model wykonawczy procesora	27
Segmentacja	28
Segment stanu zadania	32
Sprzętowe błędy w bocznym kanale	35
Wykonywanie instrukcji poza kolejnością	36
Predyktor skoku	36
Pamięci podręczne procesora	37
Ataki przeprowadzane bocznym kanałem	39
Zabezpieczenia w systemie Windows przed atakami przeprowadzanymi bocznym kanałem	43
Cieniowanie KVA	43
Sprzętowa kontrola skoków pośrednich (IBRS, IBPB, STIBP, SSBD)	47
Sekwencja Retpoline i optymalizacja importu	50
Parowanie STIBP	53
Zlecanie pułapek	56
Zlecanie przerw	58
Przerwania sterowane liniami i komunikatami	77
Obsługa czasomierza	94
Systemowe wątki robocze	109
Zlecanie wyjątków	113
Obsługa wywołań systemowych	119
Podsystem WoW64 (Windows-on-Windows)	132
Rdzeń podsystemu WoW64	133
Przekierowanie systemu plików	137
Przekierowanie rejestru	138
Symulacja procesora x86 na platformie AMD64	139

Procesory ARM	141
Modele pamięci	141
Symulacja procesora ARM32 na procesorze ARM64	142
Symulacja procesora x86 na procesorze ARM64	143
Menedżer obiektów	152
Obiekty wykonawcze	155
Struktura obiektu	159
Synchronizacja	199
Synchronizacja na wysokim poziomie IRQL	201
Synchronizacja na niskim poziomie IRQL	206
Zaawansowane wywołanie procedury lokalnej	237
Model połączeń	238
Model komunikatów	240
Model asynchroniczny	242
Widoki, regiony i sekcje	243
Atrybuty	244
Krople, uchwyt i zasoby	245
Przekazywanie uchwytów	246
Bezpieczeństwo	247
Wydajność	248
Zarządzanie energią	249
Atrybut bezpośredniego zdarzenia	249
Diagnostowanie i śledzenie komunikacji	250
Funkcja powiadamiania w systemie Windows	252
Funkcjonalności WNF	252
Zastosowania WNF	253
Nazwy stanów WNF i ich przechowywanie	261
Agregacja zdarzeń WNF	265
Diagnostyka w trybie użytkownika	266
Obsługa jądra	266
Obsługa natywnych aplikacji	268
Obsługa podsystemu Windows	270
Aplikacje pakietowe	270
Aplikacje UWP	272
Aplikacje Centennial	273
Menedżer HAM	276
Repozytorium stanów	278
Minirepozytorium zależności	281
Zadania wykonywane w tle i infrastruktura brokerska	282
Konfigurowanie i uruchamianie aplikacji pakietowych	285
Aktywacja pakietu	285
Rejestracja pakietów	291
Podsumowanie	293

Rozdział 9. Technologie virtualizacji	295
Hipernadzorca systemu Windows	295
Partycje, procesy i wątki	297
Uruchamianie hipernadzorcy	303
Menedżer pamięci hipernadzorcy	309
Planiści platformy Hyper-V	317
Hiperwywołania i TLFS hipernadzorcy	329
Przechwyty	331
Syntetyczny kontroler przerwań (SynIC)	332
API platformy hipernadzorcy systemu Windows i partycje EXO	335
Wirtualizacja zagnieżdżona	338
Hipernadzorca Windows w procesorze ARM64	345
Stos wirtualizacji	347
Usługa menedżera maszyn wirtualnych i procesy robocze	347
Sterownik VID i menedżer pamięci stosu wirtualizacji	349
Narodziny maszyny wirtualnej (VM)	350
VMBus	356
Obsługa sprzętu wirtualnego	363
Maszyny wirtualne wspierane przez VA	370
Bezpieczeństwo oparte na wirtualizacji (VBS)	374
Wirtualne poziomy zaufania (VTL) i wirtualny tryb bezpieczny (VSM)	374
Usługi świadczone przez VSM i wymagania	377
Bezpieczne jądro	380
Wirtualne przerwania	381
Bezpieczne przechwyty	384
Wywołania systemowe wirtualnego trybu bezpiecznego VSM	385
Bezpieczne wątki i planowanie	392
Integralność kodu wymuszona przez hipernadzorcę	394
Wirtualizacja uruchomieniowa UEFI	394
Uruchamianie VSM	396
Menedżer pamięci bezpiecznego jądra	400
Łatanie „na gorąco”	405
Tryb izolowanego użytkownika	408
Tworzenie trustletów	409
Bezpieczne urządzenia	413
Enklawy oparte na VBS	415
Atestacja uruchomieniowa strażnika systemu	423
Podsumowanie	427
Rozdział 10. Zarządzanie, diagnostyka i śledzenie	429
Rejestr	429
Przeglądanie rejestru i zmiana jego ustawień	429
Używanie rejestru	430
Typy danych rejestru	431

Struktura logiczna rejestru	432
Gałęzie różnych aplikacji w rejestrze	441
Rejestr transakcyjny TxR (ang. Transactional Registry)	442
Monitorowanie aktywności rejestru	444
Wewnętrzne mechanizmy monitora procesów	444
Wewnętrzne mechanizmy rejestru	446
Reorganizacja gałęzi rejestru	455
Obszar nazw rejestru oraz działanie rejestru	456
Stabilne przechowywanie	459
Filtrowanie rejestru	463
Wirtualizacja rejestru	464
Optymalizacje rejestru	467
Usługi Windows	468
Aplikacje działające jako usługi	468
Konta usług	476
Menedżer kontrolny usługi (SCM)	492
Programy kontrolne usług	496
Uruchamianie usług typu autostart	497
Usługi typu autostart uruchamiane z opóźnieniem	504
Usługi uruchamiane przez wyzwalacze	504
Błędy uruchamiania	506
Akceptowanie rozruchowej i ostatniej znanej dobrej konfiguracji	507
Usterki usług	509
Wylączanie usług	511
Współdzielone procesy usług	512
Znaczniki usług	516
Usługi użytkownika	516
Usługi pakietowe	520
Usługi chronione	521
Planowanie zadań i menedżer UBPM	523
Harmonogram zadań	523
Zunifikowany menedżer procesów działających w tle (UBPM)	529
Interfejsy COM Harmonogramu zadań	534
Instrumentacja zarządzania Windows (WMI)	534
Architektura Instrumentacji zarządzania systemem Windows WMI	534
Dostawcy WMI	536
Model CIM i język MOF	537
Asocjacja klas	541
Implementacja usługi WMI	543
Zabezpieczenia WMI	545
Śledzenie zdarzeń w systemie Windows (ETW)	546
Inicjalizacja usługi ETW	548
Sesje usługi ETW	550

Dostawcy usługi ETW	554
Dostarczanie zdarzeń	557
Wątek rejestratora usługi ETW	558
Konsumowanie zdarzeń	560
Rejestratory systemowe	563
Zabezpieczenia usługi ETW	570
Śledzenie dynamiczne (DTrace)	574
Architektura wewnętrzna	577
Biblioteka typów platformy DTrace	584
Raportowanie błędów w systemie Windows (WER)	585
Awaryjne aplikacje użytkownika	587
Awaryjne w trybie jądra (awaryjne systemu)	594
Wykrywanie zawieszania się procesów	603
Flagi globalne	605
Biblioteki shim jądra	609
Inicjalizacja silnika bibliotek shim	609
Baza danych bibliotek shim	612
Biblioteki shim sterowników	613
Biblioteki shim urządzeń	616
Podsumowanie	617
Rozdział 11. Buforowanie i systemy plików	619
Terminologia	619
Podstawowe funkcje menedżera bufora	620
Scentralizowany bufor	621
Zarządzanie pamięcią	621
Spójny bufor	622
Buforowanie bloków wirtualnych	623
Buforowanie strumieni	623
Obsługa odtwarzalnych systemów plików	624
Rozszerzone zestawy robocze NTFS MFT	625
Obsługa partycji pamięci	625
Zarządzanie wirtualną pamięcią bufora	626
Wielkość bufora	627
Wirtualny rozmiar bufora	628
Wielkość zestawu roboczego	628
Fizyczny rozmiar bufora	628
Struktury bufora	630
Ogólnosystemowe struktury bufora	630
Indywidualne plikowe struktury danych	633
Interfejsy systemu plików	635
Kopiowanie danych z i do bufora	637
Buforowanie za pomocą funkcji mapujących i przypinających	637
Buforowanie za pomocą funkcji bezpośredniego dostępu do pamięci	638

Szybkie operacje wejścia/wyjścia	638
Odczytywanie danych z wyprzedzeniem i zapisywanie z opóźnieniem	640
Inteligentny odczyt z wyprzedzeniem	641
Usprawnienia odczytu z wyprzedzeniem	642
Buforowanie zapisu zwrotnego i zapis z opóźnieniem	643
Wyłączenie zapisu z opóźnieniem	648
Wymuszenie zapisu bufora na dysku	648
Zapis zmapowanych plików	649
Dławienie zapisów	650
Wątki systemowe	651
Zapis agresywny i zapis o niskim priorytecie	651
Pamięć dynamiczna	652
Rejestrowanie operacji wejścia/wyjścia menedżera bufora	653
Systemy plików	655
Systemy plików w systemie Windows	655
CDFS	655
UDF	655
FAT12, FAT16 i FAT32	656
exFAT	659
NTFS	660
ReFS	661
Architektura sterownika systemu plików	661
Lokalne sterowniki systemu plików	662
Zewnętrzne sterowniki systemu plików	663
Operacje w systemie plików	670
Jawne operacje wejścia/wyjścia na plikach	671
Moduł menedżera pamięci zapisujący zmodyfikowane i zmapowane strony	674
Moduł menedżera bufora zapisujący z opóźnieniem	674
Moduł menedżera bufora odczytujący z wyprzedzeniem	674
Moduł menedżera pamięci obsługujący błędy stron	675
Sterowniki filtrów systemu plików i minifiltry	675
Filtrowanie nazwanych potoków i slotów pocztowych	677
Kontrola plików ponownej analizy	677
Process Monitor	678
System NTFS	680
Ogólne wymagania	680
Odtwarzalność	680
Bezpieczeństwo	681
Nadmiarowość danych i odporność na błędy	681
Zaawansowane funkcjonalności	682
Wiele strumieni danych	682
Nazwy w formacie Unicode	684
Uniwersalne indeksowanie	684

Dynamiczne mapowanie uszkodzonych klastrów	685
Twarde dowiązania	685
Symboliczne (miękkie) dowiązania i złącza	686
Kompresja i pliki rozrzedzone	688
Rejestrowanie zmian	688
Indywidualne przydziały użytkowników	689
Śledzenie dowiązań	690
Szyfrowanie	690
Obsługa podsystemu POSIX	691
Defragmentacja	693
Dynamiczne partycjonowanie	696
Obsługa woluminów warstwowych	697
Sterownik systemu plików NTFS	701
Struktura NTFS na dysku	704
Woluminy	704
Klastry	705
Tablica MFT	705
Numery rekordów plików	709
Rekordy plików	709
Nazwy plików	713
Tunelowanie	715
Atrybuty rezydentne i nierezydentne	716
Kompresja i pliki rozrzedzone	719
Kompresja rozrzedzonych danych	719
Kompresja nierozrzedzonych danych	721
Pliki rozrzedzone	723
Plik dziennika zmian	723
Indeksowanie	727
Identyfikatory obiektów	728
Śledzenie przydziałów	729
Skonsolidowane zabezpieczenia	730
Punkty ponownej analizy	732
Rezerwy magazynu i rezerwacje	733
Obsługa transakcji	736
Izolacja	737
Funkcje transakcyjne	737
Implementacja dyskowa	738
Implementacja dziennika	740
Odzyskiwanie plików w systemie NTFS	741
Projekt	741
Rejestrowanie metadanych	742
Usługa LFS	742
Rodzaje rekordów dziennika	744

Odzyskiwanie	746
Przebieg analizy	747
Przebieg ponowienia transakcji	748
Przebieg wycofania transakcji	748
Odzyskiwanie uszkodzonych klastrów	750
Samonaprawa	754
Sprawdzanie podłączonego dysku i szybka naprawa	755
Szyfrowany system plików	757
Pierwsze szyfrowanie pliku	760
Proces deszyfrowania	762
Tworzenie kopii zapasowych zaszyfrowanych plików	763
Kopiowanie zaszyfrowanych plików	764
Odciążenie szyfrowania BitLocker	764
Szyfrowanie plików online	765
Dyski DAX	767
Model sterownika DAX	768
Woluminy DAX	769
Buforowane i niebuforowane operacje wejścia/wyjścia na woluminach DAX	770
Mapowanie wykonywalnych obrazów	771
Woluminy blokowe	775
Sterowniki filtrów systemu plików i woluminy DAX	776
Operacje buforowane i niebuforowane	777
Obsługa dużych i olbrzymich stron	778
Obsługa wirtualnych dysków PM i przestrzeni dyskowych	782
System ReFS	785
Architektura silnika Minstore	786
Fizyczny układ drzewa B+	788
Alokatory	789
Tablica stron	790
Operacje wejścia/wyjścia silnika Minstore	791
Architektura systemu	793
Dyskowe struktury danych	796
Identyfikatory obiektów	797
Bezpieczeństwo i dziennik zmian	798
Zaawansowane funkcjonalności systemu ReFS	799
Klonowanie bloków pliku (obsługa migawek)	799
Zapis w locie	802
Odzyskiwanie danych	803
Wykrywanie wycieków klastrów	805
Woluminy SMR	807
Obsługa woluminów warstwowych i SMR	808
Scalanie kontenerów	810
Pliki skompresowane i porzucone	813

Storage Spaces	814
Wewnętrzna architektura	815
Usługi Storage Spaces	816
Podsumowanie	820
Rozdział 12. Uruchamianie i zamykanie systemu	821
Proces rozruchu	821
Rozruch UEFI	822
Proces rozruchu BIOS	826
Bezpieczny rozruch	826
Menedżer rozruchu systemu Windows	829
Menu rozruchowe	847
Uruchomienie programu rozruchowego	848
Mierzony rozruch	850
Zaufane uruchamianie systemu	853
Program ładujący system Windows	856
Rozruch systemu za pomocą urządzenia iSCSI	859
Moduł ładujący hipernadzorcę	860
Zasada przejścia w tryb VSM	861
Bezpieczne uruchamianie	864
Inicjalizacja jądra i podsystemów wykonawczych	866
Faza nr 1 inicjalizacji jądra	872
Procesy smss.exe, csrss.exe i wininit.exe	877
ReadyBoot	882
Obrazy uruchamiane automatycznie	884
Zamknięcie systemu	884
Hibernacja i szybkie uruchamianie	887
Środowisko WinRE	891
Tryb awaryjny	893
Ładowanie sterowników w trybie awaryjnym	895
Programy użytkownika uwzględniające tryb awaryjny	896
Plik stanu rozruchu	897
Podsumowanie	897
Skorowidz	898