

Windows od środka

Architektura systemu, procesy,
wątki, zarządzanie pamięcią
i dużo więcej

Wydanie VII

Professional



Pavel Yosifovich
Alex Ionescu
Mark E. Russinovich
David A. Solomon

Tytuł oryginału: Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (7th Edition)

Tłumaczenie: Piotr Pilch (wstęp, rozdz. 1, 3, 4, 6), Zbigniew Waśko (rozdz. 2, 5, 7)

ISBN: 978-83-8322-554-8

Authorized translation from the English language edition, entitled: WINDOWS INTERNALS, PART 1: SYSTEM ARCHITECTURE, PROCESSES, THREADS, MEMORY MANAGEMENT, AND MORE, Seventh Edition; ISBN 0735684189; by Pavel Yosifovich; and by Alex Ionescu; and by Mark E. Russinovich; and David A. Solomon; published by Pearson Education, Inc, publishing as Microsoft Press. Copyright © 2017 by Pavel Yosifovich, Alex Ionescu, Mark E. Russinovich and David A. Solomon

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

Polish language edition published by Helion S.A. Copyright © 2018, 2023.

Microsoft and the trademarks listed at <https://www.microsoft.com> on the “Trademarks” webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Helion S.A.

ul. Kościuszki 1c, 44-100 Gliwice

tel. 32 230 98 63

e-mail: helion@helion.pl

WWW: <https://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<https://helion.pl/user/opinie/wino7v>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Pliki z przykładami omawianymi w książce można znaleźć pod adresem:

<https://ftp.helion.pl/przyklady/wino7v.zip>

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

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
	Wieloprocessorowość 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 SwitchBack	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 beczynności	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 scalonych	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 SuperFetch)	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

ROZDZIAŁ 1.

Zagadnienia i narzędzia

W rozdziale zostaną zaprezentowane zagadnienia i terminy związane z systemem operacyjnym Microsoft Windows, które będą wykorzystywane w książce, takie jak interfejs API systemu Windows, procesy, wątki, pamięć wirtualna, tryb jądra i tryb użytkownika, obiekty, dojścia, zabezpieczenia i rejestr. Zostaną również przedstawione narzędzia, których możesz użyć do poznawania wewnętrznych mechanizmów systemu Windows, takie jak debugger jądra, Monitor wydajności oraz kluczowe narzędzia oferowane przez witrynę Windows Sysinternals (<http://www.microsoft.com/technet/sysinternals>). Poza tym wyjaśnimy, jak zastosować zestawy Windows Driver Kit (WDK) oraz Windows Software Development Kit (SDK) w roli zasobów służących do znajdowania dodatkowych informacji o wewnętrznych mechanizmach systemu Windows.

Zadbaj o zrozumienie wszystkiego, co zaprezentowano w tym rozdziale, ponieważ w przypadku reszty książki założono, że tak będzie.

Wersje systemu operacyjnego Windows

W książce omówiono najnowsze wersje systemów operacyjnych Microsoft Windows przeznaczonych dla klientów i serwerów, a mianowicie system Windows 10 (wersja 32-bitowa dla procesorów x86 i ARM oraz wersja 64-bitowa dla procesorów x64) oraz system Windows Server 2012 R2 (dostępny tylko w wersji 64-bitowej). Jeśli nie zostało to wyraźnie określone, treść książki dotyczy wszystkich tych wersji. W roli podstawowych informacji w tabeli 1.1 wyszczególniono nazwy systemów Windows wraz z numerem wewnętrznym ich wersji oraz datą opublikowania.

Począwszy od systemu Windows 7, numery wersji wydają się schodzić z dobrze zdefiniowanej drogi. W jego przypadku numer wersji to 6.1, a nie 7. Gdy w momencie pojawienia się systemu Windows Vista numer wersji podniesiono na 6.0, z powodu popularności systemu Windows XP niektóre aplikacje nie były w stanie wykryć poprawnego systemu operacyjnego, ponieważ projektanci zastosowali sprawdzanie głównego numeru większego lub równego 5 oraz dodatkowego numeru większego lub równego 1, co w przypadku systemu Windows Vista nie było spełnione. Wyciągając z tego lekcję, w celu zminimalizowania takich niezgodności firma Microsoft zdecydowała się określić główny numer wersji jako 6 oraz dodatkowy numer wersji jako 2 (większe niż 1). W wypadku systemu Windows 10 numer wersji został jednak uaktualniony do 10.0.

TABELA 1.1. Wersje systemu operacyjnego Windows

Nazwa produktu	Numer wewnętrzny wersji	Data opublikowania
Windows NT 3.1	3.1	Lipiec 1993 r.
Windows NT 3.5	3.5	Wrzesień 1994 r.
Windows NT 3.51	3.51	Maj 1995 r.
Windows NT 4.0	4.0	Lipiec 1996 r.
Windows 2000	5.0	Grudzień 1999 r.
Windows XP	5.1	Sierpień 2001 r.
Windows Server 2003	5.2	Marzec 2003 r.
Windows Server 2003 R2	5.2	Grudzień 2005 r.
Windows Vista	6.0	Styczeń 2007 r.
Windows Server 2008	6.0 (Service Pack 1)	Marzec 2008 r.
Windows 7	6.1	Październik 2009 r.
Windows Server 2008 R2	6.1	Październik 2009 r.
Windows 8	6.2	Październik 2012 r.
Windows Server 2012	6.2	Październik 2012 r.
Windows 8.1	6.3	Październik 2013 r.
Windows Server 2012 R2	6.3	Październik 2013 r.
Windows 10	10.0 (kompilacja 10240)	Lipiec 2015 r.
Windows 10 version 1511	10.0 (kompilacja 10586)	Listopad 2015 r.
Windows 10 version 1607 (Anniversary Update)	10.0 (kompilacja 14393)	Lipiec 2016 r.
Windows Server 2016	10.0 (kompilacja 14393)	Październik 2016 r.



Uwaga. Począwszy od systemu Windows 8, funkcja `API GetVersionEx` systemu Windows zwraca domyślnie jego numer wersji jako 6.2 (Windows 8) niezależnie od faktycznie używanego systemu operacyjnego (funkcja ta jest też określona jako niezalecana). Ma to na celu zminimalizowanie problemów ze zgodnością, ale również jest to wskaźnik, że w większości sytuacji sprawdzanie wersji systemu nie jest najlepszym rozwiązaniem. Wynika to z tego, że niektóre komponenty mogą być instalowane niestandardowo bez zgodności z oficjalną wersją systemu Windows. Jeśli jednak wymagasz informacji o faktycznej wersji systemu operacyjnego, możesz ją uzyskać za pomocą funkcji `Veri fyVers ionInfo` lub nowszych pomocniczych interfejsów API wersji, takich jak `IsWindows80rGreater`, `IsWindows8Point10rGreater`, `IsWindows100rGreater` i `IsWindowsServer` oraz innych podobnych. Dodatkowo zgodność z systemem operacyjnym może zostać wskazana w manifeście pliku wykonywalnego, co powoduje zmianę wyników działania funkcji `Veri fyVers ionInfo`.

Informacje o wersji systemu Windows możesz wyświetlić za pomocą narzędzia `ver` działającego w trybie wiersza poleceń lub przy użyciu narzędzia `winver` z interfejsem graficznym. Poniżej zaprezentowano zrzut ekranu narzędzia `winver` uruchomionego w systemie Windows 10 Home (wersja 1607).



Powyższe okno zawiera też numer kompilacji systemu Windows (w przykładzie 14393.1358), który może być przydatny dla uczestników programu Windows Insider (osób, które zarejestrowały się w celu uzyskania możliwości zaznajomienia się z wcześniejszymi wersjami testowymi systemu Windows). Numer kompilacji może być też pomocny przy zarządzaniu aktualizacjami zabezpieczeń, ponieważ informuje o tym, jaki zainstalowano poziom poprawek.

Windows 10 i przyszłe wersje systemu Windows

W przypadku systemu Windows 10 firma Microsoft zadeklarowała, że będzie aktualizować system Windows szybciej, niż następowało to wcześniej. Nie pojawi się oficjalnie Windows 11. Zamiast tego w ramach usługi Windows Update (lub innego modelu usług dla przedsiębiorstw) istniejący system Windows 10 zostanie zaktualizowany do nowszej wersji. Gdy pisano książkę, nastąpiły dwie takie aktualizacje: w listopadzie 2015 r. (aktualizacja znana jako *wersja 1511*, odwołująca się do roku i miesiąca udostępnienia) oraz w lipcu 2016 r. (*wersja 1607*, która jest znana również pod marketingową nazwą *Anniversary Update*).



Uwaga. Wewnętrznie firma Microsoft w dalszym ciągu fałowo tworzy wersje systemu Windows. Na przykład początkowa wersja systemu Windows 10 miała nazwę kodową *Threshold 1*, natomiast aktualizacja z listopada 2015 r. nosiła nazwę *Threshold 2*. Trzy kolejne fazy aktualizacji mają nazwy *Redstone 1* (wersja 1607), *Redstone 2* i *Redstone 3*.

Windows 10 i platforma OneCore

Przez lata zostało rozwiniętych kilka wariantów systemu Windows. Oprócz najpopularniejszego systemu Windows działającego na komputerach PC, dostępna jest konsola do gier Xbox 360 z odmianą systemu Windows 2000. Urządzenie Windows Phone 7 wyposażone jest w wariant oparty na systemie Windows CE (system operacyjny czasu rzeczywistego firmy Microsoft). Utrzymywanie i rozszerzanie wszystkich tych baz kodu jest oczywiście utrudnione. W związku z tym firma Microsoft zdecydowała się na połączenie w jedno jąder oraz pomocniczych plików binarnych podstawowej platformy. Proces ten rozpoczął się w przypadku systemów Windows 8 i Windows Phone 8, które korzystają ze wspólnego jądra (systemy Windows 8.1 i Windows Phone 8.1 mają jednakowy interfejs API środowiska uruchomieniowego systemu Windows). Proces łączenia zakończono w systemie Windows 10. Uzyskana wspólna platforma nosi nazwę OneCore. Działa ona na komputerach PC, telefonach, konsoli do gier Xbox One oraz na urządzeniach HoloLens i Internet of Things (IoT), takich jak Raspberry Pi 2.

Oczywiście wszystkie te rodzaje urządzeń różnią się znacząco od siebie. W wypadku części z nich niektóre funkcje są po prostu niedostępne. Na przykład obsługa myszy lub fizycznej klawiatury w przypadku urządzenia HoloLens nie ma sensu, dlatego nie możesz oczekiwać obecności odpowiednich komponentów w wersji systemu Windows 10 przeznaczonej dla tego urządzenia. Jednakże jądro, sterowniki i binaria podstawowej platformy są zasadniczo takie same (wraz z ustawieniami opartymi na rejestrze i/lub zasadach, które mają sens ze względu na wydajność lub z innych powodów). Tego rodzaju przykładowa zasada zostanie zaprezentowana w punkcie „Mechanizm API Sets” rozdziału 3., „Procesy i zadania”.

W książce obszernie omówiono wewnętrzne mechanizmy jądra platformy OneCore, niezależnie od tego, na jakim urządzeniu działa. Eksperymenty opisane w książce koncentrują się jednak na komputerze stacjonarnym wyposażonym w mysz i klawiaturę (głównie ze względu na wygodę), ponieważ nie jest łatwe (a czasami oficjalnie niemożliwe) przeprowadzenie doświadczeń w przypadku innych urządzeń, takich jak telefony lub konsola Xbox One.

Podstawowe pojęcia i terminy

W poniższych punktach dokonano wprowadzenia do najbardziej fundamentalnych pojęć obecnych w systemie Windows, które mają kluczowe znaczenie dla zagadnień omówionych w pozostałej części książki. Wiele pojęć, takich jak procesy, wątki i pamięć wirtualna, objaśniono szczegółowo w kolejnych rozdziałach.

Interfejs API systemu Windows

Interfejs programowania aplikacji API (ang. *Application Programming Interface*) systemu Windows to systemowy interfejs programowania trybu użytkownika zapewniający dostęp do rodziny systemów operacyjnych Windows. Przed wprowadzeniem 64-bitowych wersji systemu Windows interfejs programowania 32-bitowych wersji tego systemu nosił nazwę *Win32 API*, aby odróżnić go od oryginalnego 16-bitowego interfejsu API systemu Windows, który był interfejsem programowania pierwotnych 16-bitowych wersji systemu Windows. W książce termin *interfejs API systemu Windows* odnosi się zarówno do 32-bitowych, jak i 64-bitowych interfejsów programowania.



Uwaga. Czasami w miejsce terminu *interfejs API systemu Windows* używamy terminu *Win32 API*. Oba terminy odnoszą się jednak do wariantów 32- i 64-bitowych.



Uwaga. Interfejs API systemu Windows opisano w dokumentacji zestawu SDK systemu Windows (zajrzyj do punktu „Windows Software Development Kit” zamieszczonego w dalszej części rozdziału). Dokumentacja jest dostępna bezpłatnie pod adresem <https://developer.microsoft.com/en-us/windows/desktop/develop>. Dołączono ją również do wszystkich poziomów subskrypcji w portalu Microsoft Developer Network (MSDN), z którym związany jest program wsparcia projektantów aplikacji. Znakomity opis tego, jak utworzyć podstawowy interfejs API systemu Windows, zamieszczono w książce *Windows via C/C++. Fifth Edition* napisanej przez Jeffreya Richtera i Christophe’a Nasarre’a (Microsoft Press, 2007 r.).

Warianty interfejsu API systemu Windows

Pierwotnie interfejs API systemu Windows składał się wyłącznie z funkcji napisanych w stylu języka C. Obecnie projektanci mogą skorzystać z tysięcy takich funkcji. Język C był naturalnym wyborem w początkach istnienia systemu Windows, ponieważ stanowił najmniejszy wspólny mianownik (oznacza to, że kod napisany w tym języku był dostępny również z poziomu innych języków), a ponadto był na tyle niskopoziomowy, aby udostępniać usługi systemu operacyjnego. Wadą była niewielka liczba funkcji oraz brak spójności nazewniczej i logicznego grupowania (na przykład przestrzenie nazw w języku C++). Rezultatem tych trudności było utworzenie kilku nowszych interfejsów API korzystających z innego mechanizmu API, czyli modelu COM (ang. *Component Object Model*).

Model COM został pierwotnie zaprojektowany w celu umożliwienia aplikacjom pakietu Microsoft Office komunikacji i wymiany danych między dokumentami (na przykład osadzanie wykresu Excela w dokumencie Worda lub prezentacji programu PowerPoint). Taka możliwość nosi nazwę funkcji OLE (ang. *Object Linking and Embedding*). Oryginalnie funkcja ta została zaimplementowana za pomocą starego mechanizmu przesyłania komunikatów systemu Windows o nazwie *Dynamic Data Exchange* (DDE). Mechanizm ten z natury był ograniczony, dlatego opracowano nową metodę komunikacji, czyli model COM. Tak naprawdę, początkowo w momencie opublikowania około 1993 r. miał on nazwę OLE 2.

Model COM oparty jest na dwóch podstawowych zasadach. Po pierwsze, klienci komunikują się z obiektami (czasami nazywanymi obiektami serwerowymi COM) za pośrednictwem interfejsów, czyli odpowiednio zdefiniowanych kontraktów z zestawem logicznie powiązanych metod grupowanych w ramach mechanizmu rozsyłania tabeli wirtualnej, który w wypadku kompilatorów języka C++ stanowi też typowy sposób implementowania rozsyłania funkcji wirtualnych. Efektem tego jest zgodność binarna oraz usunięcie problemów z przekłamywaniem nazw kompilatora. W konsekwencji możliwe jest wywołanie tych metod w wielu językach (i kompilatorach), takich jak C, C++, Visual Basic, .NET, Delphi oraz innych. Po drugie, implementacja komponentów ładowana jest dynamicznie zamiast statycznego powiązania jej z klientem.

Termin *serwer modelu COM* odnosi się zwykle do biblioteki Dynamic Link Library (DLL) lub pliku wykonywalnego (EXE), gdzie implementowane są klasy modelu COM. Model ten oferuje inne ważne funkcje powiązane z zabezpieczeniami, marshallingiem realizowanym między procesami,

modelem wątkowości itp. Obszerne omówienie modelu COM wykracza poza zakres książki. Znakomitą prezentację tego modelu można znaleźć w książce *Essential COM* autorstwa Dona Boxa (Addison-Wesley, 1998 r.).



Uwaga. Przykłady interfejsów API dostępnych za pośrednictwem modelu COM obejmują DirectShow, Windows Media Foundation, DirectX, DirectComposition, Windows Imaging Component (WIC) oraz Background Intelligent Transfer Service (BITS).

Architektura Windows Runtime

W systemie Windows 8 wprowadzono nowy interfejs API oraz wspierające środowisko uruchomieniowe o nazwie *Windows Runtime* (określane czasem za pomocą skrótu *WinRT*, którego nie należy mylić z wycofaną wersją Windows RT systemu operacyjnego Windows opartego na architekturze ARM). Architektura Windows Runtime składa się z usług platformy kierowanych szczególnie do projektantów tak zwanych aplikacji *Windows Apps* (znanych wcześniej pod nazwami *Metro Apps*, *Modern Apps*, *Immersive Apps* i *Windows Store Apps*). Aplikacje Windows Apps mogą być przeznaczone dla wielu wariantów urządzeń, począwszy od niewielkich urządzeń IoT i telefonów, a skończywszy na tabletach, laptopach i komputerach stacjonarnych, a nawet takich urządzeniach, jak konsola Xbox One i Microsoft HoloLens.

Z perspektywy interfejsu API architektura WinRT zbudowana jest na bazie modelu COM, poszerzając jego podstawową infrastrukturę o różne rozszerzenia. Na przykład w architekturze tej dostępne są kompletne metadane typów (przechowywane w plikach WINMD oraz oparte na formacie metadanych środowiska .NET), które rozszerzają podobne pojęcie obecne w modelu COM znane jako biblioteki typów. Z punktu widzenia projektu interfejsów API architektura WinRT jest znacznie bardziej spójna niż klasyczne funkcje API systemu Windows, oferując hierarchie przestrzeni nazw, jednolite nazewnictwo oraz wzorce programistyczne.

W przeciwieństwie do zwykłych aplikacji systemu Windows (nazywanych obecnie *aplikacjami dla komputerów stacjonarnych z systemem Windows* lub *klasycznymi aplikacjami systemu Windows*), aplikacje Windows Apps podlegają nowym regułom.

Relacja między różnymi interfejsami API i aplikacjami nie jest bezpośrednia. Aplikacje dla komputerów stacjonarnych mogą korzystać z podzbioru interfejsów API architektury WinRT. Z kolei aplikacje Windows Apps mogą używać podzbioru interfejsów API architektury Win32 i modelu COM. W dokumentacji portalu MSDN znajdziesz szczegóły dotyczące tego, jakie interfejsy API są dostępne z poziomu każdej platformy aplikacji. Zauważ jednak, że na podstawowym poziomie binarnym interfejs API architektury WinRT w dalszym ciągu bazuje na starszych binariach i interfejsach API systemu Windows, nawet pomimo tego, że dostępność określonych interfejsów API może nie być udokumentowana lub wspierana. Nie jest to nowy natywny interfejs API systemu, lecz podobnie jak w przypadku środowiska .NET, nadal korzysta on z tradycyjnego interfejsu API systemu Windows.

Aplikacje napisane w językach C++, C# (lub innych językach .NET) oraz JavaScript mogą z łatwością stosować interfejsy API architektury WinRT, co zawdzięczają projekcom językowym opracowanym z myślą o tej architekturze. W wypadku języka C++ firma Microsoft utworzyła niestandardowe rozszerzenie o nazwie C++/CX, które upraszcza korzystanie z typów architektury WinRT. Zwykła warstwa współdziałania modelu COM przeznaczona dla środowiska .NET (z kilkoma wspierającymi rozszerzeniami uruchomieniowymi) umożliwia dowolnemu językowi .NET

zastosowanie interfejsów API architektury WinRT w naturalny i prosty sposób, tak jakby to było czyste środowisko .NET. Z myślą o projektantach używających języka JavaScript opracowano rozszerzenie *WinJS* zapewniające dostęp do architektury WinRT, choć nadal muszą oni używać kodu HTML do budowania interfejsu użytkownika aplikacji.



Uwaga. Nawet pomimo tego, że kod HTML może być używany w aplikacjach Windows Apps, w dalszym ciągu ma on postać lokalnej aplikacji klienckiej, a nie aplikacji internetowej uzyskiwanej z serwera WWW.

Środowisko .NET Framework

Środowisko .NET Framework stanowi część systemu Windows. W tabeli 1.2 podano informacje o wersji tego środowiska zainstalowanego jako część danej wersji systemu Windows. Nowsza wersja środowiska może zostać jednak zainstalowana w nowszych wersjach systemu operacyjnego.

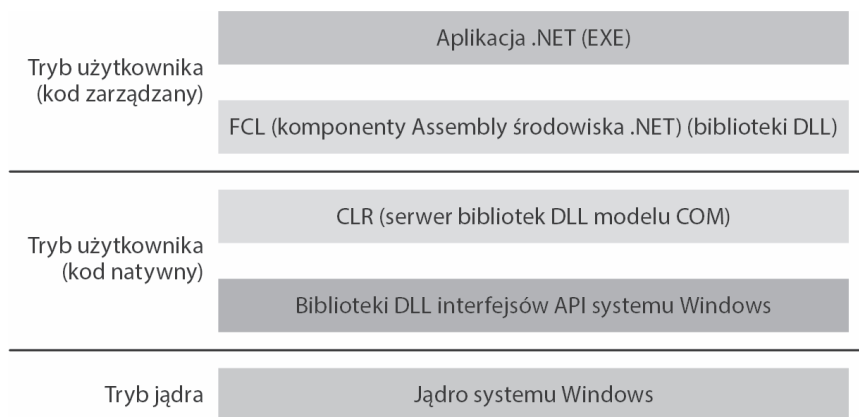
TABELA 1.2. Domyślne instalacje środowiska .NET Framework w systemie Windows

Wersja systemu Windows	Wersja środowiska .NET Framework
Windows 8	4.5
Windows 8.1	4.5.1
Windows 10	4.6
Windows 10 (wersja 1511)	4.6.1
Windows 10 (wersja 1607)	4.6.2

Środowisko .NET Framework złożone jest z następujących dwóch podstawowych komponentów:

- **Common Language Runtime (CLR).** Jest to mechanizm uruchomieniowy środowiska .NET, który obejmuje kompilator Just In Time (JIT) dokonujący translacji instrukcji CIL (ang. *Common Intermediate Language*) na język maszynowy bazowego procesora sprzętowego, a także zarządcę „odśmiecania” pamięci, weryfikowanie typów, zabezpieczenia dostępu do kodu itp. Mechanizm implementowany jest jako serwer wewnątrzprocesowy modelu COM (biblioteka DLL), a ponadto korzysta z różnych rozwiązań zapewnianych przez interfejs API systemu Windows.
- **.NET Framework Class Library (FCL).** Jest to duża kolekcja typów implementujących funkcjonalność, która jest zwykle wymagana przez aplikacje klienta i serwera, taką jak usługi interfejsu użytkownika, obsługa sieci, dostęp do bazy danych itp.

Oferując takie oraz inne elementy, w tym nowe języki programowania wysokiego poziomu (C#, Visual Basic, F#) oraz narzędzia wspierające, środowisko .NET Framework poprawia efektywność pracy projektanta, a ponadto zwiększa bezpieczeństwo i niezawodność w obrębie aplikacji opartych na tym środowisku. Na rysunku 1.1 pokazano relację między środowiskiem .NET Framework i systemem operacyjnym.



RYSUNEK 1.1. Diagram prezentuje relację między środowiskiem .NET i systemem operacyjnym Windows

Usługi, funkcje i programy

Kilka terminów w dokumentacji programisty i użytkownika systemu Windows ma odmienne znaczenie w różnych kontekstach. Na przykład termin *usługa* może odwoływać się do umożliwiającego wywołanie programu w systemie operacyjnym, sterownika urządzenia lub procesu serwerowego. Następująca lista pozwala się zorientować, jakie znaczenie w książce mają określone terminy:

- **Funkcje interfejsu API systemu Windows.** Są to udokumentowane podprogramy w interfejsie API systemu Windows umożliwiające wywołanie. Przykładowe funkcje obejmują `CreateProcess`, `CreateFile` i `SendMessage`.
- **Natywne usługi systemowe (lub wywołania systemowe).** Są to nieudokumentowane usługi bazowe w systemie operacyjnym, które mogą być wywoływane w trybie użytkownika. Na przykład usługa `NtCreateUserProcess` to wewnętrzna usługa systemowa, jaką wywołuje funkcja `CreateProcess` systemu Windows w celu utworzenia nowego procesu.
- **Funkcje obsługi jądra (lub programy).** Są to podprogramy wewnątrz systemu operacyjnego Windows, które mogą być wywoływane tylko w trybie jądra (zostanie zdefiniowany w dalszej części rozdziału). Na przykład `ExAllocatePoolWithTag` to program wywoływany przez sterowniki urządzeń w celu przydziału pamięci ze stert systemu Windows (nazywanych *pulami*).
- **Usługi systemu Windows.** Są to procesy uruchamiane przez menedżer sterowania usługami systemu Windows. Na przykład usługa Harmonogram zadań działa w obrębie procesu trybu użytkownika, który obsługuje polecenie `schtasks` (podobne do poleceń `at` i `cron` systemu UNIX). Zauważ, że choć w rejestrze sterowniki urządzeń systemu Windows są definiowane jako „usługi”, w książce nie są one postrzegane w ten sposób.
- **Biblioteki DLL (ang. *Dynamic Link Library*).** Są to umożliwiające wywołanie podprogramy połączone razem jako plik binarny, który może być dynamicznie ładowany przez aplikację korzystającą z podprogramów. Przykłady takich bibliotek obejmują biblioteki `Msvcrt.dll` (biblioteka uruchomieniowa języka C) i `Kernel32.dll` (jedna z bibliotek podsystemu interfejsu API systemu Windows). Komponenty

i aplikacje trybu użytkownika systemu Windows intensywnie używają bibliotek DLL. W porównaniu z bibliotekami statycznymi biblioteki DLL oferują korzyść polegającą na tym, że aplikacje mogą je współużytkować, a system Windows zapewnia, że w przypadku aplikacji odwołujących się do kodu biblioteki DLL w pamięci znajduje się tylko jedna jego kopia. Zauważ, że komponenty Assembly środowiska .NET bibliotek są kompilowane jako biblioteki DLL, lecz bez żadnych niezarządzanych, wyeksportowanych podprogramów. Zamiast tego w celu uzyskania dostępu do odpowiednich typów i elementów członkowskich mechanizm CLR dokonuje analizy skompilowanych metadanych.

Procesy

Choć na pierwszy rzut oka programy i procesy wyglądają podobnie, fundamentalnie się różnią. *Program* to statyczna sekwencja instrukcji, natomiast *proces* to kontener zestawu zasobów używanych podczas wykonywania instancji programu. Na najwyższym poziomie abstrakcji proces systemu Windows składa się z następujących elementów:

- **Prywatny obszar adresów wirtualnych.** Jest to zestaw adresów wirtualnych pamięci, jakie mogą zostać użyte przez proces.
- **Program wykonywalny.** Termin ten definiuje początkowy kod i dane odwzorowywane na obszar adresów wirtualnych procesu.
- **Lista otwartych dojsć.** Dojścia dokonują odwzorowania na różne zasoby systemowe, takie jak semaforey, obiekty synchronizacji oraz pliki dostępne dla wszystkich wątków w procesie.
- **Kontekst zabezpieczeń.** Jest to *token dostępu* identyfikujący użytkownika, grupy zabezpieczeń, przywileje, atrybuty, oświadczenia, możliwości, stan wirtualizacji UAC (ang. *User Account Control*), sesję oraz stan ograniczonego konta użytkownika skojarzonego z procesem, a także identyfikator *AppContainer* i powiązane z nim informacje dotyczące „piaskownicy”.
- **Identyfikator procesu.** Unikatowy identyfikator, który wewnętrznie stanowi część identyfikatora nazywanego *identyfikatorem klienta*.
- **Co najmniej jeden wątek wykonywania.** Choć „pusty” proces jest możliwy, nie jest przydatny (przeważnie).

Dostępnych jest wiele narzędzi służących do wyświetlania (i modyfikowania) procesów oraz informacji o nich. W zamieszczonych dalej eksperymentach przedstawiono różne widoki informacji o procesach, jakie możesz uzyskać za pomocą niektórych z tych narzędzi. Choć wiele spośród tych narzędzi wchodzi w skład samego systemu Windows, a także jest obecnych w zestawach *Debugging Tools for Windows* i *Windows SDK*, część narzędzi jest osobno dostępnych w portalu *Sysinternals*. Wiele z tych narzędzi prezentuje pokrywające się podzbiory informacji o podstawowych procesach i wątkach. Podzbiory te są czasami identyfikowane przez różne nazwy.

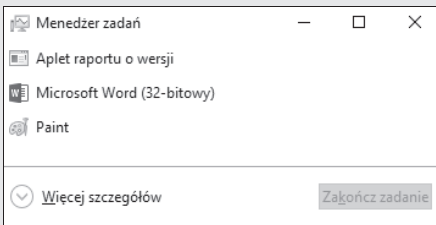
Menedżer zadań to prawdopodobnie najczęściej stosowane narzędzie do sprawdzania aktywności procesów (ponieważ w jądrze systemu Windows nie ma czegoś takiego jak „zadanie”, nazwa tego narzędzia jest trochę dziwna). W poniższym eksperymencie zaprezentowano niektóre z podstawowych funkcji Menedżera zadań.

EKSPERYMENT:**Wyświetlanie informacji o procesach za pomocą narzędzia Menedżer zadań**

Wbudowane narzędzie Menedżer zadań Windows zapewnia uproszczoną listę procesów systemowych. Narzędzie możesz uruchomić na jeden z następujących czterech sposobów:

- Użycie kombinacji klawiszy *Ctrl+Shift+Esc*.
- Kliknięcie paska zadań prawym przyciskiem myszy, a następnie kliknięcie pozycji *Menedżer zadań*.
- Użycie kombinacji klawiszy *Ctrl+Alt+Delete* i kliknięcie przycisku *Menedżer zadań*.
- Uruchomienie pliku wykonywalnego *Taskmgr.exe*.

Przy pierwszym uruchomieniu Menedżer zadań znajduje się w trybie mniejszej liczby szczegółów, w przypadku którego pokazane są wyłącznie procesy z widocznym oknem najwyższego poziomu. Prezentuje to poniższy zrzut ekranu.



W wyświetlonym oknie niewiele możesz zdziałać, dlatego kliknij przycisk rozszerzający *Więcej szczegółów*, aby aktywować pełny widok Menedżera zadań. Karta *Procesy* powinna być domyślnie wybrana.

Nazwa	5% Procesor CPU	38% Pamięć	2% Dysk	0% Sieć
Aplikacje (5)				
> Aplet raportu o wersji	0%	1,0 MB	0 MB/s	0 Mb/s
> Eksplorator Windows	0,4%	31,3 MB	0 MB/s	0,1 Mb/s
> Microsoft Word (32-bitowy)	0%	36,4 MB	0 MB/s	0 Mb/s
> Paint	0%	7,4 MB	0 MB/s	0 Mb/s
> Task Manager	1,2%	9,6 MB	0 MB/s	0 Mb/s
Procesy w tle (34)				
ACMON (32-bitowy)	0%	0,3 MB	0 MB/s	0 Mb/s
ASUS Color Engine (32-bitowy)	0%	0,3 MB	0 MB/s	0 Mb/s
ASUS Smart Gesture Center	0%	0,8 MB	0 MB/s	0 Mb/s
ASUS Smart Gesture Helper	0%	0,2 MB	0 MB/s	0 Mb/s
ASUS Smart Gesture Loader	0%	0,2 MB	0 MB/s	0 Mb/s
COM Surrogate	0%	1,5 MB	0 MB/s	0 Mb/s
Device Association Framework ...	0%	5,4 MB	0 MB/s	0 Mb/s

Karta *Procesy* zawiera listę procesów z następującymi czterema kolumnami: *Procesor CPU*, *Pamięć*, *Dysk* i *Sieć*. W celu wyświetlenia dodatkowych kolumn prawym przyciskiem myszy kliknij nagłówek widocznej kolumny. Dostępne kolumny to *Nazwa procesu*, *Identyfikator PID*, *Typ*, *Stan*, *Wydawca* i *Wiersz polecenia*. Niektóre procesy mogą być dodatkowo rozszerzone przez ukazanie widocznych okien najwyższego poziomu utworzonych przez proces.

Aby uzyskać jeszcze więcej szczegółów dotyczących procesów, kliknij kartę *Szczegóły*. Możesz też prawym przyciskiem myszy kliknąć proces i wybrać pozycję *Przejdź do szczegółów* w celu aktywowania karty *Szczegóły* i wybrania konkretnego procesu.

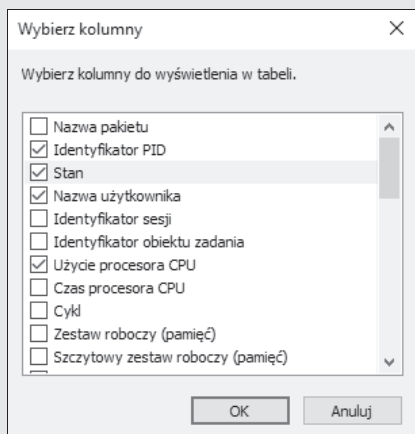


Uwaga. Karta *Procesy* Menedżera zadań systemu Windows 7 w przybliżeniu odpowiada zawartości karty *Szczegóły* Menedżera zadań systemu Windows 8 lub nowszego. Karta *Aplikacje* Menedżera zadań systemu Windows 7 zawiera widoczne okna najwyższego poziomu, a nie procesy jako takie. W nowym Menedżerze zadań systemu Windows 8 lub nowszego informacje te są obecnie widoczne w obrębie karty *Procesy*.

Nazwa	Ident...	Stan	Nazwa uży...	Uży...	Pamięć (pr...	Opis
ACMON.exe	4448	Uruchomiony	user	00	276 K	ACMON
AsusTPCenter.exe	6384	Uruchomiony	user	00	800 K	ASUS Smart Gesture Ce...
AsusTPHelper.exe	6788	Uruchomiony	user	00	192 K	ASUS Smart Gesture Hel...
AsusTPLoader.exe	6068	Uruchomiony	user	00	220 K	ASUS Smart Gesture Loa...
audiodg.exe	1620	Uruchomiony	LOCAL SE...	00	5 528 K	Izolacja wykresu urzędz...
ColorUserService.exe	4504	Uruchomiony	user	00	280 K	ASUS Color Engine
csrss.exe	532	Uruchomiony	SYSTEM	00	800 K	Proces wykonawczy klie...
csrss.exe	620	Uruchomiony	SYSTEM	01	1 204 K	Proces wykonawczy klie...
dasHost.exe	1824	Uruchomiony	LOCAL SE...	00	5 528 K	Device Association Fra...
dllhost.exe	6984	Uruchomiony	user	00	1 512 K	COM Surrogate
dwm.exe	996	Uruchomiony	DWM-1	02	20 168 K	Menedżer okien pulpitu
explorer.exe	3744	Uruchomiony	user	00	31 540 K	Eksplorator Windows
HeciServer.exe	2216	Uruchomiony	SYSTEM	00	1 152 K	Intel(R) Capability Licen...
HprSnap6.exe	6496	Uruchomiony	user	00	9 460 K	HyperSnap
igfxCUIService.exe	1328	Uruchomiony	SYSTEM	00	1 400 K	igfxCUIService Module
igfxEM.exe	4692	Uruchomiony	user	00	4 636 K	igfxEM Module
igfxHK.exe	4712	Uruchomiony	user	00	4 040 K	igfxHK Module
igfxTray.exe	4732	Uruchomiony	user	00	4 856 K	igfxTray Module
LavasoftTcpService.e...	2224	Uruchomiony	SYSTEM	02	9 036 K	LavasoftTcpService.exe
lsass.exe	740	Uruchomiony	SYSTEM	00	4 176 K	Local Security Authority...
MSASCuiL.exe	6152	Uruchomiony	user	00	2 636 K	Windows Defender notif...
MsmPngEng.exe	2312	Uruchomiony	SYSTEM	00	48 064 K	Antimalware Service Exe...
msnaint.exe	6696	Uruchomiony	user	00	7 592 K	Paint

Karta *Szczegóły* również prezentuje procesy, lecz w bardziej zwięzły sposób. Karta nie uwzględnia okien utworzonych przez procesy, a ponadto zapewnia więcej różnorodnych kolumn z informacjami.

Zauważ, że procesy są identyfikowane przez nazwę obrazu, którego są instancją. W przeciwieństwie do niektórych obiektów systemu Windows, procesom nie można nadać nazw globalnych. W celu wyświetlenia dodatkowych *szczegółów* prawym przyciskiem myszy kliknij wiersz nagłówek i kliknij pozycję *Wybierz kolumny*. Zostanie zaprezentowana lista kolumn.



Oto niektóre kluczowe kolumny:

- **Wątki.** Kolumna zawiera liczbę wątków w każdym procesie. Liczba ta powinna standardowo wynosić co najmniej 1, ponieważ nie ma bezpośredniej możliwości utworzenia procesu bez żadnych wątków (poza tym taki proces jest naprawdę bezużyteczny). Jeśli proces nie zawiera żadnych wątków, oznacza to zwykle, że z jakiegoś powodu proces nie może zostać usunięty (prawdopodobnie na skutek jakiegoś kodu sterownika z błędami).
- **Dojścia.** Kolumna prezentuje liczbę dojsć obiektów jądra otwartych przez wątki działające w obrębie procesu (zostanie to opisane w dalszej części niniejszego rozdziału).
- **Stan.** Kolumna ta jest trochę zawiła. W wypadku procesów pozbawionych jakiegokolwiek interfejsu użytkownika normalną sytuacją powinien być stan *Uruchomiony*, choć wszystkie wątki mogą na coś oczekiwać (np. przesyłanie sygnału do obiektu jądra lub zakończenie operacji wejścia-wyjścia). W przypadku takich procesów inna opcja to stan *Wstrzymany*, który ma miejsce, gdy wszystkie wątki procesu znajdują się w stanie wstrzymania. Spowodowanie czegoś takiego przez sam proces jest mało prawdopodobne, ale może zostać osiągnięte w sposób programowy przez wywołanie dla procesu nieudokumentowanego, natywnego interfejsu API `NtSuspendProcess`, co zwykle odbywa się za pośrednictwem narzędzia (na przykład odpowiednią opcję oferuje opisane dalej narzędzie *Process Explorer*). W wypadku procesów tworzących interfejs użytkownika stan *Uruchomiony* oznacza, że interfejs ten jest aktywny. Inaczej mówiąc, wątek, który utworzył okno lub okna, oczekuje na dane wejściowe interfejsu użytkownika (z technicznego punktu widzenia jest to kolejka komunikatów powiązana z wątkiem). Stan *Wstrzymany* jest możliwy tak jak w przypadku braku interfejsu, ale dla aplikacji *Windows Apps* (udostępniających architekturę *Windows Runtime*) stan ten występuje normalnie, gdy w wyniku zminimalizowania przez użytkownika aplikacja utraci swój status pierwszoplanowej. Takie procesy są wstrzymywane po pięciu sekundach, dlatego nie zużywają żadnych zasobów procesora lub zasobów sieciowych. Dzięki temu nowa aplikacja pierwszoplanowa ma możliwość skorzystania z wszystkich zasobów komputera. Jest to szczególnie ważne w przypadku urządzeń zasilanych z baterii, takich jak tablety i telefony. Trzecia możliwa wartość w kolumnie *Stan* to stan *Nie odpowiada*.

Może on wystąpić, gdy wątek w procesie, który utworzył interfejs użytkownika, nie sprawdził przez co najmniej 5 sekund swojej kolejki komunikatów pod kątem aktywności związanej z interfejsem. Proces (a faktycznie wątek będący w posiadaniu okna) może być zajęty realizowaniem jakiegoś zadania intensywnie obciążającego procesor lub oczekiwać na zupełnie coś innego (np. zakończenie operacji wejścia-wyjścia). W każdym razie interfejs użytkownika jest zablokowany, a system Windows wskazuje to przez przyciemnienie odpowiednich okien i dołączenie do ich paska tytułu komunikatu (*Nie odpowiada*).

Każdy proces wskazuje również na swój proces nadrzędny lub proces tworzący (który nie zawsze w wypadku tego procesu jest procesem tworzącym). Jeśli proces nadrzędny już nie istnieje, odpowiednia informacja nie jest aktualizowana. Możliwe jest zatem, że proces odwołuje się do nieistniejącego procesu nadrzędnego. Nie stanowi to problemu, ponieważ nic nie jest zależne od zapewnienia aktualności tej informacji. W przypadku narzędzia Process Explorer pod uwagę brany jest czas uruchomienia procesu nadrzędnego, co ma na celu uniknięcie dołączania procesu podrzędnego na podstawie zastosowanego identyfikatora procesu. Działanie to ilustruje poniższy eksperyment.



Uwaga. Dlaczego proces nadrzędny nie będzie taki sam jak jego proces tworzący? W określonych sytuacjach niektóre procesy, które wydają się tworzone przez konkretną aplikację użytkownika, mogą korzystać z pomocy brokera lub procesu pomocniczego odpowiedzialnego za wywołanie interfejsu API tworzenia procesów. W takich przypadkach wprowadzające w błąd (a czasem niepoprawne, jeśli niezbędne jest dziedziczenie obszaru adresów lub dojsčia) byłoby wyświetlenie procesu brokera jako procesu tworzącego. W związku z tym ma miejsce operacja nazywana ponownym określaniem procesu nadrzędnego. Odpowiedni przykład zaprezentowano w rozdziale 7., „Bezpieczeństwo”.

EKSPERYMENT: Wyświetlanie drzewa procesów

Identyfikator procesu nadrzędnego lub procesu tworzącego to unikatowy atrybut związany z procesem, który nie jest wyświetlany przez większość narzędzi. Wartość tego atrybutu możesz uzyskać za pomocą narzędzia Monitor wydajności (lub w sposób programowy), tworząc żądanie dotyczące identyfikatora procesu tworzącego. Narzędzie *Tlist.exe* należące do zestawu Debugging Tools for Windows umożliwia wyświetlenie drzewa procesów przy użyciu opcji `/t`. Oto przykładowe dane wynikowe polecenia `tlist /t`:

```
System Process (0)
System (4)
  smss.exe (360)
  csrss.exe (460)
  wininit.exe (524)
  services.exe (648)
  svchost.exe (736)
    unsecapp.exe (2516)
    WmiPrvSE.exe (2860)
    WmiPrvSE.exe (2512)
    RuntimeBroker.exe (3104)
    SkypeHost.exe (2776)
    ShellExperienceHost.exe (3760) Host środowiska powłoki systemu Windows
```

```

ApplicationFrameHost.exe (2848) OleMainThreadWndName
  SearchUI.exe (3504) Wyszukiwarka
  WmiPrvSE.exe (1576)
  TiWorker.exe (6032)
  waapihost.exe (5088)
  svchost.exe (788)
  svchost.exe (932)
  svchost.exe (960)
  svchost.exe (976)
  svchost.exe (68)
  svchost.exe (380)
  VSSVC.exe (1124)
  svchost.exe (1176)
  sihost.exe (3664)
  taskhostw.exe (3032) Task Host Window
  svchost.exe (1212)
  svchost.exe (1636)
  spoolsv.exe (1644)
  svchost.exe (1936)
  OfficeClickToRun.exe (1324)
  MSOIDSVC.EXE (1256)
  MSOIDSVCM.EXE (2264)
  MBAMAgent.exe (2072)
  MsMpEng.exe (2116)
  SearchIndexer.exe (1000)
  SearchProtocolHost.exe (824)
  svchost.exe (3328)
  svchost.exe (3428)
  svchost.exe (4400)
  svchost.exe (4360)
  svchost.exe (3720)
  TrustedInstaller.exe (6052)
  lsass.exe (664)
  csrss.exe (536)
  winlogon.exe (600)
  dwm.exe (1100) DWM Notification Window
  explorer.exe (3148) Program Manager
  OneDrive.exe (4448)
  cmd.exe (5992) C:\windows\system32\cmd.exe - tlist /t
  conhost.exe (3120) CicMarshalWnd
  tlist.exe (5888)
  SystemSettingsAdminFlows.exe (4608)

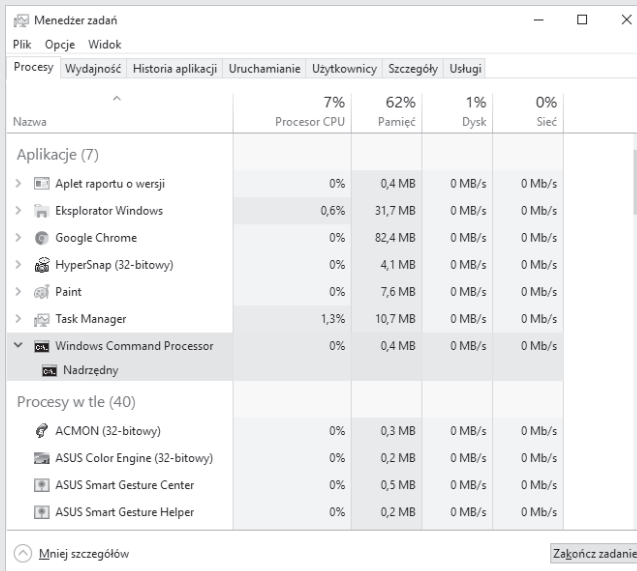
```

Na liście zastosowano wcięcie dla każdego procesu, aby pokazać jego relację między procesem nadrzędnym i podrzędnym. Procesy, których procesy nadrzędne nie istnieją, są wyrównywane do lewej strony (tak jak proces `explorer.exe` w powyższym przykładzie), ponieważ jeśli nawet występuje proces nadrzędny względem procesu nadrzędnego danego procesu, nie ma możliwości znalezienia tej relacji. System Windows utrzymuje jedynie identyfikator procesu tworzącego dany proces, a nie odnośnik do procesu nadrzędnego względem tego procesu tworzącego itd.

Liczba podana w nawiasach okrągłych to identyfikator procesu, a tekst następujący po nim w przypadku niektórych procesów to tytuł okna utworzonego przez dany proces.

Aby potwierdzić, że system Windows nie śledzi więcej informacji niż tylko identyfikator procesu nadrzędnego, wykonaj następujące kroki:

1. Użyj kombinacji klawisza z logo systemu Windows i klawisza *R*, wpisz polecenie **cmd** i naciśnij klawisz *Enter*, aby otworzyć okno wiersza poleceń.
2. Wpisz polecenie **title Nadrzędny** w celu zmiany tytułu okna na *Nadrzędny*.
3. Wpisz polecenie **start cmd**, aby otworzyć drugie okno wiersza poleceń.
4. W oknie tym wpisz polecenie **title Podrzędny**.
5. W tym samym oknie wpisz polecenie **mspaint**, aby uruchomić program Microsoft Paint.
6. Powróć do drugiego okna wiersza poleceń i wpisz polecenie **exit**. Zauważ, że program Paint pozostaje aktywny.
7. Użyj kombinacji klawiszy *Ctrl+Shift+Esc* w celu otwarcia Menedżera zadań.
8. Jeśli Menedżer zadań działa w trybie mniejszej liczby szczegółów, kliknij przycisk *Więcej szczegółów*.
9. Kliknij kartę *Procesy*.
10. Znajdź aplikację *Windows Command Processor* i rozwiń jej węzeł. Powinien być widoczny tytuł *Nadrzędny*, tak jak na poniższym zrzucie ekranu.



11. Prawym przyciskiem myszy kliknij wpis *Windows Command Processor* i wybierz pozycję *Przejdź do szczegółów*.
12. Prawym przyciskiem myszy kliknij proces *cmd.exe* i wybierz pozycję *Zakończ drzewo procesów*.
13. W oknie dialogowym potwierdzenia Menedżera zadań kliknij pozycję *Zakończ drzewo procesów*.

Pierwsze okno wiersza poleceń zniknie, ale w dalszym ciągu powinno być widoczne okno programu Paint, ponieważ było ono „wnukiem” zakończonego procesu wiersza poleceń. Ze względu na to, że zakończono proces pośredni (nadrzędny względem programu Paint), nie ma łącz między jego procesem nadrzędnym („dziadkiem”) i „wnukiem”.

Narzędzie Process Explorer dostępne w witrynie Sysinternals zapewnia więcej szczegółów dotyczących procesów i wątków niż jakiegokolwiek inne oferowane narzędzie. Z tego właśnie powodu zauważysz, że zostało ono użyte w kilku eksperymentach zamieszczonych w książce. Oto niektóre z unikatowych cech prezentowanych lub zapewnianych przez narzędzie Process Explorer:

- Token zabezpieczeń procesu, taki jak listy grup i przywilejów oraz stan wirtualizacji.
- Wyróżnianie w celu ukazania zmian w procesie, wątku, bibliotekach DLL i liście dojsć.
- Lista usług wewnątrz procesów udostępniających usługi, w tym nazwa wyświetlana i opis.
- Lista dodatkowych atrybutów procesu, takich jak zasady minimalizowania oraz ich ochrona procesu.
- Procesy stanowiące część zadania oraz jego szczegóły.
- Procesy udostępniające aplikacje .NET i szczegóły dotyczące środowiska .NET, takie jak lista elementów AppDomain, ładowane komponenty Assembly oraz liczniki wydajności CLR.
- Procesy udostępniające architekturę Windows Runtime (procesy immersywne).
- Czas uruchomienia procesów i wątków.
- Kompletna lista plików mapowanych w pamięci (nie tylko biblioteki DLL).
- Możliwość wstrzymywania procesu lub wątku.
- Możliwość kończenia działania poszczególnych wątków.
- Łatwe identyfikowanie tego, jakie procesy wykorzystały w danym czasie najwięcej zasobów procesora.



Uwaga. Monitor wydajności może informować o wykorzystaniu procesora przez procesy dla danego ich zestawu, ale nie wyświetli automatycznie procesów utworzonych po rozpoczęciu sesji monitorowania wydajności. Umożliwia to jedynie ręczne śledzenie z wykorzystaniem binarnego formatu danych wyjściowych.

Narzędzie Process Explorer zapewnia również w jednym miejscu łatwy dostęp do następujących informacji:

- Drzewo procesów pozwalające na zwijanie jego części.
- Dojścia otwarte w procesie, w tym dojścia bez nazwy.
- Lista bibliotek DLL (i plików mapowanych w pamięci) w procesie.
- Aktywność wątków w procesie.
- Stosy wątków trybu użytkownika i trybu jądra, w tym mapowanie adresów na nazwy za pomocą biblioteki *Dbghelp.dll* wchodzącej w skład zestawu Debugging Tools for Windows.
 - Dokładniejsza wartość procentowa związana z wykorzystaniem procesora, która bazuje na liczbie cykli wątków. Jest to jeszcze lepsza reprezentacja dokładnej aktywności procesora, co zostało objaśnione w rozdziale 4., „Wątki”.
 - Poziom integralności.
- Szczegóły dotyczące menedżera pamięci, takie jak maksymalna ilość pamięci zadeklarowanej oraz limity stronicowanej pamięci jądra i puli niestronicowanej (inne narzędzia podają jedynie bieżącą wielkość).

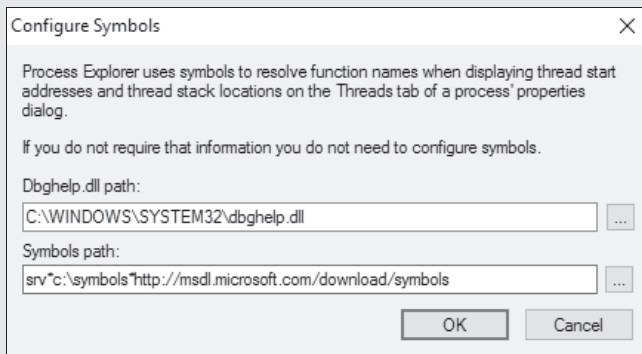
Poniżej zamieszczono wprowadzający eksperyment wykorzystujący narzędzie Process Explorer.

EKSPERYMENT:

Wyświetlanie szczegółów procesu za pomocą narzędzia Process Explorer

Pobierz najnowszą wersję narzędzia Process Explorer z witryny Sysinternals i uruchom je z uprawnieniami standardowego użytkownika. Alternatywnie prawym przyciskiem myszy kliknij plik wykonywalny i z menu wybierz polecenie *Uruchom jako administrator*, aby narzędzie uruchomić z uprawnieniami administratora. Spowoduje to zainstalowanie przez narzędzie Process Explorer sterownika oferującego więcej funkcji. Poniższy opis dotyczy dowolnego sposobu uruchomienia tego narzędzia.

Przy pierwszym załadowaniu narzędzia należy skonfigurować symbole. W przeciwnym razie po dwukrotnym kliknięciu procesu i kliknięciu karty *Threads* pojawi się komunikat informujący o tym, że aktualnie nie są skonfigurowane symbole. W przypadku poprawnego skonfigurowania symboli narzędzie Process Explorer może uzyskać dostęp do informacji o symbolach w celu wyświetlenia nazwy symbolicznej funkcji uruchamiającej wątek, a także funkcji znajdujących się na stosie wywołania wątku. Jest to przydatne przy identyfikowaniu tego, jakie działania wątki realizują wewnątrz procesu. W celu skorzystania z symboli musi zostać zainstalowany zestaw Debugging Tools for Windows (zostanie to opisane w dalszej części rozdziału). Kliknij następnie menu *Options*, wybierz pozycję *Configure Symbols* oraz podaj ścieżkę do pliku *Dbghelp.dll* w folderze zestawu Debugging Tools i poprawną ścieżkę do symboli. Na przykład w systemie 64-bitowym taka konfiguracja będzie poprawna, jeśli zestaw Debugging Tools for Windows zainstalowano w położeniu domyślnym jako część zestawu WDK.



W powyższym przykładzie użyto serwera symboli na żądanie, aby zapewnić dostęp do symboli. Kopia plików symboli przechowywana jest na komputerze lokalnym w folderze *C:\symbols* (jeśli wolne miejsce na dysku stanowi problem, folder może zostać zastąpiony innym folderem, takim jak zlokalizowany na innym dysku). Więcej informacji o konfigurowaniu serwera symboli znajdziesz pod adresem <https://msdn.microsoft.com/en-us/library/windows/desktop/ee416588.aspx>.



Wskazówka. Serwer symboli firmy Microsoft możesz skonfigurować przez ustawienie dla zmiennej środowiskowej o nazwie `_NT_SYMBOL_PATH` wartości podanej na zamieszczonym wcześniej zrzucie ekranu. Różne narzędzia, takie między innymi jak Process Explorer, debuggery wchodzące w skład zestawu Debugging Tools for Windows i Visual Studio, szukają automatycznie tej wartości. Ułatwi to uniknięcie konieczności osobnego konfigurowania każdego narzędzia.

Po uruchomieniu narzędzie Process Explorer wyświetla domyślnie widok drzewa procesów. Możesz rozwinąć dolny panel, aby ujrzeć otwarte dojścia lub mapowane biblioteki DLL i pliki mapowane w pamięci. Narzędzie prezentuje też podpowiedź dotyczącą ścieżki i wiersza poleceń procesu, która staje się widoczna w momencie umieszczenia kursora myszy nad nazwą procesu. W wypadku niektórych typów procesów podpowiedź zawiera również dodatkowe informacje. Oto one:

- Usługi w obrębie procesu udostępniającego usługi (np. *Svchost.exe*).
- Zadania w obrębie procesu udostępniającego zadania (np. *TaskHostw.exe*).
- Element docelowy procesu *Rundll32.exe*, który używany jest na potrzeby elementów panelu sterowania i innych funkcji.
- Informacje o klasie modelu COM podczas udostępniania wewnątrz procesu *Dllhost.exe* (określany też mianem domyślnego komponentu COM+ Surrogate).
- Informacje o dostawcy na potrzeby procesów hosta WMI (*Windows Management Instrumentation*), takich jak *WMIPrvse.exe*.
- Informacje dotyczące procesów aplikacji Windows Apps (procesy udostępniające architekturę Windows Runtime, które w skrócie opisano wcześniej w rozdziale w podpunkcie „Architektura Windows Runtime”).

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
MSASGUL.exe		3 108 K	11 940 K	6152	Windows Defender notification icon	Microsoft Corporation
MailboxEng.exe	0.33	139 816 K	100 256 K	2312	Antimalware Service Executable	Microsoft Corporation
NetSrv.exe		12 684 K	7 736 K	4740	Microsoft Network Realtime Inspection Service	Microsoft Corporation
OfficeClickToRun.exe		38 669 K	39 295 K	2172	Microsoft Office Click-to-Run (CTS)	Microsoft Corporation
PDVD10Serv.exe		1 500 K	7 992 K	6250	PowerDVD PC Service	CyberLink Corp.
PresentationFontCache.exe		32 220 K	19 382 K	4060	PresentationFontCache.exe	Microsoft Corporation
process64.exe	4.82	20 732 K	39 324 K	3912	System Idle Process Explorer	System Idle - www.sysinternals.com
RAVBack4.exe		5 820 K	1 196 K	1016	HD Audio Background Process	Realtek Semiconductor
RAVBack4.exe		5 500 K	1 164 K	5200	HD Audio Background Process	Realtek Semiconductor
RAVConf4.exe		3 824 K	1 344 K	1468	Menedżer Realtek HD Audio	Realtek Semiconductor
RuntimeBroker.exe		18 748 K	42 296 K	4200	Runtime Broker	Microsoft Corporation
SearchIndexer.exe		31 352 K	38 680 K	2343	Indeksator programu Microsoft Windows Search	Microsoft Corporation
SearchIndexer.exe	Suspended	79 200 K	68 344 K	7992	SearchIndexer.exe	Microsoft Corporation
services.exe	0.07	2 840 K	5 696 K	732	Usługi i aplikacja Kontroler	Microsoft Corporation
ShellExperienceHost.exe	< 0.01	30 748 K	67 240 K	5184	Windows Shell Experience Host	Microsoft Corporation
shost.exe		4 880 K	19 828 K	4016	Shell Infrastructure Host	Microsoft Corporation
Spoolsv.exe	Suspended	4 680 K	3 840 K	6972	Microsoft Spooler	Microsoft Corporation
smss.exe		396 K	1 040 K	356	Menedżer sesji systemu Windows	Microsoft Corporation
spoolsv.exe		7 188 K	12 428 K	1944	Spooler SubSystem App	Microsoft Corporation
svchost.exe	0.01	8 840 K	21 616 K	828	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe		6 812 K	11 428 K	960	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe	0.01	33 098 K	56 432 K	492	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe	0.02	58 376 K	64 540 K	536	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe	< 0.01	13 020 K	20 820 K	1156	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe	0.02	21 168 K	27 720 K	1176	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe		9 176 K	20 452 K	1184	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe		7 232 K	15 800 K	1468	Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
svchost.exe					Proces hosta dla usług systemu Windows	Microsoft Corporation
System					Usługa Menedżera zasobów systemu Windows [LocalManager]	Microsoft Corporation
					Usługa autodyktowania serwisu proxy w sieci Web HTTP [WinHttpProxySvc]	Microsoft Corporation
					Usługa systemu Windows do tworzenia czołówek [FontCache]	Microsoft Corporation

Command Line: C:\WINDOWS\system32\svchost.exe -k LocalService (LocalService) Services: Host dostawcy oprogramowania funkcji [SpHdnt] Host usług diagnostycznych [NtdServiceHost] System zdarzeń COM+ [EventSystem] Usługa kety sieci [wscntfrms] Usługa interfejsu magazynu sieciowego [nsi] Usługa Menedżera zasobów systemu Windows [LocalManager] Usługa autodyktowania serwisu proxy w sieci Web HTTP [WinHttpProxySvc] Usługa systemu Windows do tworzenia czołówek [FontCache]

CPU Usage: 34.0%

Oto kroki pozwalające na zaznajomienie się z podstawowymi możliwościami narzędzia Process Explorer:

1. Zauważ, że procesy udostępniające usługi są domyślnie wyróżnione na różowo. Procesy utworzone samodzielnie są wyróżnione na niebiesko. Aby zmienić te kolory, wyświetl menu rozwijane, a następnie wybierz pozycje *Options* i *Configure Colors*.
2. Kursor myszy umieść nad nazwą obrazu procesów. Zauważ, że podpowiedź wyświetla pełną ścieżkę. Jak już wspomniano, w wypadku niektórych typów procesów w podpowiedzi widoczne są dodatkowe szczegóły.
3. Po kliknięciu pozycji *View* i *Select Columns* na karcie *Process Image* zaznacz opcję *Image Path*.
4. Aby posortować procesy, kliknij nagłówek kolumny *Process*. Zauważ, że znika widok drzewa (możesz wyświetlić ten widok lub dokonać sortowania według dowolnej z widocznych kolumn). Ponownie kliknij nagłówek kolumny *Process*, aby zastosować sortowanie w kolejności od Z do A. Kliknij nagłówek trzeci raz w celu przywrócenia widoku drzewa.
5. Wyświetl menu *View* i wyłącz zaznaczenie opcji *Show Processes from All Users*, aby zostały wyświetlone tylko procesy utworzone samodzielnie.
6. Kliknij menu *Options*, wybierz pozycję *Difference Highlight Duration* i zmień wartość na 3 sekundy. Wywołaj następnie nowy proces (jakikolwiek). Zauważ, że przez 3 sekundy nowy proces wyróżniony jest na zielono. Zakończ ten nowy proces. Zwróć uwagę na to, że zanim proces przestanie być widoczny, przez 3 sekundy jest on wyróżniony na czerwono. Może to być przydatne przy obserwacji procesów tworzonych i kończonych w systemie.
7. Dwukrotnie kliknij proces i w obrębie wyświetlonych właściwości procesu sprawdź różne dostępne karty (karty będą używane w różnych eksperymentach zamieszczonych w książce, w których objaśniono prezentowane informacje).

Wątki

Wątek to obiekt wewnątrz procesu, którego wykonanie planuje system Windows. Bez wątku niemożliwe byłoby uruchomienie programu procesu. Wątek uwzględnia następujące zasadnicze komponenty:

- Zawartość zestawu rejestrów procesora reprezentujących jego stan.
- Dwa stosy — jeden dla wątku używany podczas wykonywania w trybie jądra oraz jeden na potrzeby wykonywania w trybie użytkownika.
- Prywatny obszar pamięci nazywany *pamięcią lokalną wątku TLS* (ang. *Thread Local Storage*) przeznaczony dla podsystemów, bibliotek uruchomieniowych i bibliotek DLL.
- Unikatowy identyfikator nazywany *identyfikatorem wątku* (część wewnętrznej struktury określanej mianem *identyfikatora klienta*; identyfikatory procesów i wątków są generowane poza tą samą przestrzenią nazw, dlatego nigdy się nie nakładają).

Ponadto wątki mają czasami własny kontekst zabezpieczeń lub token, który często używany jest przez wielowątkowe aplikacje serwerowe naśladujące kontekst zabezpieczeń obsługiwanych przez nie klientów.

Zmienne rejestry, stopy i prywatny obszar pamięci są określane mianem *kontekstu* wątku. Ponieważ związane z tym informacje są inne dla każdej architektury sprzętowej z uruchomionym systemem Windows, z konieczności taka struktura jest powiązana z architekturą. Funkcja `GetThreadContext` systemu Windows zapewnia dostęp do informacji specyficznych dla danej architektury (nazywanych blokiem `CONTEXT`).

Ponieważ przełączanie wykonywania między dwoma wątkami angażuje dyspozytora jądra, może to być wymagająca operacja, zwłaszcza wtedy, gdy dwa wątki często wzajemnie się przełączają. Aby zmniejszyć związany z tym koszt, system Windows implementuje dwa mechanizmy: *włókna* (ang. *fibers*) i *planowanie w trybie użytkownika UMS* (ang. *User Mode Scheduling*).



Uwaga. Wątki aplikacji 32-bitowej działającej w 64-bitowym systemie Windows będą zawierać zarówno 32-bitowe, jak i 64-bitowe konteksty, których podsystem Wow64 (Windows on Windows) użyje w razie potrzeby do przełączania uruchomionej aplikacji z trybu 32-bitowego do trybu 64-bitowego. Wątki te będą mieć dwa stopy użytkownika oraz dwa bloki `CONTEXT`, a zwykle funkcje API systemu Windows będą zwracać kontekst 64-bitowy. Funkcja `Wow64GetThreadContext` zwróci jednak kontekst 32-bitowy.

Włókna

Włókna umożliwiają aplikacji planowanie jej własnych wątków wykonania, zamiast polegać na wbudowanym w system Windows mechanizmie planowania opartym na priorytetach. Włókna są często nazywane *wątkami lekkimi*. Z punktu widzenia planowania włókna są niewidoczne dla jądra, ponieważ implementowane są w trybie użytkownika w bibliotece `Kernel32.dll`. Aby zastosować włókna, tworzone jest najpierw wywołanie funkcji `ConvertThreadToFiber` systemu Windows. Przekształca ona wątek w działające włókno. Dalej nowe włókno uzyskane w wyniku przekształcenia może tworzyć dodatkowe włókna za pośrednictwem funkcji `CreateFiber` (każde włókno może mieć własny zestaw włókien). W przeciwieństwie jednak do wątku, włókno nie rozpoczyna wykonywania do momentu ręcznego wybrania go za pomocą wywołania funkcji `SwitchToFiber`. Nowe włókno jest uruchomione do chwili jego zakończenia lub wywołania przez nie tej funkcji, co ponownie powoduje wybranie kolejnego włókna do uruchomienia. Więcej informacji na temat funkcji włókien zamieszczono w dokumentacji zestawu SDK systemu Windows.



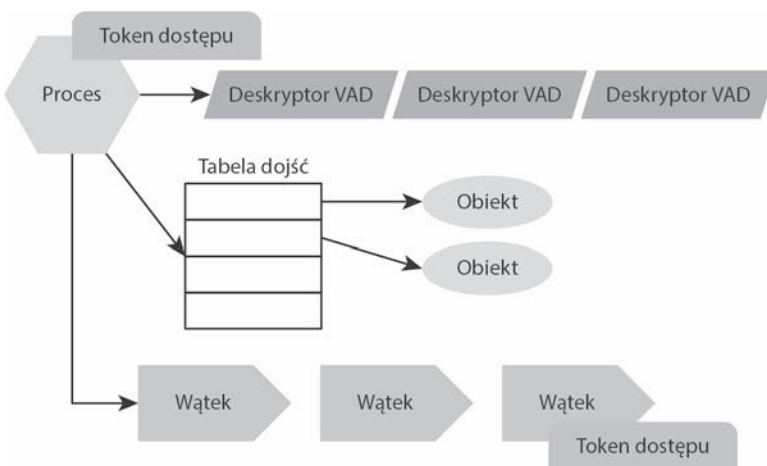
Uwaga. Użycie włókien nie jest zwykle dobrym pomysłem. Wynika to stąd, że są one niewidoczne dla jądra. Powodują one ponadto takie problemy, jak współużytkowanie pamięci lokalnej wątku (TLS), ponieważ kilka włókien może działać w tym samym wątku. Choć istnieje pamięć lokalna włókna FLS (ang. *Fiber Local Storage*), nie rozwiązuje ona wszystkich problemów ze współużytkowaniem, a niezależnie od tego włókna związane z operacjami wejścia-wyjścia będą kiepsko działać. Ponadto włókna nie mogą działać jednocześnie na więcej niż jednym procesorze i są ograniczone wyłącznie do wielozadaniowości równoległej. W większości sytuacji najlepszym rozwiązaniem jest umożliwienie jądra systemu Windows obsługi planowania za pomocą odpowiednich wątków dostępnego zadania.

Wątki planowania w trybie użytkownika

Wątki planowania w trybie użytkownika (UMS), które są dostępne wyłącznie w 64-bitowych wersjach systemu Windows, zapewniają te same podstawowe korzyści co włókna, a ponadto mają tylko kilka mankamentów. Wątki UMS mają własny stan wątków jądra, dlatego są widoczne dla jądra, co pozwala wielu wątkom UMS tworzyć blokujące wywołania systemowe, a także współużytkować zasoby i rywalizować o nie. Gdy dwa lub więcej wątków UMS wymaga zrealizowania działań w trybie użytkownika, mogą w nim okresowo przełączać konteksty wykonywania (przez przechodzenie z jednego wątku do drugiego), a nie angażować do tego dyspozytora. Z perspektywy jądra w dalszym ciągu działa ten sam jego wątek i nic nie uległo zmianie. Gdy wątek UMS wykonuje operację wymagającą uzyskania dostępu do jądra (na przykład w przypadku wywołania systemowego), dokonuje przełączenia do własnego dedykowanego wątku trybu jądra (jest to określane mianem *bezpośredniego przełączenia kontekstu*). Choć współbieżne wątki UMS w dalszym ciągu nie mogą działać na wielu procesorach, są one zgodne z modelem wywłaszczalnym, który nie do końca oferuje możliwości współpracy.

Chociaż wątki mają własny kontekst wykonywania, każdy wątek w procesie współużytkuje jego obszar adresów wirtualnych (oprócz reszty zasobów należących do procesu). Oznacza to, że wszystkie wątki w procesie dysponują pełnym (z odczytem i zapisem) dostępem do obszaru adresów wirtualnych procesu. Wątki nie mogą jednak przypadkowo odwoływać się do obszaru adresów innego procesu, chyba że inny proces udostępnia część swojego prywatnego obszaru adresów jako sekcję wspólnej pamięci (w interfejsie API systemu Windows nazywanej *obiektem mapowania plików*) lub jeden proces ma możliwość otwarcia innego procesu w celu użycia międzyprocesowych funkcji pamięci, takich jak `ReadProcessMemory` i `WriteProcessMemory` (z których domyślnie może skorzystać proces działający na bazie tego samego konta użytkownika, a nie wewnątrz komponentu `AppContainer` lub innego typu „piaskownicy”, chyba że dla procesu docelowego zastosowano określone elementy ochrony).

Oprócz prywatnego obszaru adresów i jednego lub większej liczby wątków, każdy proces ma kontekst zabezpieczeń oraz listę otwartych dość powiązanych z obiektami jądra, takimi jak pliki i sekcje wspólnej pamięci, lub z jednym z obiektów synchronizacji, takich jak obiekty *mutex*, zdarzenia lub semafora. Zilustrowano to na rysunku 1.2.



RYSUNEK 1.2. Proces i jego zasoby

Kontekst zabezpieczeń każdego procesu jest przechowywany w obiekcie nazywanym *tokenem dostępu*. Token dostępu procesu zawiera związaną z nim identyfikację zabezpieczeń i dane uwierzytelniające. Domyślnie wątki nie mają własnego tokenu dostępu, ale mogą go uzyskać, dzięki czemu poszczególne wątki mają możliwość naśladowania kontekstu zabezpieczeń innego procesu (w tym procesów zdalnego systemu Windows) bez wpływu na inne wątki procesu (w rozdziale 7. zamieszczono więcej szczegółów dotyczących zabezpieczeń procesów i wątków).

Deskryptory adresów wirtualnych VAD (Virtual Address Descriptor) to struktury danych używane przez menedżer pamięci do śledzenia adresów wirtualnych wykorzystywanych przez proces. Te struktury danych opisano obszerniej w rozdziale 5.

Zadania

System Windows zapewnia rozszerzenie modelu procesów nazywane *zadaniem*. Główną funkcją obiektu zadania jest umożliwienie przetwarzania grup procesów jako jednostki oraz zarządzania nimi. Obiekt zadania pozwala kontrolować określone atrybuty oraz zapewnia limity procesowi lub procesom powiązanim z zadaniem. Obiekt ten zapisuje też podstawowe informacje rejestracyjne dla wszystkich procesów powiązanych z zadaniem, a także dla procesów, które zostały z nim skojarzone, ale później zostały zakończone. Pod pewnymi względami obiekt zadania kompensuje brak w systemie Windows strukturalnego drzewa procesów, a przy tym w wielu aspektach oferuje większe możliwości niż drzewo procesów w stylu obecnego w systemie UNIX.



Uwaga. Narzędzie Process Explorer może prezentować procesy zarządzane przez zadanie z wykorzystaniem domyślnego koloru brązowego, co jednak standardowo nie jest możliwe (w celu aktywowania tej funkcji wyświetl menu *Options* i wybierz pozycję *Configure Colors*). Ponadto strony właściwości takiego procesu oferują dodatkową kartę *Job*, która zapewnia informacje o samym obiekcie zadania.

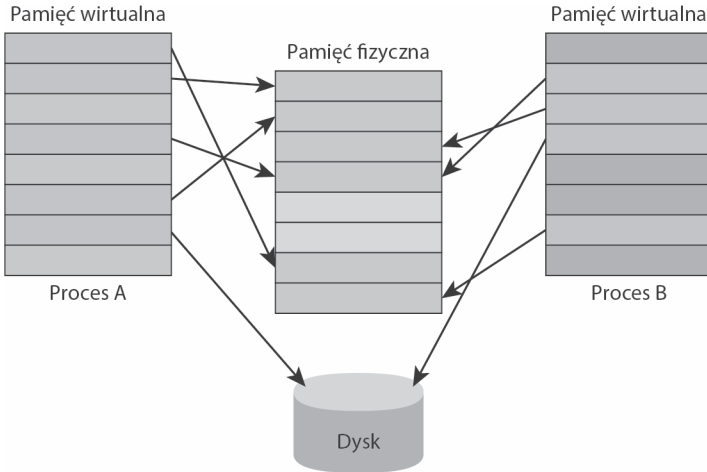
Znacznie więcej na temat wewnętrznej struktury procesów i zadań znajdziesz w rozdziale 3. W rozdziale 4. przeczytasz o wątkach i ich algorytmach planowania.

Pamięć wirtualna

System Windows implementuje system pamięci wirtualnej oparty na płaskim (liniowym) obszarze adresów, który zapewnia każdemu procesowi „wrażenie” dysponowania własnym dużym, prywatnym obszarem adresów. Pamięć wirtualna oferuje widok logiczny pamięci, który może nie odpowiadać jej układowi fizycznemu. W środowisku uruchomieniowym menedżer pamięci wspierany sprzętowo dokonuje translacji lub *mapowania* adresów wirtualnych na adresy fizyczne, w których dane są faktycznie przechowywane. Kontrolując elementy ochrony i mapowanie, system operacyjny może zapewnić, że poszczególne procesy nie kolidują ze sobą lub nadpisują dane systemowe.

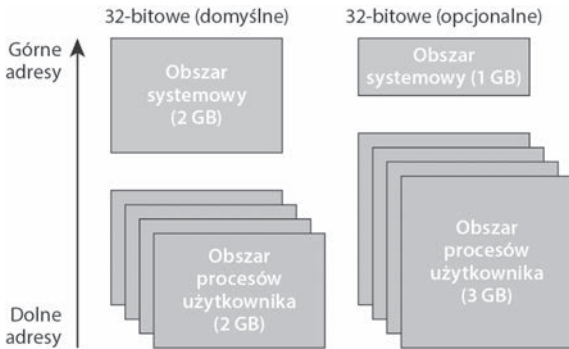
Ponieważ większość systemów dysponuje znacznie mniejszą ilością pamięci fizycznej, niż wynosi wielkość pamięci wirtualnej używanej przez działające procesy, menedżer pamięci transferuje lub *stronicuje* na dysk część zawartości pamięci. Stronicowanie danych na dysku powoduje zwolnienie pamięci fizycznej, dzięki czemu może ona zostać przeznaczona dla innych procesów lub samego systemu operacyjnego. Gdy wątek uzyskuje dostęp do adresu wirtualnego, dla którego wykonano operację stronicowania na dysk, menedżer pamięci wirtualnej ładuje informacje ponownie do pamięci z dysku.

Aplikacje nie muszą być modyfikowane w żaden sposób, aby mogły skorzystać ze stronicowania, ponieważ obsługa sprzętowa umożliwia menedżerowi pamięci przeprowadzanie stronicowania bez wiedzy lub udziału procesów lub wątków. Na rysunku 1.3 pokazano dwa procesy korzystające z pamięci wirtualnej, w której część fragmentów jest mapowana na pamięć fizyczną (RAM), a część jest stronicowana na dysk. Zauważ, że ciągłe porcje pamięci wirtualnej mogą być mapowane na nieciągłe porcje w pamięci fizycznej. Porcje takie są nazywane stronami i mają domyślną wielkość wynoszącą 4 kB.



RYSUNEK 1.3. Mapowanie pamięci wirtualnej na pamięć fizyczną z zastosowaniem stronicowania

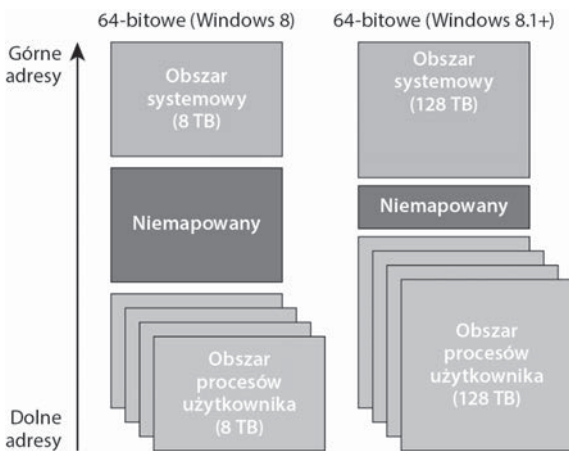
Wielkość obszaru adresów wirtualnych jest inna dla każdej platformy sprzętowej. W wypadku 32-bitowych systemów x86 całkowity obszar adresów wirtualnych ma teoretyczną, maksymalną wielkość równą 4 GB. Domyślnie system Windows alokuje dolną połowę tego obszaru adresów (adresy od 0x00000000 do 0x7FFFFFFF) procesom na potrzeby ich unikatowej pamięci prywatnej, a górną połowę (adresy od 0x80000000 do 0xFFFFFFFF) przeznaczają do wykorzystania własnej pamięci chronionej. Mapowania dolnej połowy obszaru zmieniają się, aby uwzględnić obszar adresów wirtualnych aktualnie wykonywanego procesu. Z kolei większość mapowań górnej połowy zawsze jest złożona z pamięci wirtualnej systemu operacyjnego. System Windows oferuje opcje rozruchowe, takie jak kwalifikator `increaseuserva` w bazie danych Boot Configuration Database (opisano ją w rozdziale 5.), które zapewniają procesom uruchamiającym specjalnie oznaczone programy możliwość użycia maksymalnie 3 GB prywatnego obszaru adresów, pozostawiając systemowi 1 GB (pod terminem „specjalnie oznaczone” kryje się to, że w nagłówku obrazu wykonywalnego musi zostać ustawiona flaga dużego obszaru adresów). Taka opcja pozwala aplikacjom, takim jak serwery bazy danych, utrzymywać większe porcje bazy w obszarze adresów procesu. Dzięki temu zmniejsza się potrzeba mapowania na dysk widoków podzbiorów bazy danych, a tym samym zwiększa się ogólna wydajność (choć w niektórych przypadkach utrata 1 GB pamięci przez system może powodować bardziej wyraźne spadki wydajności w skali całego systemu). Na rysunku 1.4 pokazano dwa typowe układy obszaru adresów wirtualnych obsługiwane przez 32-bitowy system Windows (opcja `increaseuserva` umożliwia obrazom wykonywalnym oznaczonym za pomocą flagi dużego obszaru adresów zastosowanie pamięci o wielkości od 2 do 3 GB).



RYSUNEK 1.4. Typowe układy obszaru adresów 32-bitowego systemu Windows

Choć 3 GB jest lepsze niż 2 GB, w dalszym ciągu nie jest to obszar adresów wirtualnych wystarczający do mapowania bardzo dużych baz danych (liczących wiele gigabajtów). Aby umożliwić to w 32-bitowym systemie Windows, zapewniany jest przez niego mechanizm AWE (ang. *Address Windowing Extensions*), który pozwala 32-bitowej aplikacji przydzielić maksymalnie 64 GB pamięci fizycznej, a następnie mapować widoki lub okna na własny obszar adresów wirtualnych aplikacji o wielkości 2 GB. Choć użycie mechanizmu AWE powoduje obciążenie projektanta nakładem pracy związanym z zarządzaniem mapowaniem pamięci wirtualnej na fizyczną, daje możliwość uzyskania bezpośredniego dostępu do większej ilości pamięci fizycznej, niż może być mapowane w dowolnym momencie w 32-bitowym obszarze adresów procesu.

64-bitowy system Windows zapewnia procesom znacznie większy obszar adresów: 128 TB w wypadku systemów Windows 8.1, Server 2012 R2 oraz nowszych. Na rysunku 1.5 pokazano uproszczony widok układów 64-bitowych systemowych obszarów adresów (szczegółowy opis zamieszczono w rozdziale 5.). Zauważ, że podane wielkości nie reprezentują ograniczeń architektury obowiązujących dla tych platform. 64 bity obszaru adresów to 2 do potęgi 64. lub 16 EB (gdzie 1 EB równa się 1024 PB lub 1 048 576 TB), ale obecnie używane urządzenia 64-bitowe ograniczają to do mniejszych wartości. Niemapowany obszar oznaczony na rysunku 1.5 jest znacznie większy niż możliwy obszar mapowany (w systemie Windows 8 około miliona razy większy), co oznacza, że obrazy nie są (na razie) skalowane.



RYSUNEK 1.5. Układy obszaru adresów 64-bitowego systemu Windows

W rozdziale 5. opisano szczegóły implementacji menedżera pamięci, w tym sposób działania translacji adresów, a także to, jak system Windows zarządza pamięcią fizyczną.

Porównanie trybu jądra i trybu użytkownika

Aby uniemożliwić aplikacjom użytkownika dostęp do krytycznych danych systemu operacyjnego i/lub ich modyfikację, w systemie Windows stosowane są dwa tryby dostępu do procesora (jeśli nawet procesor, z którego korzysta system, obsługuje więcej niż dwa tryby): *tryb użytkownika* i *tryb jądra*. Kod aplikacji użytkownika działa w trybie użytkownika, natomiast kod systemu operacyjnego (np. usługi systemowe i sterowniki urządzeń) w trybie jądra. Tryb jądra odwołuje się do trybu wykonywania w procesorze, który zapewnia dostęp do całej pamięci systemowej i wszystkich instrukcji procesora. W wypadku części procesorów tryby takie są odróżniane za pomocą terminu *poziom przywilejów kodu* lub *poziom pierścienia*, natomiast w przypadku pozostałych są stosowane takie terminy, jak *tryb nadzorczy* i *tryb aplikacji*. Niezależnie od użytych terminów, dzięki zapewnieniu jądra systemu operacyjnego z wyższym poziomem przywilejów niż w przypadku aplikacji trybu użytkownika procesor dostarcza projektantom systemów niezbędną bazę do zapewnienia, że niepoprawnie działająca aplikacja nie może wpłynąć niekorzystnie na stabilność całego systemu.



Uwaga. Architektury procesorów x86 i x64 definiują cztery poziomy przywilejów (lub pierścienie), aby ochronić kod systemu i dane przed nadpisaniem nieumyślnie lub celowo przez kod o niższych przywilejach. Na potrzeby trybu jądra i trybu użytkownika system Windows używa odpowiednio poziomu przywilejów 0 (lub pierścienia 0) oraz poziomu przywilejów 3 (lub pierścienia 3). Powodem stosowania przez system Windows tylko dwóch poziomów jest to, że w niektórych architekturach sprzętowych, takich jak ARM obecnie i MIPS/Alpha w przeszłości, zaimplementowano zaledwie dwa poziomy przywilejów. Zdecydowanie się na całkowite minimum pozwoliło uzyskać efektywniejszą i bardziej przenośną architekturę, zwłaszcza z tego względu, że inne poziomy pierścieni architektury x86/x64 nie oferują takich samych gwarancji co pierścienie od 0 do 3.

Choć każdy proces systemu Windows ma własny obszar pamięci prywatnej, kod sterowników urządzeń i kod systemu operacyjnego w trybie jądra współużytkują pojedynczy obszar adresów wirtualnych. Każda strona w pamięci wirtualnej jest oznaczona w celu wskazania, w jakim trybie dostępu musi znajdować się procesor, aby mógł odczytać i/lub zapisać stronę. Strony w obszarze systemowym mogą być dostępne tylko w trybie jądra, natomiast wszystkie strony w obszarze adresów użytkownika są dostępne zarówno w trybie użytkownika, jak i w trybie jądra. Strony tylko do odczytu (zawierające na przykład dane statyczne) nie mogą być zapisywane w żadnym trybie. Ponadto w wypadku procesorów zabezpieczających przed atakami przepełnienia bufora pamięci system Windows oznacza strony zawierające dane jako niemożliwe do wykonania. W ten sposób system zapobiega nieumyślnemu lub celowemu wykonaniu kodu w obszarach danych (jeśli włączona jest funkcja DEP — *Data Execution Prevention*).

System Windows nie zapewnia żadnej ochrony dotyczącej prywatnej pamięci systemowej do odczytu i zapisu, która używana jest przez komponenty działające w trybie jądra. Inaczej mówiąc, w trybie jądra kod systemu operacyjnego i sterowników urządzeń ma pełny dostęp do pamięci obszaru systemowego, a ponadto przy uzyskiwaniu dostępu do obiektów może pominąć zabezpieczenia systemu Windows. Ponieważ większa część tego systemu działa w trybie jądra, kluczowe znaczenie ma staranne projektowanie i testowanie komponentów uruchamianych w trybie jądra, aby zapewnić, że nie naruszą one bezpieczeństwa systemu lub nie spowodują jego niestabilności.

Taki brak ochrony uwidacznia też potrzebę zachowania czujności przy ładowaniu zewnętrznego sterownika urządzenia, a zwłaszcza wtedy, gdy nie jest on podpisany, ponieważ w trybie jądra sterownik dysponuje pełnym dostępem do wszystkich danych systemu operacyjnego. Ryzyko to było jednym z powodów wprowadzenia w systemie Windows 2000 mechanizmu podpisywania sterowników, który ostrzega (i blokuje po przeprowadzeniu odpowiedniej konfiguracji) użytkownika, jeśli podejmowana jest próba dodania sterownika Plug and Play bez podpisu (więcej informacji o podpisywaniu sterowników zamieszczono w rozdziale 6., „System operacji wejścia-wyjścia”). Mechanizm ten nie wpływa jednak na inne typy sterowników. Poza tym, mechanizm Driver Verifier ułatwia twórcom sterowników urządzeń znajdowanie błędów, takich jak nadpisanie bufora lub wycieki pamięci, które mogą spowodować problemy z zabezpieczeniami lub niezawodnością (mechanizm ten również omówiono w rozdziale 6.).

W przypadku 64-bitowych wersji systemu Windows 8.1 oraz jego wersji dla urządzeń ARM zasada KMCS (ang. *Kernel-Mode Code-Signing*) podpisywania kodu w trybie jądra wymusza konieczność podpisywania wszystkich sterowników urządzeń (a nie tylko sterowników Plug and Play) przy użyciu klucza kryptograficznego przydzielonego przez jeden z głównych urzędów certyfikacji kodu. Użytkownik nie może wprost wymusić instalacji niepodpisanego sterownika, nawet jako administrator. Jednak w ramach jednorazowego wyjątku ograniczenie to może zostać ręcznie wyłączone. Umożliwia to automatyczne podpisanie i testowanie sterowników, a ponadto powoduje umieszczenie na tapecie pulpitu znaku wodnego informującego o trybie testowym i wyłączenie określonych funkcji zarządzania prawami cyfrowymi (DRM — *Digital Rights Management*).

W systemie Windows 10 firma Microsoft wprowadziła jeszcze bardziej znaczącą zmianę, która została wymuszona rok po udostępnieniu jako część lipcowej aktualizacji Anniversary Update (wersja 1607). Od tego czasu wszystkie nowe sterowniki dla systemu Windows 10 muszą być podpisane tylko przez dwa akceptowane urzędy certyfikacji za pomocą certyfikatu SHA-2 Extended Validation (EV), a nie przy użyciu zwykłego certyfikatu SHA-1 opartego na pliku oferowanego przez 20 urzędów. Sterownik urządzenia podpisany za pomocą certyfikatu EV musi zostać przesłany firmie Microsoft za pośrednictwem portalu System Device (SysDev) w celu poświadczenia podpisu i otrzymania podpisu Microsoftu. W tej sytuacji jądro będzie podpisywać wyłącznie sterowniki dla systemu Windows 10 podpisane przez firmę Microsoft bez żadnych wyjątków, pomijając wcześniej wspomniany tryb testowy. Sterowniki podpisane przed datą opublikowania systemu Windows 10 (lipiec 2015 r.) mogą na razie być nadal ładowane z użyciem zwykłego podpisu.

Jak dotąd w wypadku systemu operacyjnego Windows Server 2016 podjęto najbardziej stanowczą decyzję. Bazowanie na wcześniej podanych wymaganiach w postaci certyfikatów EV sprawia, że samo podpisywanie poświadczenia staje się niewystarczające. Aby sterownik dla systemu Windows 10 został załadowany w systemie serwera, musi przejść rygorystyczny proces certyfikacji WHQL (ang. *Windows Hardware Quality Labs*) jako część pakietu HCK (ang. *Hardware Compatibility Kit*), a ponadto musi zostać przesłany do formalnej oceny. Możliwość załadowania w takich systemach będą mieć tylko sterowniki podpisane za pomocą certyfikatu WHQL, które zapewniają administratorom systemu określone gwarancje dotyczące zgodności, bezpieczeństwa, wydajności i stabilności. Podsumowując, ograniczenie liczby zewnętrznych sterowników, które mogą zostać załadowane w pamięci trybu jądra, powinno spowodować znaczne zwiększenie poziomu stabilności i bezpieczeństwa.

W wypadku konkretnych dostawców i platform, a nawet konfiguracji systemu Windows dla przedsiębiorstw może istnieć dowolna liczba dostosowanych zasad podpisywania, takich jak oferowane przez technologię Device Guard, która w skrócie zostanie opisana w następnym punkcie, „Hipernadzorca”, a później w rozdziale 7. W związku z tym przedsiębiorstwo może

wymagać podpisów WHQL nawet w systemach klienckich Windows 10 albo może zażądać pominięcia tego wymogu w systemie Windows Server 2016.

Jak się okaże w rozdziale 2., „Architektura systemu”, aplikacje użytkownika dokonują przełączenia z trybu użytkownika do trybu jądra w momencie tworzenia wywołania usługi systemowej. Na przykład funkcja `ReadFile` systemu Windows wymaga ostatecznie wywołania jego wewnętrznego programu, który w rzeczywistości obsługuje odczyt danych z pliku. Ponieważ program ten uzyskuje dostęp do wewnętrznych struktur danych systemu, musi działać w trybie jądra. Użycie specjalnej instrukcji procesora wyzwala przejście z trybu użytkownika do trybu jądra, a ponadto powoduje aktywowanie przez procesor usługi systemowej rozdzielającej kod w jądrze. To z kolei powoduje wywołanie odpowiedniej funkcji wewnętrznej w pliku `Ntoskrnl.exe` lub `Win32k.sys`. Przed przekazaniem kontroli wątkowi użytkownika tryb procesora z powrotem przełączany jest na tryb użytkownika. W ten sposób system operacyjny chroni siebie i swoje dane przed wglądem procesów użytkownika i modyfikowaniem.



Uwaga. Przejście z trybu użytkownika do trybu jądra (i z powrotem) nie wpływa na planowanie wątków *jako takie*. Przejście trybów *nie* jest przełączaniem kontekstu. W rozdziale 2. zamieszczono dodatkowe szczegóły dotyczące rozdzielania usług systemowych.

A zatem normalną sytuacją jest to, że wątek użytkownika spędza część swojego czasu wykonywania w trybie użytkownika, a część w trybie jądra. Okazuje się, że ponieważ spora część systemu graficznego i systemu obsługującego okna również działa w trybie jądra, aplikacje intensywnie korzystające z grafiki więcej czasu spędzają w trybie jądra niż w trybie użytkownika. Prosty sposób sprawdzenia tego jest uruchomienie tego rodzaju aplikacji, takiej jak Microsoft Paint, i obserwowanie za pomocą liczników wydajności (wyszczególnionych w tabeli 1.3) podziału czasu między trybem użytkownika i trybem jądra. Bardziej zaawansowane aplikacje mogą używać nowszych technologii, takich jak Direct2D i DirectComposition, które większość obliczeń wykonują w trybie użytkownika, a do jądra kierują tylko nieprzetworzone dane związane z powierzchniami. Dzięki temu skraca się czas trwania operacji przejścia między trybem użytkownika i trybem jądra.

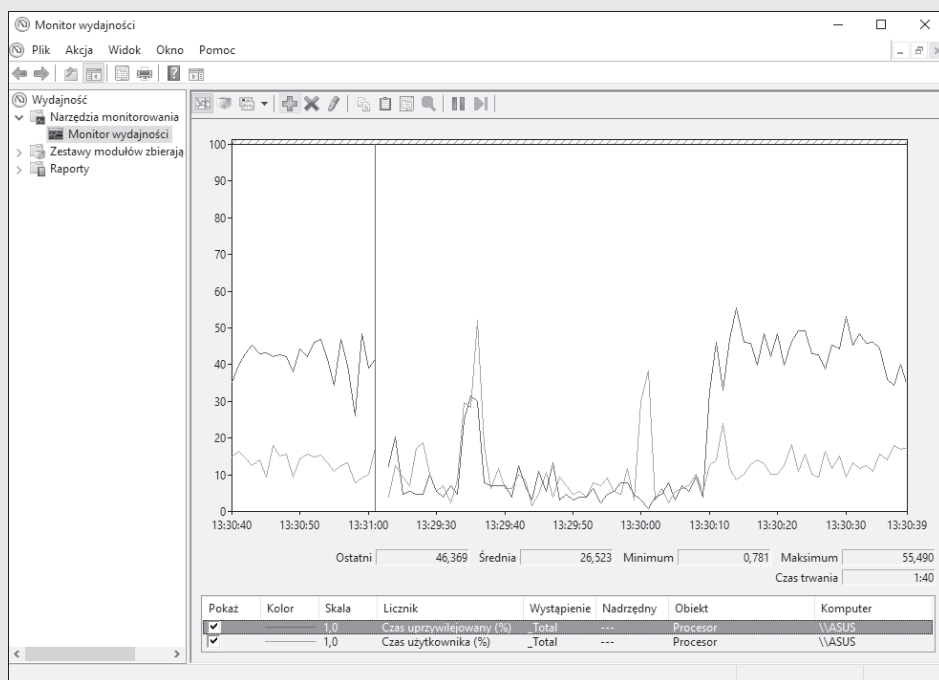
TABELA 1.3. Liczniki wydajności powiązane z trybami

Obiekt: licznik	Funkcja
Procesor: Czas uprzywilejowany (%)	Wartość procentowa czasu, przez jaki pojedynczy procesor (lub wszystkie procesory) musi działać w trybie jądra podczas określonego interwału.
Procesor: Czas użytkownika (%)	Wartość procentowa czasu, przez jaki pojedynczy procesor (lub wszystkie procesory) musi działać w trybie użytkownika podczas określonego interwału.
Proces: Czas uprzywilejowany (%)	Wartość procentowa czasu, przez jaki wątki w procesie muszą działać w trybie jądra podczas określonego interwału.
Proces: Czas użytkownika (%)	Wartość procentowa czasu, przez jaki wątki w procesie muszą działać w trybie użytkownika podczas określonego interwału.
Wątek: Czas uprzywilejowany (%)	Wartość procentowa czasu, przez jaki wątek musi działać w trybie jądra podczas określonego interwału.
Wątek: Czas użytkownika (%)	Wartość procentowa czasu, przez jaki wątek musi działać w trybie użytkownika podczas określonego interwału.

EKSPERYMENT: Porównanie trybu użytkownika i trybu jądra

Za pomocą narzędzia Monitor wydajności możesz sprawdzić, ile czasu system spędza odpowiednio na działaniu w trybie jądra i trybie użytkownika. Wykonaj następujące kroki:

1. Wyświetl menu *Start* i wpisz **Monitor wydajności** (polecenie powinno zostać zasugerowane przed zakończeniem wpisywania go), aby uruchomić Monitor wydajności.
2. Wybierz węzeł *Monitor wydajności* poniżej węzła *Wydajność/Narzędzia monitorowania* w drzewie po lewej stronie.
3. W celu usunięcia domyślnego licznika pokazującego całkowity czas procesora kliknij przycisk *Usuń* na pasku narzędzi lub naciśnij klawisz *Delete* klawiatury.
4. Kliknij przycisk *Dodaj (+)* na pasku narzędzi.
5. Rozwiń sekcję licznika *Procesor*, kliknij licznik *Czas uprzywilejowany (%)*, a następnie, trzymając wciśnięty klawisz *Ctrl*, kliknij licznik *Czas użytkownika (%)*.
6. Kliknij kolejno przyciski *Dodaj* i *OK*.
7. Otwórz okno wiersza poleceń i wpisz polecenie `dir \\%computername%\c$ /s`, aby uruchomić skanowanie katalogów dysku C.



8. Po zakończeniu operacji zamknij narzędzie.

Te same informacje możesz uzyskać też za pomocą Menedżera zadań. Wystarczy kliknąć kartę *Wydajność*, prawym przyciskiem myszy kliknąć wykres procesora i wybrać opcję *Pokaż czas jądra*. Na pasku wykorzystania procesora pojawi się czas spędzony przez procesor w trybie jądra wyróżniony ciemniejszym odcieniem koloru jasnoniebieskiego.

Aby sprawdzić, ile czasu działa sam Monitor wydajności w trybie jądra i trybie użytkownika, ponownie uruchom to narzędzie, lecz dla każdego procesu w systemie dodaj osobne liczniki procesu *Czas użytkownika (%)* i *Czas uprzywilejowany (%)*:

1. Jeśli narzędzie Monitor wydajności jeszcze nie działa, uruchom je ponownie (jeżeli już działa, rozpocznij od pustego widoku, klikając prawym przyciskiem myszy w obszarze wykresu i wybierając pozycję *Usuń wszystkie liczniki*).
2. Kliknij przycisk *Dodaj* na pasku narzędzi.
3. W dostępnym obszarze liczników rozwiń sekcję *Proces*.
4. Wybierz liczniki *Czas uprzywilejowany (%)* i *Czas użytkownika (%)*.
5. W polu *Wystąpienia wybranego obiektu* wybierz kilka procesów (np. *mmc*, *csrss* i *Idle*).
6. Kliknij kolejno przyciski *Dodaj* i *OK*.
7. Przesuń szybko kursor myszy do tyłu i do przodu.
8. Użyj kombinacji klawiszy *Ctrl+H*, aby włączyć tryb wyróżniania. Spowoduje to wyróżnienie na czarno aktualnie wybranego licznika.
9. Przewiń liczniki do dołu widoku, aby zidentyfikować procesy, których wątki zostały uruchomione w momencie przesunięcia kursora myszy. Zwróć uwagę, czy zostały one uruchomione w trybie użytkownika, czy w trybie jądra.

Po przesunięciu kursora myszy powinno być widoczne w oknie narzędzia Monitor wydajności, że w kolumnie *Wystąpienie* procesu *mmc* zwiększa się czas dla trybu jądra i trybu użytkownika. Wynika to stąd, że proces wykonuje kod aplikacji w trybie użytkownika i wywołuje funkcje systemu Windows, które działają w trybie jądra. Zauważysz również aktywność wątku w trybie jądra w procesie o nazwie *csrss* w momencie przesunięcia kursora myszy. Powodem tej aktywności jest to, że do tego procesu dołączony jest związany z podsystemem systemu Windows wątek nieprzetworzonych danych wejściowych trybu jądra, który obsługuje dane wejściowe myszy i klawiatury (w rozdziale 2. zamieszczono więcej informacji o wątkach systemowych i podsystemach). Proces *Idle*, który niemal 100% swojego czasu spędza w trybie jądra, w rzeczywistości nie jest procesem. Jest to fałszywy proces używany do uwzględniania bezczynnych cykli procesora. Jak możesz zaobserwować na podstawie trybu, w jakim działają wątki procesu *Idle*, gdy system Windows nie ma żadnych operacji do wykonania, działa w trybie jądra.

Hipernadzorca

Ostatnie zmiany w modelach aplikacji i oprogramowania, takie jak wprowadzenie usługi w chmurze oraz wszechobecność urządzeń IoT, spowodowały konieczność określenia przez dostawców systemów operacyjnych i sprzętu bardziej efektywnych sposobów wirtualizacji innych „gości” systemu z wykorzystaniem urządzeń komputera będącego hostem. Jest to niezbędne niezależnie od tego, czy ma na celu umożliwienie udostępnienia wielu dzierżawców w farmie serwerów i uruchomienia na pojedynczym serwerze 100 izolowanych witryn internetowych, czy zapewnienie projektantom możliwości testowania dziesiątek różnych wariantów systemu operacyjnego bez konieczności kupowania dedykowanego sprzętu. Potrzeba zastosowania szybkiej, efektywnej i bezpiecznej wirtualizacji przyczyniła się do pojawienia się nowych związanych z oprogramowaniem modeli dotyczących przeprowadzania obliczeń i logiki.

Okazuje się, że obecnie określone oprogramowanie, takie jak Docker, który obsługiwany jest przez systemy Windows 10 i Windows Server 2016, działa w kontenerach zapewniających w pełni izolowane maszyny wirtualne zaprojektowane wyłącznie pod kątem uruchamiania stosu lub środowiska jednej aplikacji. Oznacza to, że granice dotyczące „gościa” i hosta zostały przesunięte jeszcze dalej.

W celu zapewnienia takich usług wirtualizacji w niemal wszystkich nowoczesnych rozwiązaniach zastosowano *hipernadzorcę* (ang. *hypervisor*), czyli specjalizowany komponent o bardzo dużych przywilejach, który umożliwia wirtualizację i izolowanie wszystkich zasobów komputera, począwszy od pamięci wirtualnej, a skończywszy na pamięci fizycznej, przerwaniach sprzętowych, a nawet urządzeniach PCI i USB. Hyper-V to przykład takiego hipernadzorca, który obsługuje funkcjonalność klienta Hyper-V dostępną w systemie Windows 8.1 oraz jego następcach. W konkurencyjnych produktach, takich jak Xen, KVM, VMware i VirtualBox, implementowany jest ich własny hipernadzorca. Każdy z nich ma swoje słabe i mocne strony.

Ze względu na swoje szczególnie duże przywileje i to, że hipernadzorca dysponuje jeszcze większym poziomem dostępu niż samo jądro, zapewnia on wyraźną korzyść, która wykracza poza samo uruchamianie wielu instancji „gości” innych systemów operacyjnych. Hipernadzorca może chronić i monitorować pojedynczą instancję hosta w celu zapewnienia gwarancji większych niż oferowane przez jądro. W systemie Windows 10 firma Microsoft stosuje obecnie hipernadzorcę Hyper-V, aby udostępnić nowy zestaw mechanizmów *zabezpieczeń VBS* (ang. *Virtualization-Based Security*). Oto one:

- **Device Guard.** Mechanizm zapewnia usługę HVCI (ang. *Hypervisor Code Integrity*) w celu zaferowania lepszych gwarancji podpisywaniu kodu niż w porównaniu z samą zasadą KMCS. Mechanizm umożliwia dostosowywanie zasady podpisów systemu Windows, zarówno w wypadku trybu użytkownika, jak i trybu jądra.
- **Hyper Guard.** Mechanizm chroni kluczowe struktury danych i kod powiązane z jądrem i hipernadzorcą.
- **Credential Guard.** Mechanizm zapobiega nieautoryzowanemu dostępowi do danych uwierzytelniających i haseł kont domenowych, a ponadto oferuje bezpieczną technologię biometryczną.
- **Application Guard.** Mechanizm zapewnia jeszcze lepszą „piaskownicę” na potrzeby przeglądarki Microsoft Edge.
- **Host Guardian i Shielded Fabric.** Mechanizmy wykorzystują funkcję v-TPM (ang. *virtual TPM*) do ochrony maszyny wirtualnej przed infrastrukturą, w wypadku której ją uruchomiono.

Ponadto hipernadzorca Hyper-V pozwala za zastosowanie określonych, kluczowych ograniczeń jądra względem programów wyszukujących luki w zabezpieczeniach (ang. *exploits*) oraz innych rodzajów ataków. Kluczową zaletą wszystkich tych technologii jest to, że w przeciwieństwie do wcześniejszych ulepszeń zabezpieczeń opartych na jądrze, nie są one podatne na złośliwe lub źle napisane sterowniki, niezależnie od tego, czy są one podpisane, czy nie. Dzięki temu technologie te są wysoce odporne na obecnie istniejące zaawansowane rozwiązania tworzone przez osoby podejmujące ataki. Jest to możliwe z powodu zaimplementowania przez hipernadzorcę wirtualnych poziomów zaufania VTL (ang. *Virtual Trust Level*). Ponieważ standardowy system operacyjny i jego komponenty działają w mniej uprzywilejowanym trybie (VTL 0), a wymienione technologie VBS pracują w trybie VTL 1 (większe przywileje), wpływu na nie może nie mieć nawet kod w trybie jądra. W związku z tym kod pozostaje w obrębie obszaru z przywilejami trybu VTL 0. Tym sposobem poziomy VTL możesz traktować jako ortogonalne względem poziomów przywilejów procesora:

tryb jądra i tryb użytkownika istnieją *wewnątrz* każdego poziomu VTL, a hipernadzorca zarządza przywilejami *między* poziomami VTL. W rozdziale 2. zamieszczono dodatkowe szczegóły dotyczące architektury wspomaganej przez hipernadzorcę, a w rozdziale 7. omówiono dokładnie zaprezentowane wcześniej mechanizmy zabezpieczeń VBS.

Oprogramowanie sprzętowe

Komponenty systemu Windows w coraz większym stopniu są zależne od bezpieczeństwa systemu operacyjnego i jego jądra. Z kolei jądro bazuje obecnie na ochronie hipernadzorczy. Pojawia się pytanie odnośnie tego, co może zapewnić, że komponenty te są bezpiecznie ładowane, a ponadto mogą uwierzytelniać swoją zawartość. Jest to zwykle zadanie rozruchowego programu ładującego, który jednak również wymaga takiego samego poziomu sprawdzania uwierzytelniania, co powoduje utworzenie coraz bardziej złożonej hierarchii zaufania.

Co zatem zapewnia główny łańcuch zaufania, który może zagwarantować nieograniczonym proces rozruchu? W nowoczesnym systemie Windows 8 i jego następcach kwestia ta podlega systemowemu oprogramowaniu sprzętowemu, które w certyfikowanych systemach musi bazować na interfejsie UEFI (ang. *Unified Extensible Firmware Interface*). Bycie częścią standardu UEFI, który narzucany jest w systemie Windows (UEFI 2.3.1b; więcej informacji dostępnych jest pod adresem <http://www.uefi.org/>), oznacza konieczność obecności bezpiecznej implementacji rozruchu z silnymi gwarancjami i wymaganiami dotyczącymi jakości podpisu oprogramowania powiązanego z procesem rozruchu. Dzięki takiemu procesowi weryfikacji uzyskuje się gwarancję bezpiecznego ładowania komponentów systemu Windows od samego początku procesu rozruchu. Dodatkowo technologie takie jak TPM (ang. *Trusted Platform Module*) mogą dokonywać pomiaru procesu w celu zapewnienia poświadczenia (zarówno lokalnie, jak i zdalnie). Dzięki partnerstwu z przedstawicielami branży firma Microsoft zarządza „białą” i „czarną” listą zgodnych ze standardem UEFI komponentów bezpiecznego rozruchu w przypadku błędów lub luk w zabezpieczeniach oprogramowania rozruchowego. Aktualizacje systemu Windows obejmują też obecnie aktualizacje oprogramowania sprzętowego (warto w tym miejscu podkreślić jego znaczenie w nowoczesnej architekturze systemu Windows z punktu widzenia gwarancji, jakie ma zapewnić).

Usługi terminalowe i wiele sesji

Usługi terminalowe odnoszą się do obsługi w pojedynczym systemie Windows wielu interaktywnych sesji użytkownika. Dzięki usługom terminalowym system Windows użytkownik zdalny może ustanowić sesję na innym komputerze, zalogować się i uruchomić aplikacje na serwerze. Serwer przekazuje do klienta graficzny interfejs użytkownika (a także inne konfigurowalne zasoby, takie jak dźwięk i schowek). Klient transmituje dane wprowadzone przez użytkownika z powrotem do serwera (podobnie do środowiska X Window System, system Windows umożliwia uruchamianie poszczególnych aplikacji w systemie serwera, gdzie zamiast zdalnego przesyłania zawartości całego pulpitu dane są wyświetlane zdalnie po stronie klienta).

Pierwsza sesja jest uważana za sesję usług lub sesję zerową. Zawiera ona usługę systemową udostępniającą procesy. Pierwsza sesja logowania w konsoli fizycznej komputera to sesja 1. Dodatkowe sesje mogą być tworzone z wykorzystaniem programu Podłączanie pulpitu zdalnego (plik *Mstsc.exe*) lub funkcji szybkiego przełączania użytkowników.

Wersje klienckie systemu Windows zezwalają na nawiązanie połączenia z komputerem przez pojedynczego użytkownika zdalnego. Jeśli jednak ktoś jest zalogowany w konsoli, stacja robocza jest zablokowana. Oznacza to, że ktoś może korzystać z systemu lokalnie lub zdalnie, lecz nie jednocześnie. Wersje systemu Windows obejmujące wersję Windows Media Center umożliwiają jedną sesję interaktywną i maksymalnie cztery sesje urządzenia Windows Media Center Extender.

Systemy serwerowe Windows obsługują dwa jednoczesne połączenia zdalne. Ma to na celu ułatwienie zarządzania zdalnego (na przykład zastosowanie narzędzi zarządzania wymagających zalogowania na zarządzanym komputerze). Systemy te wspierają też więcej niż dwie sesje zdalne, jeśli zostaną odpowiednio skonfigurowane jako serwer terminali, a ponadto dysponują właściwą licencją.

Wszystkie wersje klienckie systemu Windows obsługują wiele sesji tworzonych lokalnie za pomocą funkcji *szybkiego przełączania użytkowników*. W danym momencie może być używana tylko jedna sesja. Gdy użytkownik zdecyduje się na rozłączenie swojej sesji, a nie wylogowanie (na przykład przez kliknięcie przycisku *Start* i ikony bieżącego użytkownika, a następnie wybranie z wyświetlonego podmenu pozycji *Przełącz konto* albo przez naciśnięcie klawisza *L* przy wciśniętym klawiszu logo systemu Windows i kliknięcie innego użytkownika w dolnym lewym narożniku ekranu), bieżąca sesja, czyli procesy działające w danej sesji oraz wszystkie struktury danych sesji opisujące ją, pozostaje aktywna w systemie, który przywraca główny ekran logowania (jeśli nie jest jeszcze widoczny). W przypadku zalogowania nowego użytkownika zostanie utworzona nowa sesja.

W wypadku aplikacji, które mają rozpoznawać fakt działania w sesji serwera terminali, dostępny jest zestaw interfejsów API systemu Windows służących do programowego wykrywania tego, a także do kontrolowania różnych aspektów usług terminalowych (związane z tym szczegóły znajdziesz w dokumentacji zestawu SDK systemu Windows i interfejsu API usług pulpitu zdalnego).

W rozdziale 2. w skrócie opisano sposób tworzenia sesji. Ponadto zamieszczono w nim kilka eksperymentów prezentujących, jak za pomocą różnych narzędzi (w tym debuggera jądra) wyświetlać informacje o sesjach. W rozdziale 5. przybliżono, jak menedżer pamięci przygotowuje dane całej sesji oraz nimi zarządza.

Obiekty i dojścia

W systemie operacyjnym Windows *obiekt jądra* to pojedyncza wykonawcza instancja statycznie zdefiniowanego typu obiektu. *Typ obiektu* składa się z typu danych definiowanego w systemie, funkcji przetwarzających instancje typu danych oraz zestawu atrybutów obiektu. Jeśli tworzysz aplikacje dla systemu Windows, możesz napotkać obiekty procesu, wątku, pliku i zdarzenia. A to tylko kilka przykładów. Obiekty te bazują na obiektach niższego poziomu tworzonych i zarządzanych przez system Windows. W systemie tym *proces* to instancja typu obiektu procesu, *plik* to instancja typu obiektu pliku itd.

Atrybut obiektu jest polem danych w obiekcie, które częściowo definiuje jego stan. Na przykład obiekt typu *proces* będzie mieć atrybuty, które obejmują identyfikator procesu, podstawowy priorytet planowania oraz wskaźnik do obiektu tokena dostępu. *Metody obiektu*, czyli środki umożliwiające manipulowanie obiektami, zazwyczaj wczytują lub zmieniają atrybuty obiektu. Na przykład metoda *otwierająca* procesu będzie akceptować identyfikator procesu jako dane wejściowe i zwracać wskaźnik do obiektu jako dane wyjściowe.



Uwaga. Istnieje parametr o nazwie `ObjectAttributes`, który jest dostarczany przez element wywołujący podczas tworzenia obiektu za pomocą interfejsów API menedżera obiektów jądra. Parametru tego nie należy jednak mylić z bardziej ogólnym znaczeniem terminu używanym w książce.

Najbardziej fundamentalną różnicą między obiektem i zwykłą strukturą danych jest to, że struktura wewnętrzna obiektu jest nieprzejrzysta. W celu uzyskania danych z obiektu lub umieszczenia w nim danych niezbędne jest wywołanie usługi obiektu. Nie możesz bezpośrednio wczytać lub zmodyfikować danych wewnątrz obiektu. Różnica ta oddziela bazową implementację obiektu od kodu, który tylko z niego korzysta. Jest to technika umożliwiająca łatwe modyfikowanie z upływem czasu implementacji obiektu.

Dzięki wsparciu komponentu jądra nazywanego *menedżerem obiektów* obiekty zapewniają wygodne metody realizowania czterech następujących ważnych zadań systemu operacyjnego:

- Zapewnianie czytelnych dla użytkownika nazw zasobów systemowych.
- Współużytkowanie zasobów i danych przez procesy.
- Ochrona zasobów przed nieautoryzowanym dostępem.
- Śledzenie odwołań, które umożliwia systemowi określanie momentu, kiedy obiekt nie jest już dłużej używany, dlatego może zostać dla niego wykonana automatycznie operacja usuwania alokacji.

Nie wszystkie struktury danych w systemie operacyjnym Windows są obiektami. W obiektach umieszczane są tylko te dane, które wymagają współużytkowania, ochrony, nadania nazwy lub udostępnienia programom w trybie użytkownika (za pośrednictwem usług systemowych). Obiektami nie są struktury stosowane przez tylko jeden komponent systemu w celu implementacji funkcji wewnętrznych.

Zabezpieczenia

System Windows od początku zaprojektowano tak, aby był bezpieczny i spełniał wymagania różnych formalnych, zarówno rządowych, jak i branżowych wskaźników bezpieczeństwa, takich jak specyfikacja CCITSE (ang. *Common Criteria for Information Technology Security Evaluation*). Uzyskanie wskaźnika bezpieczeństwa akceptowanego na szczeblu rządowym pozwala systemowi operacyjnemu konkurować w tym obszarze. Oczywiście wiele związanych z tym możliwości to korzystne funkcje dowolnego systemu obsługującego wielu użytkowników.

Podstawowe możliwości systemu Windows związane z bezpieczeństwem obejmują następujące:

- Nieokreślona (na żądanie) i obowiązkowa ochrona wszystkich obiektów systemowych, które mogą być współużytkowane, takich jak pliki, katalogi, procesy, wątki itd.
- Audyt zabezpieczeń w celu umożliwienia zestawienia podmiotów lub użytkowników oraz inicjowanych przez nich działań.
- Uwierzytelnianie użytkownika podczas logowania.
- Uniemożliwienie jednemu użytkownikowi uzyskania dostępu do niezainicjowanych zasobów, takich jak wolna pamięć lub przestrzeń dyskowa, które po przydzieleniu zostały zwrócone przez drugiego użytkownika.

W systemie Windows istnieją trzy następujące formy kontroli dostępu do obiektów:

- **Uznaniowa kontrola dostępu.** Jest to mechanizm ochrony, który ma na myśli większość osób zajmujących się zabezpieczeniami systemu operacyjnego. W wypadku tej metody dostępu właściciele obiektów (np. pliki lub drukarki) udzielają dostępu innym lub go odbierają. W momencie zalogowania użytkownicy uzyskują zestaw danych uwierzytelniających zabezpieczeń lub kontekst zabezpieczeń. Przy próbie uzyskania przez użytkowników dostępu do obiektów ich kontekst zabezpieczeń porównywany jest z listą kontroli dostępu obiektu, dla którego ma miejsce próba uzyskania dostępu. Ma to na celu stwierdzenie, czy użytkownicy mają uprawnienie do wykonania żądanej operacji. W przypadku systemów Windows Server 2012 i Windows 8 taką formę kontroli uznaniowej dodatkowo ulepszono przez zaimplementowanie kontroli dostępu opartej na atrybutach (nazywanej również dynamiczną kontrolą dostępu). Lista kontroli dostępu zasobu niekoniecznie jednak identyfikuje poszczególnych użytkowników i grupy. Zamiast tego identyfikuje wymagane atrybuty lub uprawnienia nadające dostęp do zasobu (np. „Poziom zezwolenia: ściśle tajne” lub „Staż pracy: 10 lat”). Dzięki możliwości automatycznego wprowadzania takich atrybutów przez analizowanie baz danych SQL i schematów za pośrednictwem usługi Active Directory ten znacznie bardziej elegancki i elastyczny model zabezpieczeń ułatwia organizacjom unikanie kłopotliwych hierarchii grup oraz ręcznego zarządzania grupami.
- **Uprzywilejowana kontrola dostępu.** Ta forma kontroli jest niezbędna w sytuacjach, gdy uznaniowa kontrola dostępu jest niewystarczająca. Jest to metoda zapewniania, że ktoś może uzyskać dostęp do chronionych obiektów, jeśli ich właściciel jest niedostępny. Jeśli na przykład pracownik opuści firmę, administrator musi dysponować możliwością uzyskania dostępu do plików, które mogły być dostępne tylko dla tego pracownika. W tym przypadku w systemie Windows administrator może przejąć prawa właściciela pliku, dzięki czemu w razie potrzeby może zarządzać jego prawami.
- **Obowiązkowa kontrola dostępu.** Ta forma kontroli jest wymagana, gdy niezbędny jest dodatkowy poziom kontroli zabezpieczeń w celu ochrony obiektów, do których uzyskiwany jest dostęp z poziomu tego samego konta użytkownika. Obowiązkowa kontrola dostępu jest stosowana w każdym przypadku, począwszy od zapewniania części technologii „piaskownicy” aplikacjom Windows Apps (więcej na ten temat w dalszej części rozdziału), a skończywszy na izolowaniu trybu chronionego przeglądarki Internet Explorer (oraz innych przeglądarek) od konfiguracji użytkownika oraz ochronie obiektów utworzonych przez administratora z większymi uprawnieniami przed dostępem z poziomu konta administratora o mniejszych uprawnieniach (w rozdziale 7. zamieszczono więcej informacji o komponencie Kontrola konta użytkownika).

Począwszy od systemu Windows 8, do udostępniania aplikacji Windows Apps używana jest „piaskownica” o nazwie *AppContainer*, która zapewnia izolację w odniesieniu do innych komponentów *AppContainer* oraz procesów niepowiązanych z aplikacjami Windows Apps. Kod w komponentach *AppContainer* może komunikować się z brokerami (nieizolowane procesy działające z danymi uwierzytelniającymi użytkownika), a czasami z innymi komponentami *AppContainer* lub procesami za pośrednictwem dobrze zdefiniowanych kontraktów udostępnianych przez architekturę Windows Runtime. Kanonicznym przykładem jest przeglądarka Microsoft Edge, która działa w obrębie komponentu *AppContainer*, a tym samym zapewnia lepszą ochronę przed złośliwym kodem uruchomionym w granicach tego komponentu. Ponadto projektanci zewnętrznego oprogramowania mogą wykorzystać komponenty *AppContainer* do izolowania w podobny sposób ich własnych aplikacji, które nie są aplikacjami Windows Apps. Model komponentów

AppContainer wymusza znaczną zmianę w tradycyjnych modelach programowania, powodując przejście z klasycznej implementacji wielowątkowej aplikacji z pojedynczym procesem do aplikacji z wieloma procesami.

Zabezpieczenia obejmują interfejs API systemu Windows. Jego podsystem implementuje zabezpieczenia oparte na obiektach w taki sam sposób, w jaki realizuje to sam system operacyjny, czyli przez ochronę współużytkowanych obiektów systemu Windows przed nieautoryzowanym dostępem, co sprowadza się do zastosowania dla nich systemowych deskryptorów zabezpieczeń. Gdy aplikacja po raz pierwszy próbuje uzyskać dostęp do współużytkowanego obiektu, podsystem systemu Windows sprawdza, czy prawo aplikacji na to zezwala. Jeśli kontrola zabezpieczeń się powiedzie, podsystem umożliwia aplikacji kontynuowanie działania.

Obszerne omówienie zabezpieczeń systemu Windows znajdziesz w rozdziale 7.

Rejestr

Jeśli korzystałeś z systemów operacyjnych Windows, prawdopodobnie słyszałeś o rejestrze lub sprawdzałeś jego zawartość. Nie możesz zbyt obszernie dyskutować o wewnętrznych mechanizmach systemu Windows bez odwoływania się do rejestru, ponieważ jest to systemowa baza danych zawierająca informacje wymagane do rozruchu i konfiguracji systemu, systemowe ustawienia oprogramowania kontrolujące działanie systemu Windows, bazę danych zabezpieczeń oraz ustawienia konfiguracyjne poszczególnych użytkowników (określające na przykład, jaki wygaszacz ekranu ma zostać użyty). Ponadto rejestr zapewnia wgląd w ulotne dane znajdujące się w pamięci, takie jak bieżący stan urządzenia systemu (jakie sterowniki urządzeń są ładowane, używane przez nie zasoby itd.), a także liczniki wydajności systemu Windows. Liczniki te, które w rzeczywistości nie znajdują się w rejestrze, mogą być dostępne za pośrednictwem jego funkcji (choć istnieje nowszy i lepszy interfejs API zapewniający dostęp do liczników wydajności).

Choć wielu użytkowników i administratorów systemu Windows nigdy nie będzie mieć potrzeby bezpośredniego sprawdzania zawartości rejestru (ponieważ większość ustawień konfiguracyjnych może być wyświetlana lub modyfikowana za pomocą standardowych narzędzi administracyjnych), w dalszym ciągu jest to przydatne źródło informacji o wewnętrznych mechanizmach systemu Windows. Wynika to z tego, że rejestr zawiera wiele ustawień mających wpływ na wydajność i zachowanie systemu. W różnych miejscach książki napotkasz odwołania do poszczególnych kluczy rejestru, gdy będą odnosić się one do opisywanego komponentu. Większość kluczy rejestru przywoływanych w książce znajduje się w gałęzi konfiguracji całego systemu `HKEY_LOCAL_MACHINE`, dla której będzie używany skrót `HKLM`.

Ostrzeżenie. Jeśli zdecydujesz się na bezpośrednie wprowadzanie zmian w ustawieniach rejestru, musisz zachować szczególną ostrożność. Wszelkie zmiany mogą niekorzystnie wpłynąć na wydajność systemu lub, co gorsza, uniemożliwić pomyślny rozruch systemu.

Unicode

System Windows różni się od większości innych systemów operacyjnych tym, że większość wewnętrznych łańcuchów tekstowych przechowywana i przetwarzana jest jako 16-bitowe znaki Unicode (dokładnie rzecz biorąc, znaki UTF-16LE; gdy w książce jest mowa o standardzie Unicode, dotyczy to wersji UTF-16LE, chyba że wskazano inaczej). Unicode to międzynarodowy

standard zestawu znaków, który definiuje unikatowe wartości dla większości znanych na świecie zestawów znaków. Dla każdego znaku standard zapewnia 8-bitowe, 16-bitowe, a nawet 32-bitowe kodowania.

Ponieważ wiele aplikacji ma do czynienia z 8-bitowymi (jednobajtowymi) łańcuchami znaków ANSI, wiele funkcji systemu Windows, które akceptują parametry łańcuchowe, używa dwóch punktów wejścia: wersji Unicode („szeroka”, 16-bitowa) oraz wersji ANSI („wąska”, 8-bitowa). Jeśli wywołasz „wąską” wersję funkcji systemu Windows, będzie to mieć niewielki wpływ na wydajność, ponieważ przed zwróceniem aplikacji wejściowe parametry łańcuchowe są przekształcane z formatu Unicode do formatu ANSI. Jeśli zatem używasz starszej usługi lub porcji kodu wymagających uruchomienia w systemie Windows, ale kod ten napisano z wykorzystaniem łańcuchów tekstowych ze znakami ANSI, na własny użytek system dokona przekształcenia znaków ANSI do formatu Unicode. System Windows nigdy jednak nie konwertuje *danych* wewnątrz plików. Od aplikacji zależne jest to, czy dane zostaną zapisane w formacie Unicode, czy w formacie ANSI.

Niezależnie od języka, wszystkie wersje systemu Windows zawierają te same funkcje. Zamiast osobnych wersji językowych system korzysta z pojedynczych danych binarnych o zasięgu globalnym. Dzięki temu jedna instalacja może obsługiwać wiele języków (przez dodawanie różnych pakietów językowych). Aplikacje mogą również skorzystać z funkcji systemu Windows, które zezwalają na pojedyncze, globalne dane binarne aplikacji, które mogą obsługiwać wiele języków.



Uwaga. Starsze systemy operacyjne Windows 9x były pozbawione natywnej obsługi standardu Unicode. Był to jeszcze jeden powód ku temu, aby utworzyć dwie funkcje na potrzeby standardów Unicode i ANSI. Na przykład funkcja API `CreateFile` systemu Windows wcale nie jest funkcją. Jest to makro rozwijane do postaci jednej z dwóch funkcji: `CreateFileA` (ANSI) lub `CreateFileW` (Unicode, gdzie *W* odpowiada słowu *wide*). Rozwinięcie oparte jest na stałej kompilacji o nazwie `UNICODE`. Definiowana jest ona domyślnie w projektach C++ środowiska Visual Studio, gdyż korzystniejsze jest używanie funkcji Unicode. W miejsce odpowiedniego makra można jednak zastosować jawnie podaną nazwę funkcji. W zamieszczonym poniżej eksperymencie zaprezentowano takie pary funkcji.

EKSPERYMENT: Wyświetlanie wyeksportowanych funkcji

W tym eksperymencie zostanie użyte narzędzie Dependency Walker do wyświetlenia funkcji wyeksportowanych z biblioteki DLL podsystemu systemu Windows.

1. Pod adresem <http://www.dependencywalker.com/> pobierz narzędzie Dependency Walker. Jeśli używasz systemu 32-bitowego, pobierz 32-bitową wersję narzędzia. W przypadku systemu 64-bitowego pobierz wersję 64-bitową. Wyodrębnij następnie pobrany plik ZIP do wybranego folderu.
2. Uruchom narzędzie (plik `depends.exe`). Wyświetl następnie menu *File* i wybierz pozycję *Open*, aby przejść do folderu `C:\Windows\System32` (zakładając, że system Windows zainstalowano na dysku C). Zlokalizuj plik `kernel32.dll` i kliknij przycisk *Otwórz*.
3. Narzędzie Dependency Walker może wyświetlić okno komunikatu ostrzeżenia. Zignoruj i zamknij okno komunikatu.
4. Widocznych będzie kilka widoków z poziomymi i pionowymi paskami podziału. Upewnij się, że pozycja wybrana w lewym górnym widoku drzewa to plik `kernel32.dll`.

5. Spójrz na drugi widok od góry po prawej stronie. Widok ten wyszczególnia wyeksportowane funkcje dostępne w pliku *kernel32.dll*. Kliknij nagłówek listy *Function*, aby zastosować sortowanie według nazwy. Znajdź następnie funkcję *CreateFileA*. Niewiele niżej znajdziesz funkcję *CreateFileW*.

PI	Ordinal ^	Hint	Function	Entry Point
	192 (0x0C0)	189 (0x0BD)	CreateFiber	0x0029FA0
	193 (0x0C1)	190 (0x0BE)	CreateFiberEx	0x0029FB0
	194 (0x0C2)	191 (0x0BF)	CreateFile2	0x00298A0
	195 (0x0C3)	192 (0x0C0)	CreateFileA	0x00298B0
	196 (0x0C4)	193 (0x0C1)	CreateFileMappingA	0x001A340
	197 (0x0C5)	194 (0x0C2)	CreateFileMappingFromApp	api-ms-win-core-memory-l1-1-1.CreateFileMappingFromApp
	198 (0x0C6)	195 (0x0C3)	CreateFileMappingNumaA	0x005BF30
	199 (0x0C7)	196 (0x0C4)	CreateFileMappingNumaW	0x0036E60
	200 (0x0C8)	197 (0x0C5)	CreateFileMappingW	0x001CD50
	201 (0x0C9)	198 (0x0C6)	CreateFileTransactedA	0x005B7E0
	202 (0x0CA)	199 (0x0C7)	CreateFileTransactedW	0x005B840
	203 (0x0CB)	200 (0x0C8)	CreateFileW	0x00393C0
	204 (0x0CC)	201 (0x0C9)	CreateHardLinkA	0x0036B80
	205 (0x0CD)	202 (0x0CA)	CreateHardLinkTransactedA	0x003DC90
	206 (0x0CE)	203 (0x0CB)	CreateHardLinkTransactedW	0x005BF40
	207 (0x0CF)	204 (0x0CC)	CreateHardLinkW	0x0036BA0
	208 (0x0D0)	205 (0x0CD)	CreateIoCompletionPort	0x0028820

6. Jak widać, większość funkcji zawierających przynajmniej jeden argument typu łańcuchowego to w rzeczywistości pary funkcji. Na powyższym zrzucie ekranu widoczne są następujące funkcje: *CreateFileMappingA/CreateFileMappingW*, *CreateFileTransactedA/CreateFileTransactedW* i *CreateFileMappingNumaA/CreateFileMappingNumaW*.
7. W celu zlokalizowania innych funkcji możesz przewinąć listę. Możesz też otworzyć inne pliki systemowe, takie jak *user32.dll* i *advapi32.dll*.



Uwaga. Interfejsy API oparte na modelu COM w systemie Windows używają zwykle łańcuchów Unicode, które czasami są podawane przy użyciu typu BSTR. Zasadniczo jest to zakończona znakiem sterującym NULL tablica znaków Unicode o długości łańcucha wyrażonej w bajtach, która zapisywana jest 4 bajty przed początkiem tablicy znaków w pamięci. Interfejsy API środowiska Windows Runtime korzystają wyłącznie z łańcuchów Unicode podawanych przy użyciu typu HSTRING, który reprezentuje niezmienną tablicę znaków Unicode.

Więcej informacji o standardzie Unicode znajdziesz pod adresem <http://www.unicode.org/> oraz w dokumentacji dotyczącej programowania w bibliotece MSDN Library.

Analizowanie wewnętrznych mechanizmów systemu Windows

Choć spora część informacji zawartych w książce jest wynikiem analizowania kodu źródłowego systemu Windows i dyskusji prowadzonych z projektantami, nie musisz *wszystkiego* przyjmować na wiarę. Wiele szczegółów dotyczących wewnętrznych mechanizmów systemu Windows może zostać uzyskanych i zademonstrowanych przy użyciu różnych dostępnych narzędzi, takich jak dołączone do systemu Windows oraz jego narzędzi debugowania. Te pakiety narzędzi omówiono w skrócie w dalszej części rozdziału.

Aby zachęcić do eksplorowania wewnętrznych mechanizmów systemu Windows, w książce rozmieszczono ramki eksperymentów opisujących kroki, jakie możesz wykonać w celu sprawdzenia określonego aspektu związanego z wewnętrznym działaniem systemu Windows (wcześniej w rozdziale zamieszczono już kilka takich ramek). Zachęcamy do spróbowania przeprowadzenia tych eksperymentów, aby w praktyce sprawdzić wiele z opisanych w książce zagadnień związanych z wewnętrznymi mechanizmami systemu Windows.

W tabeli 1.4 zamieszczono listę podstawowych narzędzi używanych w książce, a także podano, skąd je uzyskać.

TABELA 1.4. Narzędzia służące do sprawdzania wewnętrznych mechanizmów systemu Windows

Narzędzie	Nazwa obrazu	Źródło
Startup Programs Viewer	AUTORUNS	Sysinternals
Access Check	ACCESSCHK	Sysinternals
Dependency Walker	DEPENDS	www.dependencywalker.com
Global Flags	GFLAGS	Debugging Tools
Handle Viewer	HANDLE	Sysinternals
Kernel debuggers	WINDBG, KD	WDK, Windows SDK
Object Viewer	WINOBJ	Sysinternals
Monitor wydajności	PERFMON.MSC	Wbudowane narzędzie systemu Windows
Pool Monitor	POOLMON	WDK
Process Explorer	PROCEXP	Sysinternals
Process Monitor	PROCMON	Sysinternals
Task (Process) List	TLIST	Debugging Tools
Menedżer zadań	TASKMGR	Wbudowane narzędzie systemu Windows

Monitor wydajności i Monitor zasobów

W książce odwołujemy się do narzędzia Monitor wydajności, dostępnego z poziomu folderu *Narzędzia administracyjne* panelu sterowania lub po wpisaniu polecenia **perfmon** w oknie dialogowym *Uruchamianie*. Dokładniej rzecz ujmując, koncentrujemy się na narzędziach Monitor wydajności i Monitor zasobów.

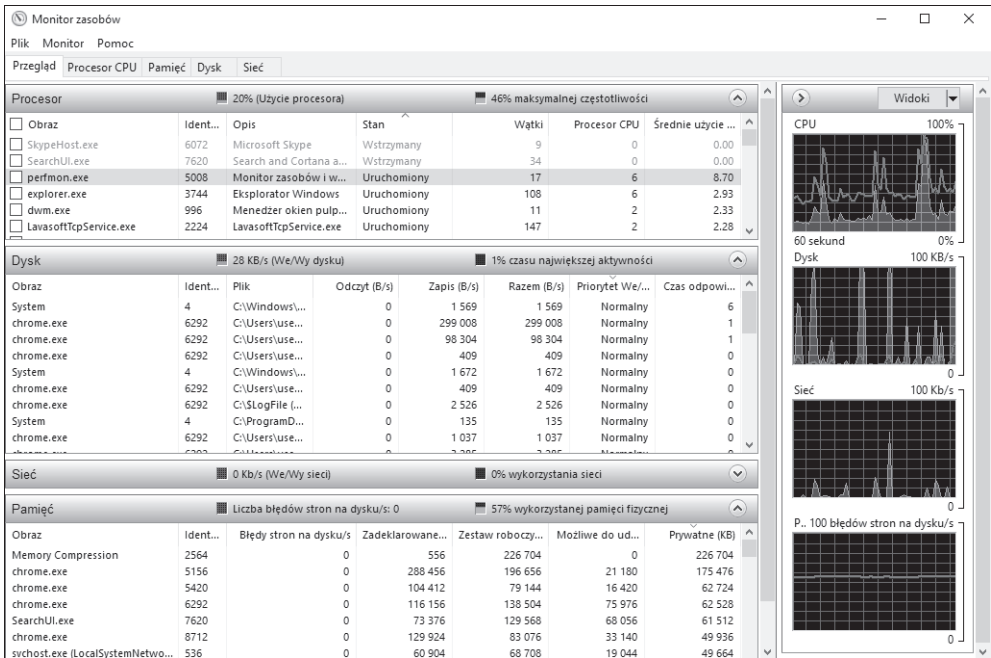


Uwaga. Monitor wydajności pełni trzy funkcje: monitorowanie systemu, wyświetlanie dzienników liczników wydajności i ustawianie alertów (przy użyciu zestawów modułów zbierających dane, które również zawierają dzienniki liczników wydajności oraz dane konfiguracji i śledzenia). Dla uproszczenia, gdy odwołujemy się do Monitora wydajności, mamy na myśli wchodzącą w skład tego narzędzia funkcję monitorowania systemu.

Monitor wydajności zapewnia więcej informacji o tym, jak działa system, niż jakiegokolwiek inne pojedyncze narzędzie. Monitor wydajności uwzględnia setki podstawowych i rozszerzalnych liczników różnych obiektów. W wypadku każdego głównego zagadnienia opisanego w książce

dołączono tabelę z odpowiednimi licznikami wydajności systemu Windows. Monitor wydajności zawiera krótki opis każdego licznika. Aby wyświetlić opisy, wybierz licznik w oknie *Dodawanie liczników* i zaznacz opcję *Pokaż opis*.

Choć wszystkie zaprezentowane w książce operacje niskopoziomowego monitorowania systemu mogą zostać zrealizowane za pomocą Monitora wydajności, system Windows oferuje również narzędzie Monitor zasobów (dostępne z menu *Start* lub na karcie *Wydajność* menedżera zadań), które zapewnia cztery podstawowe zasoby systemowe: procesor, dysk, sieć i pamięć. W wypadku ich podstawowych stanów dla zasobów tych wyświetlany jest ten sam poziom informacji, jaki możesz znaleźć w menedżerze zadań. Monitor zasobów udostępnia też jednak sekcje, które mogą być rozwijane w celu uzyskania dodatkowych informacji. Poniżej pokazano typowy widok okna narzędzia Monitor zasobów.



Po rozwinięciu karta *Procesor CPU* wyświetla informacje dotyczące użycia procesora przez poszczególne procesy, tak jak w wypadku menedżera zadań. W obrębie tej karty dodano jednak kolumnę informującą o średnim użyciu procesora, co może pozwolić lepiej zorientować się w tym, jakie procesy są najbardziej aktywne. Karta uwzględnia również osobną sekcję prezentującą usługi oraz powiązane z nimi użycie procesora i średnie użycie. Każdy proces udostępniający usługi identyfikowany jest przez grupę usług przez niego oferowanych. Podobnie jak w wypadku narzędzia Process Explorer wybranie procesu (przez kliknięcie powiązanego z nim pola wyboru) spowoduje wyświetlenie listy nazwanych dojsć otwartych przez proces, a także listy modułów (np. bibliotek DLL), które są ładowane w obszarze adresów procesu. Pole *Wyszukaj dojsca* może posłużyć do sprawdzenia, jakie procesy otworzyły dojsce do danego nazwanego zasobu.

Choć karta *Pamięć* wyświetla sporo tych samych informacji, jakie można uzyskać w menedżerze zadań, są one w uporządkowany sposób przedstawione dla całego systemu. Wykres słupkowy pamięci fizycznej prezentuje bieżącą organizację pamięci fizycznej podzieloną na następujące kategorie: sprzętowa zarezerwowana, w użyciu, zmodyfikowana, wstrzymana i wolna. W rozdziale 5. znajdziesz dokładne znaczenie tych terminów.

Z kolei karta *Dysk* oferuje dla poszczególnych plików informacje związane z operacjami wejścia-wyjścia w sposób, który ułatwia identyfikację w systemie najczęściej używanych, najczęściej zapisywanych lub najczęściej odczytywanych plików. Uzyskane wyniki mogą być dalej odfiltrowywane według procesu.

Karta *Siec* wyświetla aktywne połączenia sieciowe, procesy, do których one należą, a także informację o tym, ile danych przesyłanych jest z wykorzystaniem tych połączeń. Informacje te umożliwiają sprawdzenie aktywności sieciowej w tle, która może być trudna do określenia w inny sposób. Oprócz tego, karta zawiera aktywne w systemie połączenia TCP zorganizowane według procesów z uwzględnieniem takich danych, jak zdalny i lokalny port oraz adres, a także opóźnienie pakietów. I wreszcie, karta udostępnia listę portów nasłuchujących według procesu. Dzięki temu administrator może stwierdzić, jakie usługi lub aplikacje oczekują aktualnie na połączenia na danym porcie. Wyświetlana jest też zasada dotycząca protokołu i zapory sieciowej dla każdego portu i procesu.



Uwaga. Wszystkie liczniki wydajności systemu Windows są dostępne w sposób programowy. Więcej informacji znajdziesz w dokumentacji witryny MSDN po wpisaniu w polu wyszukiwania terminu **liczniki wydajności**.

Debugowanie jądra

Debugowanie jądra oznacza sprawdzanie wewnętrznych struktur danych jądra i/lub krokowe wykonywanie funkcji w jądrze. Jest to przydatny sposób kontrolowania wewnętrznych mechanizmów systemu Windows, ponieważ dzięki temu możesz uzyskać związane z nimi informacje, które nie są dostępne w wypadku żadnych innych narzędzi. Poza tym, bardziej przejrzyste staje się to, jak kod wykonywany jest wewnątrz jądra. Przed opisaniem różnych możliwych sposobów debugowania jądra przyjrzyjmy się zestawowi plików, które będą niezbędne do przeprowadzenia dowolnego typu debugowania jądra.

Symbole powiązane z debugowaniem jądra

Pliki symboli zawierają nazwy funkcji i zmiennych oraz układ i format struktur danych. Pliki są generowane przez konsolidator i używane przez debuggery do przywoływania i wyświetlania tych nazw w trakcie sesji debugowania. Informacje te nie są zwykle przechowywane w obrazie binarnym, ponieważ nie jest wymagane wykonywanie kodu. Oznacza to, że binaria są mniejsze i szybsze. Oznacza to też jednak, że podczas debugowania musisz upewnić się, że debugger może uzyskać dostęp do plików symboli powiązanych z obrazami przywoływanymi podczas sesji debugowania.

W celu użycia dowolnego z narzędzi debugowania jądra do sprawdzenia wewnętrznych struktur danych jądra systemu Windows, takich jak lista procesów, bloki wątków, lista załadowanych sterowników, informacje o użyciu pamięci itd., musisz dysponować poprawnymi plikami symboli przynajmniej dla obrazu jądra *Ntoskrnl.exe* (więcej o tym pliku dowiesz się w podrozdziale „Opis architektury systemu” rozdziału 2.). Pliki w tabeli symboli muszą być zgodne z wersją obrazu, z którego zostały uzyskane. Jeśli na przykład instalujesz pakiet Service Pack lub poprawkę systemu Windows, które aktualizują jądro, musisz uzyskać dopasowane, zaktualizowane pliki symboli.

Choć możliwe jest pobranie i zainstalowanie symboli dla różnych wersji systemu Windows, nie zawsze dostępne są zaktualizowane symbole dla poprawek. Najprostszym sposobem uzyskania poprawnej wersji symboli na potrzeby debugowania jest zastosowanie serwera symboli na żądanie firmy Microsoft za pomocą specjalnej składni ścieżki symboli podawanej w debuggerze. Na przykład następująca ścieżka symboli powoduje załadowanie przez narzędzia debugowania wymaganych symboli z internetowego serwera symboli i utrzymywanie kopii lokalnej w folderze `C:\symbols`:

```
srv*c:\symbols*http://msdl.microsoft.com/download/symbols
```

Debugging Tools for Windows

Zestaw Debugging Tools for Windows zawiera zaawansowane narzędzia debugowania, które w książce są wykorzystywane do eksplorowania wewnętrznych mechanizmów systemu Windows. Najnowsza wersja zestawu została dołączona jako część pakietu Windows SDK (pod adresem <https://msdn.microsoft.com/en-us/library/windows/hardware/ff551063.aspx> znajdziesz więcej szczegółów o różnych typach instalacji). Narzędzia te mogą posłużyć do debugowania procesów trybu użytkownika, a także jądra.

W skład narzędzi wchodzi cztery debuggery: `cdb`, `ntsd`, `kd` i `WinDbg`. Wszystkie bazują na jednym mechanizmie debugowania, zawartym w pliku `DbgEng.dll`, który dość dobrze udokumentowano w pliku pomocy narzędzi. Oto krótki przegląd debuggerów:

- `cdb` i `ntsd` to debuggery trybu użytkownika oparte na interfejsie użytkownika konsoli. Jedyną różnicą między nimi jest to, że debugger `ntsd` otwiera nowe okno konsoli w wypadku aktywowania go z poziomu istniejącego okna konsoli, natomiast debugger `cdb` tego nie robi.
- `kd` to debugger trybu jądra oparty na interfejsie użytkownika konsoli.
- `WinDbg` może pełnić rolę debuggera zarówno trybu użytkownika, jak i trybu jądra, ale nie jednocześnie. Debugger zapewnia użytkownikowi interfejs graficzny.
- Debuggery trybu użytkownika (`cdb`, `ntsd` oraz odpowiednio uruchomione narzędzie `WinDbg`) są w zasadzie równorzędne. To, który z nich zostanie użyty, jest kwestią preferencji.
- Debuggery trybu jądra (`kd` oraz odpowiednio uruchomione narzędzie `WinDbg`) są w zasadzie równorzędne.

Debugowanie w trybie użytkownika

Narzędzia debugowania mogą też zostać wykorzystane do dołączenia do procesu trybu użytkownika oraz do sprawdzenia i/lub wprowadzenia zmiany w pamięci procesu. W wypadku dołączania do procesu dostępne są następujące dwie opcje:

- **Inwazyjna.** Jeśli nie określono inaczej, w momencie dołączania do działającego procesu używana jest funkcja `DebugActiveProcess` systemu Windows w celu ustanowienia połączenia między debuggerem i celem debugowania. Umożliwia to sprawdzenie i/lub wprowadzenie zmiany w pamięci procesu, ustawienie punktów wstrzymania oraz wykonanie innych funkcji debugowania. System Windows pozwala na zatrzymanie debugowania bez kończenia działania procesu docelowego, pod warunkiem że debugger zostanie odłączony, a nie wyłączony.

- **Nieinwazyjna.** W przypadku tej opcji debugger po prostu otwiera proces za pomocą funkcji `OpenProcess`. Debugger nie wykonuje operacji dołączenia do procesu. Umożliwia to sprawdzenie i/lub wprowadzenie zmiany w pamięci procesu docelowego, lecz nie ustawienie punktów wstrzymania. Oznacza to również, że możliwe jest nieinwazyjne dołączenie nawet wtedy, gdy w sposób inwazyjny został dołączony inny debugger.

Za pomocą narzędzi debugowania możesz też otwierać pliki zrzutów pamięci procesu w trybie użytkownika.

Debugowanie w trybie jądra

Jak już wspomniano, dostępne są dwa debugery, które mogą posłużyć do debugowania jądra: debugger działający w trybie wiersza poleceń (*Kd.exe*) i debugger z graficznym interfejsem użytkownika (*Windbg.exe*). Możliwe jest wykonanie za pomocą tych narzędzi trzech następujących typów operacji debugowania jądra:

- Otwarcie pliku zrzutu pamięci będącego wynikiem awarii systemu Windows.
- Nawiazywanie połączenia z działającym systemem i sprawdzanie jego stanu (lub ustawianie punktów wstrzymania, jeśli debugowany jest kod sterownika urządzenia). Operacja ta wymaga dwóch komputerów: docelowego (z debugowanym systemem) i hosta (z uruchomionym debuggerem). Komputer docelowy może zostać połączony z hostem za pośrednictwem kabla Null Modem, kabla IEEE 1394, kabla do debugowania USB 2.0/3.0 lub sieci lokalnej. Rozruch systemu komputera docelowego musi się odbyć w trybie debugowania. System może zostać skonfigurowany pod kątem rozruchu w trybie debugowania za pomocą programu *Bcdedit.exe* lub *Mscnig.exe* (zauważ, że może być konieczne wyłączenie opcji bezpiecznego rozruchu w ustawieniach UEFI BIOS-u). Możliwe jest też nawiązanie połączenia z wykorzystaniem nazwanego potoku (co jest przydatne podczas debugowania systemu Windows 7 lub wcześniejszych wersji systemu Windows przy użyciu oprogramowania maszyn wirtualnych, takich jak Hyper-V, Virtual Box lub VMWare Workstation) przez udostępnienie portu szeregowego systemu operacyjnego „gościa” jako urządzenia nazwanego potoku. W wypadku „gości” z systemem Windows 8 lub nowszym należy użyć debugowania opartego na sieci lokalnej, udostępniając sieć tylko z hostem za pomocą wirtualnej karty sieciowej w systemie operacyjnym „gościa”. Spowoduje to tysiącrotny wzrost wydajności.
- System Windows umożliwia też nawiązanie połączenia z komputerem lokalnym i sprawdzenie stanu systemu. Jest to określane mianem *lokalnego debugowania jądra*. Aby je zainicjować za pomocą debuggera WinDbg, upewnij się najpierw, że system został ustawiony w trybie debugowania (na przykład przez uruchomienie programu *mscnig.exe*, kliknięcie karty *Rozruch*, a następnie kliknięcie przycisku *Opcje zaawansowane* i zaznaczenie opcji *Debuguj* oraz zrestartowanie systemu Windows). Wywołaj debugger WinDbg z uprawnieniami administratora, wyświetl menu *File*, wybierz pozycję *Kernel Debug*, kliknij kartę *Local*, a następnie przycisk *OK* (lub użyj programu *bcdedit.exe*). Na rysunku 1.6 pokazano przykładowy ekran danych wynikowych uzyskany w 64-bitowym systemie Windows. Niektóre polecenia debugera jądra, takie jak ustawiające punkty wstrzymania lub tworzące zrzut pamięci za pomocą polecenia `.dump`, nie zadziałają, gdy zostaną użyte w trybie lokalnego debugowania jądra. Zrzut może być jednak uzyskany przy użyciu narzędzia *LiveKd*, opisanego w dalszej części rozdziału.

```

Local kernel - WinDbg:10.0.10240.9 AMD64
File Edit View Debug Window Help
Command
Microsoft (R) Windows Debugger Version 10.0.10240.9 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Connected to Windows 10 10586 x64 target at (Thu Feb 11 17:41:56.379 2016 (UTC + 2:00)), ptr64 TRUE

***** Symbol Path validation summary *****
Response          Time (ms)         Location
Deferred          0                 srv*c:\symbols*http://msdl.microsoft.com/download/symbols
Symbol search path is: srv*c:\symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ntkrnlmp.exe -
Windows 10 Kernel Version 10586 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 10586.103.amd64fre.th2_release.160126-1819
Machine Name:
Kernel base = 0xfffff800`c1803000 PsLoadedModuleList = 0xfffff800`c1ae1cf0
Debug session time: Thu Feb 11 17:41:56.535 2016 (UTC + 2:00)
System Uptime: 0 days 6:30:31.302
No .natvis files found at C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\Visualizers.

lkd>
Ln 0, Col 0 | Sys 0:<None> | Proc 000:0 | Thrd 000:0 | ASM | OVR | CAPS | NUM

```

RYSUNEK 1.6. Lokalne debugowanie jądra

Po nawiązaniu połączenia w trybie debugowania jądra możesz zastosować jedno z wielu poleceń rozszerzających debugger, które są też nazywane poleceniami *bang*. Są to polecenia o nazwie zaczynającej się znakiem wykrzyknika (!). Polecenia umożliwiają wyświetlenie zawartości wewnętrznych struktur danych, takich jak wątki, procesy, pakiety żądań wejścia-wyjścia, oraz informacji dotyczących zarządzania pamięcią. W książce uwzględniono odpowiednie polecenia debuggera jądra i jego dane wyjściowe w miejscach, w których mają one zastosowanie odnośnie poszczególnych omawianych zagadnień. Znakomitym dodatkowym zasobem jest plik pomocy *Debugger.chm*, znajdujący się w folderze instalacyjnym debuggera WinDbg. W pliku tym udokumentowano wszystkie funkcje i rozszerzenia debuggera jądra. Ponadto polecenie *dt* (*display type*) może sformatować więcej niż 1000 struktur jądra, ponieważ pliki symboli jądra dla systemu Windows zawierają informacje o typach, których debugger może użyć do formatowania struktur.

EKSPERYMENT:

Wyświetlanie informacji o typach powiązanych ze strukturami jądra

Aby wyświetlić listę struktur jądra, których informacje o typach uwzględniono w symbolach jądra, w oknie debuggera jądra wpisz polecenie **dt nt!_***. Poniżej zaprezentowano część przykładowych danych wynikowych (*ntkrnlmp* to nazwa pliku wewnętrznego jądra 64-bitowego; więcej szczegółów podano w rozdziale 2.).

```

lkd> dt nt!_*
ntkrnlmp!_KSYSTEM_TIME
ntkrnlmp!_NT_PRODUCT_TYPE
ntkrnlmp!_ALTERNATIVE_ARCHITECTURE_TYPE
ntkrnlmp!_KUSER_SHARED_DATA
ntkrnlmp!_ULARGE_INTEGER
ntkrnlmp!_TP_POOL
ntkrnlmp!_TP_CLEANUP_GROUP

```

```

ntkrnlmp! _ACTIVATION_CONTEXT
ntkrnlmp! TP_CALLBACK_INSTANCE
ntkrnlmp! TP_CALLBACK_PRIORITY
ntkrnlmp! TP_CALLBACK_ENVIRON_V3
ntkrnlmp! _TEB

```

Możesz również zastosować polecenie `dt` do wyszukania konkretnych struktur, używając jego funkcji wyszukiwania za pomocą znaków wieloznacznych. Jeśli na przykład byłyby szukana nazwa struktury obiektu przerwania, należałoby wpisać polecenie `dt nt! *_interrupt*`:

```

!kd> dt nt! *_interrupt*
ntkrnlmp! _KINTERRUPT_MODE
ntkrnlmp! _KINTERRUPT_POLARITY
ntkrnlmp! _PEP ACPI_INTERRUPT_RESOURCE
ntkrnlmp! _KINTERRUPT
ntkrnlmp! _UNEXPECTED_INTERRUPT
ntkrnlmp! _INTERRUPT_CONNECTION_DATA
ntkrnlmp! _INTERRUPT_VECTOR_DATA
ntkrnlmp! _INTERRUPT_HT_INTR_INFO
ntkrnlmp! _INTERRUPT_REMAPPING_INFO

```

Możesz następnie użyć polecenia `dt` w celu sformatowania określonej struktury w następujący sposób (w wypadku struktur debugger nie rozróżnia wielkości liter):

```

!kd> dt nt! KINTERRUPT
+0x000 Type : Int2B
+0x002 Size : Int2B
+0x008 InterruptListEntry : _LIST_ENTRY
+0x018 ServiceRoutine : Ptr64 unsigned char
+0x020 MessageServiceRoutine : Ptr64 unsigned char
+0x028 MessageIndex : Uint4B
+0x030 ServiceContext : Ptr64 Void
+0x038 SpinLock : Uint8B
+0x040 TickCount : Uint4B
+0x048 ActualLock : Ptr64 Uint8B
+0x050 DispatchAddress : Ptr64 void
+0x058 Vector : Uint4B
+0x05c Irql : UChar
+0x05d SynchronizeIrql : UChar
+0x05e FloatingSave : UChar
+0x05f Connected : UChar
+0x060 Number : Uint4B
+0x064 ShareVector : UChar
+0x065 EmulateActiveBoth : UChar
+0x066 ActiveCount : Uint2B
+0x068 InternalState : Int4B
+0x06c Mode : _KINTERRUPT_MODE
+0x070 Polarity : _KINTERRUPT_POLARITY
+0x074 ServiceCount : Uint4B
+0x078 DispatchCount : Uint4B
+0x080 PassiveEvent : Ptr64 _KEVENT
+0x088 TrapFrame : Ptr64 _KTRAP_FRAME
+0x090 DisconnectData : Ptr64 Void
+0x098 ServiceThread : Ptr64 _KTHREAD
+0x0a0 ConnectionData : Ptr64 _INTERRUPT_CONNECTION_DATA
+0x0a8 IntTrackEntry : Ptr64 Void
+0x0b0 IsrDpcStats : _ISRDPSTATS
+0x0f0 RedirectObject : Ptr64 Void
+0x0f8 Padding : [8] UChar

```

Zauważ, że domyślnie polecenie `dt` nie pokazuje podstruktur (struktury w obrębie innych struktur). Aby je wyświetlić, użyj opcji `-r` lub `-b`. Zastosowanie jednej z tych opcji na przykład do wyświetlenia obiektu przerwania jądra spowoduje zaprezentowanie formatu struktury `_LIST_ENTRY` przechowywanej w polu `InterruptListEntry` (w dokumentacji opisano dokładne różnice między opcjami `-r` i `-b`).

```
lkd> dt nt! KINTERRUPT -r
+0x000 Type           : Int2B
+0x002 Size           : Int2B
+0x008 InterruptListEntry : _LIST_ENTRY
+0x000 Flink          : Ptr64 _LIST_ENTRY
+0x000 Flink          : Ptr64 _LIST_ENTRY
+0x008 Blink          : Ptr64 _LIST_ENTRY
+0x008 Blink          : Ptr64 _LIST_ENTRY
+0x000 Flink          : Ptr64 _LIST_ENTRY
+0x008 Blink          : Ptr64 _LIST_ENTRY
+0x018 ServiceRoutine : Ptr64 unsigned char
```

Polecenie `dt` pozwala nawet określić poziom rekurencji struktur przez dodanie liczby do opcji `-r`. W następującym przykładzie użyto jednego poziomu rekurencji:

```
lkd> dt nt!_KINTERRUPT -r1
```

W pliku pomocy zestawu Debugging Tools for Windows wyjaśniono, jak konfigurować i stosować debuggery jądra. W dokumentacji zestawu WDK zamieszczono dodatkowe szczegóły dotyczące korzystania z debuggerów jądra, które przeznaczone są głównie dla osób tworzących sterowniki urządzeń.

Narzędzie LiveKd

LiveKd to darmowe narzędzie dostępne w witrynie Sysinternals, które umożliwia użycie standardowych debuggerów jądra firmy Microsoft, które właśnie opisano, do sprawdzania działającego systemu bez konieczności przeprowadzania jego rozruchu w trybie debugowania. Takie rozwiązanie może być przydatne, gdy niezbędne okaże się rozwiązywanie problemów na poziomie jądra w wypadku komputera, którego nie uruchomiono w trybie debugowania. Określone problemy mogą być trudne do właściwego odtworzenia, dlatego rozruch z włączoną opcją *debugowania* może nie umożliwić ujawnienia błędu w prosty sposób.

Narzędzie LiveKd jest uruchamiane tak jak w wypadku debuggera WinDbg lub kd. Narzędzie to przekazuje wybranemu debuggerowi wszystkie podane opcje wiersza poleceń. Domyślnie narzędzie uruchamia debugger jądra trybu wiersza poleceń (kd). Aby załadować debugger WinDbg, użyj opcji `-w`. W celu wyświetlenia plików pomocy dla opcji narzędzia LiveKd zastosuj opcję `-?`.

Narzędzie LiveKd prezentuje debuggerowi plik symulowanego zrzutu pamięci po awarii, dlatego możesz wykonać dowolne operacje, które są obsługiwane w przypadku zrzutu pamięci po awarii. Ponieważ narzędzie to na potrzeby symulowanego zrzutu korzysta z pamięci fizycznej, debugger jądra może mieć do czynienia z sytuacjami, w których struktury danych są w trakcie wprowadzania zmian przez system, a tym samym są niespójne. Każdorazowo po wywołaniu debugger zaczyna działać z wykorzystaniem nowego widoku stanu systemu. Aby odświeżyć migawkę, wprowadź polecenie `q` w celu zakończenia pracy debuggera. Narzędzie LiveKd zapyta, czy zamierzasz ponownie uruchomić debugger. Jeśli debugger zapętlili się podczas wyświetlania danych wynikowych, użyj kombinacji klawiszy `Ctrl+C`, aby przerwać tę operację i zakończyć działanie debuggera. W przypadku jego zawieszenia użyj kombinacji klawiszy `Ctrl+Break`, która spowoduje zakończenie procesu debuggera. Narzędzie LiveKd zapyta następnie, czy debugger ma zostać ponownie uruchomiony.

Windows Software Development Kit

Zestaw Windows Software Development Kit (SDK) stanowi część programu subskrypcji MSDN. Możesz go pobrać bezpłatnie pod adresem <https://developer.microsoft.com/en-US/windows/downloads/windows-10-sdk>. W trakcie instalacji środowisko Visual Studio również zapewnia opcję instalacji zestawu SDK. Wersje zawarte w zestawie Windows SDK zawsze są zgodne z najnowszą wersją systemu operacyjnego Windows, natomiast wersja dołączona do środowiska Visual Studio może być starszą wersją, która była aktualna w chwili jej udostępnienia. Oprócz zestawu Debugging Tools for Windows, zestaw SDK zawiera pliki nagłówkowe języka C oraz biblioteki niezbędne do kompilowania i konsolidowania aplikacji dla systemu Windows. Z perspektywy wewnętrznych mechanizmów systemu Windows godne zainteresowania elementy zestawu Windows SDK obejmują pliki nagłówkowe interfejsu API systemu Windows (na przykład zawarte w folderze `C:\Program Files (x86)\Windows Kits\10\Include`) oraz narzędzia SDK (poszukaj folderu `Bin`). Godną uwagi jest też dokumentacja. Jest ona dostępna w trybie online; można ją też pobrać w celu korzystania w trybie offline. Kilka spośród tych narzędzi jest też dołączonych w postaci przykładowego kodu źródłowego zarówno w zestawie Windows SDK, jak i bibliotece MSDN Library.

Windows Driver Kit

Zestaw Windows Driver Kit (WDK) również jest dostępny w ramach programu subskrypcji MSDN. Tak jak zestaw Windows SDK, zestaw WDK może zostać bezpłatnie pobrany. Jego dokumentację dołączono do biblioteki MSDN Library.

Choć zestaw WDK przeznaczony jest dla projektantów sterowników urządzeń, stanowi on bogate źródło informacji o wewnętrznych mechanizmach systemu Windows. Na przykład w rozdziale 6. opisano architekturę systemu wejścia-wyjścia, model sterowników oraz podstawowe struktury danych sterowników urządzeń, ale nie omówiono w nim szczegółowo poszczególnych funkcji obsługi jądra. Dokumentacja zestawu WDK zawiera obszerny opis, zarówno w postaci kursu, jak i materiału referencyjnego, wszystkich funkcji obsługi jądra i mechanizmów systemu Windows używanych przez sterowniki urządzeń.

Oprócz dokumentacji, zestaw WDK uwzględnia pliki nagłówkowe (w szczególności pliki `ntddk.h`, `ntifs.h` i `wdm.h`), które definiują kluczowe wewnętrzne struktury danych i stałe, a także interfejsy do wielu wewnętrznych programów systemowych. Pliki te przydają się podczas eksplorowania wewnętrznych struktur danych systemu Windows za pomocą debuggera jądra, ponieważ choć ogólny układ i zawartość tych struktur zaprezentowano w książce, nie uwzględniono szczegółowych opisów na poziomie pól (na przykład dotyczących wielkości i typów danych). Kilka tych struktur danych, takich jak nagłówki rozdzielacza obiektów, bloki oczekiwania, zdarzenia, muteksy, semaforey itp., opisano jednak szczegółowo w zestawie WDK.

Aby zaznajomić się z systemem operacji wejścia-wyjścia i modelem sterowników w zakresie szerszym niż zaprezentowany w książce, przeczytaj dokumentację zestawu WDK, a zwłaszcza podręczniki *Kernel-Mode Driver Architecture Design Guide* i *Kernel-Mode Driver Reference*. Za wartościową możesz też uznać książkę *Programming the Microsoft Windows Driver Model* (wydanie drugie; Microsoft Press, 2002 r.) autorstwa Waltera Oneya oraz książkę *Developing Drivers with the Windows Driver Foundation* napisaną przez Penny Orwick i Guya Smitha (Microsoft Press, 2007 r.).

Narzędzia z witryny Sysinternals

W wielu eksperymentach zamieszczonych w książce wykorzystano darmowe narzędzia, które możesz pobrać z witryny Sysinternals. Większość tych narzędzi napisał Mark Russinovich, współautor książki. Do najpopularniejszych narzędzi należą Process Explorer i Process Monitor. Zauważ, że wiele z tych narzędzi uwzględnia instalację i uruchamianie sterowników urządzeń trybu jądra, dlatego wymagają uprawnień administratora lub zwiększonych uprawnień. Niemniej jednak w wypadku standardowego konta użytkownika lub mającego mniejsze uprawnienia część narzędzi może działać z ograniczoną funkcjonalnością.

Ponieważ narzędzia z witryny Sysinternals są często aktualizowane, upewnij się, że dysponujesz najnowszą wersją. Aby być powiadamianym o aktualizacjach narzędzi, możesz śledzić blog witryny Sysinternals, który oferuje kanał RSS. W celu zaznajomienia się z opisem wszystkich narzędzi, sposobem korzystania z nich oraz analizami przypadków rozwiązywania problemów zajrzyj do książki *Windows Sysinternals Administrator's Reference* autorstwa Marka Russinovicha i Aarona Margosisa (Microsoft Press, 2011 r.). Do zadawania pytań i prowadzenia dyskusji dotyczących narzędzi użyj forów witryny Sysinternals.

Podsumowanie

W rozdziale dokonano wprowadzenia do kluczowych zagadnień technicznych i terminów związanych z systemem Windows, które będą używane w książce. Zaprezentowano też w skrócie wiele przydatnych narzędzi służących do poznawania wewnętrznych mechanizmów systemu Windows. Jesteś już gotowy do rozpoczęcia eksploracji wnętrza systemu. Na początek przyjrzymy się ogólnie architekturze systemu i jej kluczowym komponentom.

Skorowidz

A

- ACE, Access Control Entry, 713
 - obiekt nadzoru systemu, 714
 - wpisy warunkowe, 730
- ACL, Access Control List, 356, 555, 713, 717
- ACPI, Advanced Configuration and Power Interface, 103, 648
- Active Directory, 667
- adapter
 - czujnika, 784
 - magazynu, 785
 - silnika, 784
- adres
 - ładowania biblioteki, 406
 - PTE, 481
- AIT, Application Impact Telemetry, 204
- algorytm
 - FIFO, 456
 - haszowania strony, 503
 - LRU, 456
 - żądania stronicowania, 440
- analiza
 - importu, 199
 - tabeli importu, 184
 - wirtualnej przestrzeni adresowej, 403
 - wydajności operacji wejścia-wyjścia, 605
- ANSI, 54
- anulowanie operacji wejścia-wyjścia, 589
- APC, Asynchronous Procedure Call, 99, 425
- API, Application Programming Interface, 22, 108
 - lokalne, 346
 - mapowania plików, 346
 - Sets, 204
 - sterty, 346
 - wirtualne, 346
- APIC, Advanced Programmable Interrupt Controller, 103
- aplikacje
 - desktopowe, 750
 - konsolowe, 85, 90
 - multimedialne, 282
 - POSIX, 91
 - UWP, 748
- AppLocker, 827
- architektura
 - kontenerów, 215
 - systemu, 67, 69
 - centrum wykonawcze, 96
 - jądro, 99
 - komponenty, 84
 - mechanizmy bezpieczeństwa, 81
 - podsystemy, 84, 91
 - procesy systemowe, 112
 - przenośność, 72
 - skalowalność, 75
 - sterowniki urządzeń, 105
 - warstwa abstrakcji sprzętowej, 102
 - wersja Checked build, 79
 - wieloprotocessorowość symetryczna, 73
 - VBS, 82
 - Windows Runtime, 24
- argumenty funkcji CreateProcess*, 127
- asercje bezpieczeństwa, 821
- ASLR, Address Space Layout Randomization, 194, 407
- asocjacyjny bufor translacji, 415
- asynchroniczne wywoływanie procedur, 425
- atak typu MitM, 673

atrybuty
 obiektów, 50
 KMDF, 641
 plików, 556
 procesów, 158, 159, 160
 programów Trustlet, 150
 zabezpieczeń kontenera aplikacji, 759
 automatyczne
 przesyłanie rzutów awaryjnych, 834
 zwiększanie priorytetu, 286
 awaria, 823, 824, 825
 awaryjne wyłączenie maszyny, 834
 AWE, Address Windowing Extensions, 42, 361

B

baza danych
 dyspozytora, 258
 menedżera SAM, 666
 numerów stron pamięci, 465
 PFN, 426, 467, 468
 procesu Lsass, 666
 załadowanych modułów, 194
 zgodności aplikacji, 184
 bezpieczeństwo, 663–841
 ACL, 713
 Active Directory, 667
 AppLocker, 827
 asercje, 821
 biometria, 784
 deskryptory zabezpieczeń, 711
 dostawcy poświadczeń, 667
 globalne zasady inspekcji, 745
 identyfikacja aplikacji, 826
 identyfikatory zabezpieczeń, 684
 inicjacja procesu Winlogon, 776
 inspekcje dostępu do obiektów, 742
 inspekcje zabezpieczeń, 740
 interfejs AuthZ, 728
 Kerberos, 703
 klasy, 663
 komponenty, 668
 kontenery aplikacji, 748, 751
 kontrola dostępu, 711
 kontrola konta użytkownika, 787
 kryteria oceny zaufanych systemów, 663
 LAN Manager 2, 703
 logowanie, 774
 mechanizm CFG, 808, 818
 ochrona obiektów, 678
 ochrona poświadczeń, 670
 ochrona przed poprawkami jądra, 834
 ochrona urządzeń, 676
 oparte na wirtualizacji, 669
 osłabianie exploitów, 801
 pakiety uwierzytelniania, 667
 PatchGuard, 835
 personifikacja, 702
 pochodzenie pakietu, 752
 poziomy integralności, 688
 prawa konta, 732
 przywileje, 732
 sieciowe, 703
 sterownik zabezpieczenia urządzeń, 667
 stert, 379
 superprzywileje, 739
 system zabezpieczeń, 666
 środowiska AppContainer, 757
 tokeny, 692
 Windows Hello, 786
 wirtualizacja, 788
 wspólne kryteria, 665
 zasady ograniczeń oprogramowania, 832
 bezpieczna komunikacja, 673
 bezpieczne
 procesy, 154
 sekcje, 152
 urządzenia, 152
 bezpieczny magazyn, 153
 biblioteka, 26
 Advapi32.dll, 71, 88
 Basesrv.dll, 87
 Bootvid.dll, 104
 Csrsv.dll, 87
 FSRTL, 98
 Gdi32.dll, 71, 88
 Halacpi.dll, 103
 Hal.dll, 71, 102, 340
 Iumdll.dll, 82
 Kdcom.dll, 104
 Kernel32.dll, 71, 88
 Kernelbase.dll, 82
 loggingplatform.dll, 194
 lumbase.dll, 82
 MSVCR120.dll, 194
 Netlogon.dll, 667
 ntdll.dll, 71, 93, 176, 215, 759
 ole32.dll, 194

biblioteka

- Pshed.dll, 104
- Winsrv.dll, 87
- Sxssrv.dll, 87
- User32.dll, 71, 88
- rpcrt4.dll, 153
- wsock32.dll, 194

biblioteki

- debuggera jądra, 98
- DLL, 26
 - ładowanie, 193
 - przekierowywanie nazw, 191
 - rozwiązywanie nazw, 189
- dostawców poświadczeń, 123
- hipernadzorczy, 98
- podsystemu, 71, 84, 88
 - wywoływanie funkcji, 86
 - wykonawcze systemu plików, 98

bilet, 671

- TGT, 672
- użytkownika, 675

biometria, 784

bit przejścia, 423

bitmapa

- CFG, 813, 815
- ochrony przepływu sterowania, 814
- PTE, 414
- zapisu sprzętowego, 414

blok

- kontrolny procesora, 100
- PRCB, 330

blokada

- krytyczna, 271
- UEFI, 674
- wirująca, 584

blokowanie pamięci, 350

błędy

- strony, 420
- strony klastrowanej, 426
- strony kolidującej, 425
- żądania strony wyzerowanej, 469

brokery, 772

buforowanie

- operacji wejścia-wyjścia, 580
- plików, 562
- stron enklawy, 512
- translacji, 339, 415

C

CCI, Custom Code Integrity, 676

cele projektowe, 67

centrum

- dystrybucji kluczy, 672
- wykonawcze, 71, 96

certyfikat

- podsystemu Smss, 141
- WMC, 137

CFG, Control Flow Guard, 809

chronione procesy, 137

CLR, Common Language Runtime, 25

COM, Component Object Model, 23

cykle zegara, 263

częstotliwość interwałów zegara, 261

czuwanie, 519

D

DAC, Dynamic Access Control, 728

DACL, Discretionary Access Control List, 679, 711–714, 722, 724

DAM, Desktop Activity Moderator, 207

DDE, Dynamic Data Exchange, 703

DDI, Device Driver Interface, 108

debugowanie, 149

- procesu, 592

- trybu jądra, 58, 61, 233, 240

- trybu użytkownika, 59, 238, 239

Debugging Tools for Windows, 59

DEP, Data Execution Prevention, 43, 356, 359

deskryptor

- adresu wirtualnego, 348, 422, 440
- rotacja, 443

- zabezpieczeń, 711

- przeglądanie zawartości, 715

- znaczniki, 711

DFSS, Dynamic Fair Share Scheduling, 207, 317, 323

diagnostyczna infrastruktura systemu, 98

diagram stanów stron, 469

Direct Switch, 287

DMA, Direct Memory Access, 83

dobrowolne przełączanie, 288

dodawanie procesorów, 330

dojścia, 50

domeny, 667

dostawcy poświadczeń, 123, 667

- dostęp
 - bezpośredni do pamięci, 83
 - do buforu, 578
 - do obiektu, 720, 721, 742
 - do zasobów procesora, 278
 - do zasobów zdalnych, 672
 - sekwencyjny do pliku, 522
 - DPC, Deferred Procedure Call, 99, 440, 535
 - Driver Verifier, 606
 - Low Resources Simulation, 612
 - opcje weryfikacji, 608, 609
 - Special Pool, 609
 - sprawdzanie poziomu IRQL, 611
 - Systematic Low Resources Simulation, 613
 - śledzenie puli, 611
 - DRM, Digital Rights Management, 44
 - drzewo
 - procesów, 31, 113
 - urządzeń, 616
 - dublowanie procesu, 525
 - dynamiczna
 - kontrola dostępu, 728
 - wymiana danych, 703
 - dynamiczne ładowanie sterowników, 529
 - dziedziczenie wpisów ACE, 714
- E**
- EKU, Enhanced Key Usage, 140
 - enklawy pamięci, 510
 - inicjalizacja, 515
 - konstruowanie, 512
 - przygotowywanie, 512
 - wczytywanie danych, 514
 - EPC, Enclave Page Cache, 512
 - etapy tworzenia procesu, 156–176
 - ETW, Event Tracing for Windows, 81, 312
 - exploity, 801
- F**
- fabryki procesów roboczych, 332
 - FCL, Framework Class Library, 25
 - FIFO, Filter Device Object, 456, 600, 619
 - filtrowanie
 - menedżera obiektów, 838
 - systemu plików, 838
 - filtrujące sterowniki systemu plików, 106
 - filtry LightWeight, 838
 - FLS, Fiber Local Storage, 184
 - FTH, Fault-Tolerant Heap, 385
 - fundament sterownika, 108
 - funkcja, 26
 - __fastfail, 822
 - AccessCheck, 683, 722
 - AccessCheckByType, 722
 - AllocateUserPhysicalPagesNuma, 443
 - AppLocker, 827
 - AssignProcessToJobObject, 209
 - ChangeWindowMessageFilterEx, 721
 - CreateEnclave, 511
 - CreateFile, 193, 704
 - CreateFileMapping, 353, 562
 - CreateFileMappingNuma, 443
 - CreateProcess, 125, 155, 164, 186, 832
 - CreateProcessAsUser, 125
 - CreateProcessInternalW, 157, 164
 - CreateProcessWithLogonW, 125
 - CreateProcessWithTokenW, 125
 - CreateRemoteThread, 223
 - CreateRemoteThreadEx, 237
 - CreateRestrictedToken, 705
 - CreateThread, 223, 238
 - CsrCreateProcess, 175
 - DAM, 207
 - DbgPrintEx, 80
 - DdeImpersonateClient, 703
 - DEP, 43
 - DeviceControl, 96
 - DFSS, 207
 - Direct Switch, 287
 - ETW, 204
 - ExAllocatePool, 363
 - ExAllocatePoolWithTag, 111
 - ExInitializeNPagedLookasideList, 369
 - ExInitializePagedLookasideList, 369
 - ExitProcess, 183
 - FlushViewOfFile, 348, 444
 - GetEffectiveRightsFromAcl, 722
 - GetFileSecurity, 682
 - GetQueuedCompletionStatus, 595
 - GetSystemInfo, 351
 - GetSystemTimeAdjustment, 261
 - HeapLock, 373
 - HeapSetInformation, 374
 - HeapUnlock, 373
 - HyperGuard, 839, 841
 - ImpersonateNamedPipeClient, 703

funkcja

ImpersonateSelf, 703
 InitializeEnclave, 511
 IoCompleteRequest, 570
 IoCreateSystemThread, 114
 IoInvalidDeviceRequest, 552, 566
 IoSetCompletionRoutine, 570
 IoSkipCurrentIrpStackLocation, 570
 IoStartNextPacket, 578
 IoStartPacket, 577
 IsEnclaveTypeSupported, 511
 ISR, 577
 KeAcquireInterruptSpinLock, 585
 KeBalanceSetManager, 461
 KeInitializeThread, 111
 KePerformGroupConfiguration, 304
 KeReleaseInterruptSpinLock, 585
 KeRemoveQueueEx, 597
 KiAdjustLookasideDepth, 369
 KiDirectSwitchThread, 287
 KiSearchForNewThread, 317
 KiSearchForNewThreadOnProcessor, 317
 KPP, 835–838
 LdrInitializeThunk, 178
 LdrpApplyFileNameRedirection, 205
 LdrpInitializeProcess, 178
 LogonUser, 703
 MapViewOfFile, 353
 MapViewOfFileExNuma, 443
 MiAddPagesToEnclave, 514
 MiCreateEnclave, 513
 MiInitializeCfg, 815
 MiInitializeEnclavePfn, 513
 MiInitializeRelocations, 405
 MiReclaimSystemVa, 397
 MmLockPagableCodeSection, 351
 MmLockPagableDataSection, 351
 MmLockPagableSectionByHandle, 351
 MmProbeAndLockPages, 351
 NT, 670
 NtCreateLowBoxToken, 770
 NtCreateThreadEx, 236
 NtCreateUserProcess, 128, 162
 NtDelayExecutionThread, 316
 NtLoadEnclaveData, 515
 NtManagePartition, 500
 NtSetInformationProcess, 477
 NtSetInformationThread, 477
 ObCheckObjectAccess, 681, 682
 ObpCreateHandle, 681
 OpenFileMapping, 353
 Pages, 351
 PoFxRegisterComponentPerfStates, 659
 PoFxRegisterDevice, 658
 PoRegisterDeviceForIdleDetection, 657
 PoRequestPowerIrp, 654
 PostQueuedCompletionStatus, 597
 PsCreateSystemThread, 114
 PspAllocateProcess, 178
 ReadFileEx, 578
 ReadProcessMemory, 347, 354, 386
 Ready Boost, 523
 Ready Drive, 524
 ReadyBoot, 453
 RpcImpersonateClient, 703
 RtlAssert, 80
 RtlCloneUserProcess, 526
 RtlCreateProcessReflection, 525
 RtlpCreateUserProcess, 526
 RtlUserThreadStart, 238
 SeAccessCheck, 682, 683
 SeDefaultObjectMethod, 681
 SetProcessInformation, 477
 SetFileSecurity, 682
 SetNamedSecurityInfo, 725
 SetProcessWorkingSetSize, 457, 458
 SetThreadInformation, 477
 SetSecurityInfo, 725
 StartService, 120
 UpdateProcThreadAttributes, 127
 VerifierAllocatePool, 608
 VfLoadDriver, 608
 VirtualAlloc, 347, 433, 441, 471, 514
 VirtualAllocExNuma, 443
 VirtualFree, 348
 VirtualFreeEx, 348
 VirtualLock, 350
 VirtualProtect, 354
 VirtualProtectEx, 354
 VirtualQuery, 354
 VirtualQueryEx, 354
 Windows Hello, 786
 WriteFile, 682
 WriteFileEx, 578
 WriteProcessMemory, 354
 ZwMapViewOfSection, 353
 ZwOpenSection, 353
 ZwUnmapViewOfSection, 353

funkcje
 bezpieczeństwa, 380
 debugowania sterzy, 380
 eksportowane, 96
 interfejsu API, 26
 obsługi jądra, 26
 pomocnicze, 71
 sterowników urządzeń, 96, 546
 tworzące procesy, 126
 wewnętrzne, 96
 wspomagające DirectX, 88
 wywołwalne z trybu użytkownika, 96
 zabezpieczeń, 683
 zaufanej ścieżki, 664

G

GDI, Graphics Device Interface, 88
 GDT, Global Descriptor Table, 100, 330
 globalna tabela deskryptorów, 100
 globalne zasady inspekcji, 745
 głębokie zamrożenie, 296
 główna tabela plików, 453
 graficzny interfejs
 edytorów zabezpieczeń, 726
 użytkownika, 71, 85, 276
 granice izolacji silosów, 216
 grupa
 asynchronicznego LPC, 98
 funkcji bibliotek wykonawczych, 98
 menedżera obiektów, 97
 planowania, 322
 procedur wspomagających centrum
 wykonawcze, 98
 gry, 282
 GUI, 71, 85, 276
 GUID, 713

H

HAL, Hardware Abstraction Layer, 71, 102, 531
 hasło, 670
 hibernacja, 519
 hierarchia
 obiektów środowiska KMDF, 640
 zadań, 210
 hipernadzorca, 47, 71, 669
 hiperprzestrzeń, 387

host PowerShell, 833
 HVCI, HyperVisor Code Integrity, 676
 HyperGuard, 839

I

IBAC, Identity-Based Access Control, 729
 idealny
 procesor, 310
 węzeł, 311
 identyfikacja aplikacji, 826
 identyfikator
 aplikacji, 752
 GUID, 201, 713
 hosta pakietu, 752
 kontenera, 623
 LUID, 696, 780
 procesu nadrzędnego, 31
 programu Trustlet, 151
 RID, 684
 scenariusza, 150
 SID, 685, 724
 urządzenia, 150, 620
 zabezpieczeń, 684
 identyfikowanie bezpiecznych procesów, 154
 IDT, Interrupt Dispatch Table, 100
 IHV, Independent Hardware Vendor, 107
 implementacja sekwencji SAS, 777
 import, 199
 informacje
 na temat pamięci systemowej, 341
 na temat pliku wymiany, 432
 na temat procesu UWP, 753
 na temat wirtualnego pliku stronicowania,
 432
 o ochronie przepływu sterowania, 810
 o podsystemie, 91
 o procesach, 28
 o procesorach logicznych, 301
 o stercie, 376
 o sterownikach KMDF, 636
 o systemie, 544
 o systemie NUMA, 302
 o systemowych wpisach PTE, 393
 o wątkach, 229
 o wątku chronionego procesu, 242
 o węźle urządzeń, 624
 infrastruktura diagnostyczna Windows, 525

inicjalizacja
 enklawy pamięci, 515
 procesu, 176
 po imporcie, 200
 Winlogon, 776

inspekcje
 dostępu do obiektów, 742, 743
 zabezpieczeń, 740

instalacja sterownika, 633
 ogólnego, 631
 Plug and Play, 627

instancja programu Trustlet, 151

integralność przepływu sterowania, 808

interaktywny menedżer logowania, 667

interfejs
 ACPI, 103
 API, 22, 154
 MF, 137
 SetPriorityClass, 245
 usługi biometrycznej, 784
 AuthZ, 728
 logowania, 667
 programistyczny aplikacji, 108, 511
 sterownika urządzenia, 108
 sterownika urządzenia biometrycznego, 784
 urządzeń graficznych, 88

interfejsy nieudokumentowane, 110

IOMMU, I/O Memory Management Unit, 83

IPC, Inter-Partition Communication, 71, 93

IPI, Inter-Processor Interrupt, 426

IRQL, Interrupt Request Level, 535

IUM, Isolated User Mode, 81

izolacja
 silosów, 214
 uprawnień interfejsu użytkownika, 721

izolowany tryb użytkownika, 81

J

jądro, 71, 99
 zastępcze, 82

jądrowy
 blok kontrolny procesora, 100
 obszar kontrolny procesora, 100

jednostka zarządzająca pamięcią, 413
 wejścia-wyjścia, 83

język C, 73

K

kategorie planowania, 283

KDC, Key Distribution Center, 672

Kerberos, 675, 703, 779

klasa Win32_OperatingSystem, 80

klasy bezpieczeństwa, 663

klient FTH, 385

klucz
 NTOWF, 672
 sterowników rejestru, 631
 tożsamości, 153
 urządzenia, 621
 zrzutu po awarii, 149

KMCS, Kernel-Mode Code-Signing, 44

KMDF, Kernel-Mode Driver Framework, 108, 634

kod
 awarii, 823–825
 asercji bezpieczeństwa, 822
 systemowy, 387

koligacja, 307

kompatybilność, 68

kompilacja testowa, 79

kompilator, 822

komponenty
 dynamicznej kontroli dostępu, 728
 hosta skryptów, 833
 jądra VReg, 215
 kluczowe systemu, 84
 logowania, 775
 systemu operacji wejścia-wyjścia, 529
 VBS, 670

kompresja pamięci, 491, 497

konfiguracja
 funkcji AppLocker, 829
 kwantu czasu, 264, 267
 mechanizmu DFSS, 324
 obiektu EPROCESS, 166
 obiektu procesu wykonawczego, 171
 obszaru adresów, 169
 struktury PEB, 170
 zaawansowanych zasad inspekcji, 747
 zasad inspekcji, 741
 zasad ograniczeń oprogramowania, 832

konstruowanie enklawy, 512

konteksty silosów, 216, 218

- kontener, 213, 713
 - aplikacji, 748, 751, 763, 767
 - uchwyty, 769
 - typu sandbox, 498
 - kontrakt
 - Clfs, 105
 - Ium, 105
 - Kcminitcfg, 105
 - Ksecurity, 105
 - Ksigningpolicy, 105
 - Ksr, 105
 - Tm, 105
 - Ucode, 105
 - Werkernel, 105
 - kontrola
 - dostępu, 711
 - dynamiczna, 728
 - obowiązkowa, 52
 - oparta na tożsamości, 729
 - uprzywilejowana, 52
 - uznaniowa, 52
 - dysku, 389
 - konta użytkownika, 787
 - ustawienia, 800
 - zasilania urzędnika, 657
 - konwersja wpisu PTE, 505
 - kopiowanie przy zapisie, 359, 361
 - KPCR, Kernel Procesor Control Region, 100
 - KPP, Kernel Patch Protection, 669, 835
 - KPRCB, Kernel Procesor Control Block, 100
 - kryteria oceny
 - bezpieczeństwa, 665
 - zaufanych systemów, 663
 - KSE, Kernel Shim Engine, 98
 - kwant, 260
 - cykle zegara, 263
 - konfiguracja, 264, 267
 - kontrolowanie, 263
 - upłynięcie, 289
 - wartość rejestru, 266
 - zmienny, 265
- L**
- LAN Manager 2, 703
 - lekki proces chroniony, 115
 - LFH, Low-Fragmentation Heap, 372, 203
 - licznik
 - pamięci zadeklarowanej, 436
 - poziomu użycia plików stronicowania, 436
 - wydajności, 45, 341
 - LIFO, 595
 - limity
 - deklaracji, 350, 432
 - pamięci, 489
 - wykorzystania procesora, 327
 - zadań, 207
 - lista
 - ACL, 356, 555, 713, 717
 - DACL, 717
 - listy
 - asocjacyjne, 369
 - deskryptorów pamięci, 409
 - kontroli dostępu, 356, 555, 713, 717
 - systemowe 711
 - uznaniowe, 711
 - stron
 - oczekujących, 471
 - wolnych, 470
 - wyzerowanych, 469
 - zmodyfikowanych, 471
 - załadowanych sterowników, 544
 - zestawów roboczych, 460
 - logowanie, 774
 - etapy, 777
 - komponenty, 775
 - losowość, 834
 - LRU, 456
 - LSASS, Local Security Authority Subsystem Service, 666
 - LXSS Manager, 92
- Ł**
- ładowanie
 - bibliotek DLL, 184, 193
 - obrazu, 184
 - ogólnego sterownika, 631
 - sterowników, 529, 631
 - sterowników Plug and Play, 620
 - ładunek deklaracji, 350, 432, 435

M

- mapowanie adresów, 40
 - wirtualnych, 410
- maska koligacji, 75, 307
 - rozszerzona, 309
 - systemowa, 310
- maski dostępu, 683, 723
- MDL, Memory Descriptor List, 409
- mechanizm
 - API Sets, 204
 - AppLocker, 667
 - ASLR, 407
 - automatycznego podwyższania uprawnień, 799
 - AWE, 42, 362
 - bezpiecznego logowania, 664
 - CFG, 809, 817
 - konstruowanie bitmapy, 815
 - debugujący trybu użytkownika, 98
 - DFSS, 325
 - Driver Verifier, 606
 - FTH, 386
 - HyperGuard, 839
 - KMCS, 678
 - LFH, 203
 - pageheap, 381, 382
 - PatchGuard, 839
 - SLAT, 83
 - SuperFetch, 515
 - VBS, 669
 - VTL, 81
- mechanizmy
 - kontrolowania dostępu, 664
 - ochrony, 839
 - osłabiania exploitów, 809
 - personifikacji, 680
 - potoków komunikacji międzyprocesowej, 93
 - systemu, 55
 - wirtualizacji
 - plików, 791
 - UAC, 692
- menedżer
 - cyklu życia procesu, 429
 - erraty, 98
 - konfiguracji, 96
 - kontroli usług, 112, 119
 - logowania, 667
 - magazynów, 495
 - mechanizmu Driver Verifier, 607
 - obiektów, 51, 769
 - okien pulpitu, 88
 - operacji wejścia-wyjścia, 530, 531
 - pamięci, 97, 337
 - podręcznej, 97
 - przepisywanie stron pamięci, 479
 - strategia rozmieszczania, 456
 - stronicowanie na żądanie, 452
 - synchronizacja wewnętrzna, 344
 - usługi, 345
 - zdarzenia powiadamiające, 464
 - procesów, 96
 - SCM, 544
 - sesji, 112, 115, 215, 389
 - sterty, 370
 - technologii PnP, 531, 614
 - urządzeń, 624
 - urządzeń Plug-and-Play, 97
 - wejścia-wyjścia, 97
 - zabezpieczeń kont, 666
 - zadań, 28, 113, 249
 - karta Procesy, 28
 - karta Szczegóły, 29
 - kluczowe kolumny, 29
 - wykorzystanie pamięci, 342
 - zasilania, 97, 531, 648, 652
 - zbioru zrównoważonego, 114
 - zestawu roboczego, 457
 - zestawu równowagi, 338, 461
- MFT, Master File Table, 453
- minimalna lista TCB, 142
- MLUI, Multiple Language User Interface, 184
- MMU, Memory Management Unit, 413
- model
 - COM, 23
 - obiektów KMDF, 638
 - Piko, 91
 - sterowników, 107
 - systemu operacyjnego, 68
 - WDM, 107
 - zabezpieczenia sieciowego, 703
- moduł zapisu stron
 - zmapowanych, 338
 - zmodyfikowanych, 338
- modyfikowanie koligacji procesu, 308
- monitor
 - bezpieczeństwa odwołań, 96, 666
 - silosów, 218

SRM, 217, 669, 682, 692
 wydajności, 56, 211
 zasobów, 56
 monitorowanie
 zabezpieczeń, 664
 wykorzystania puli, 365
 możliwości, capabilities, 749
 kontenera aplikacji, 763, 765
 muteks, 584

N

nadrzędny deskryptor zabezpieczeń, 149
 narzędzia Sysinternals, 65
 narzędzie
 Access Check, 56
 AIT, 204
 cpustres.exe, 312
 Dependency Walker, 56
 Global Flags, 56, 381
 Handle Viewer, 56
 Kernel debuggers, 56
 LiveKd, 63
 Menedżer zadań, 28, 56
 Monitor wydajności, 56, 249
 Object Viewer, 56
 Pool Monitor, 56
 Poolmon, 366
 Process Explorer, 34, 56, 109, 142, 242,
 544, 686
 Process Monitor, 56, 455
 PsGetSid, 686
 RAMMap, 343
 Startup Programs Viewer, 56
 Task List, 56
 TestLimit, 348
 Tlist.exe, 31
 Trustlet, 148
 VMMap, 343
 WinDbg, 761
 Windows Performance Analyzer, 312
 Windows Performance Recorder, 312
 WinObj, 550
 natywne usługi systemowe, 26
 niezawodność, 68
 NTFS, 92, 466, 681
 NUMA, Non-Uniform Memory Access, 301, 443
 numer SVN, 149

O

obiekt, 50
 EPROCESS, 166
 EKV, 140
 FiDO, 619
 IoCompletion, 594, 596
 KMDF, 638
 obiekty
 jądra, 50, 99
 kontrolne, 99
 mapowania plików, 39
 metody dostępu, 720
 nadzoru systemu, 714
 odwzorowania pliku, 338, 444
 plików, 555
 atrybuty, 556
 rozszerzenia, 557
 potomne, 713
 reguły obowiązkowości, 691
 sekcji, 338, 352, 444
 atrybuty, 445
 sterowników, 548
 urzędzeń, 548
 zadania, 214
 obliczanie
 kwantu czasu, 262
 rozmiaru pliku stronicowania, 429
 obowiązkowa kontrola dostępu, 52
 obrazy
 natywne, 95
 systemowe, 340
 obsługa
 błędów strony, 420
 kompilatora, 822
 pamięci, 77
 procesorów, 77
 sprzętu, 102
 systemów plików, 530
 technologii Plug and Play, 530, 615, 625
 usług systemowych, 71
 usługi WMI, 530, 531
 zabezpieczeń, 703
 zadania, 209
 zarządzania zasilaniem, 530
 zewnętrznych procesów, 143

- ochrona
 - CFG w jądrze, 820
 - hasła, 671
 - klucza NTOWF, 672
 - komponentów, 835–841
 - obiektów, 678
 - pamięci, 354
 - poświadczeń, 670
 - przed poprawkami jądra, 669, 834, 835
 - przepływu sterowania, 809
 - urządzenia, 676
- OEM, Original Equipment Manufacturer, 107
- ograniczanie
 - ryzyka ataku, 803–807
 - uruchamiania plików, 827
- ograniczenia
 - adresowania wirtualnego, 396
 - oprogramowania, 832
 - pamięci fizycznej, 488
- okienka i grafika, 71
- OLE, Object Linking and Embedding, 23
- opcja Izolowany tryb użytkownika, 81
- operacje wejścia-wyjścia, 271, 529–662
 - agnostyczne względem wątków, 589
 - analiza wydajności, 605
 - anulowanie, 589
 - asynchroniczne, 560
 - bezpośrednie, 581
 - buforowane, 579
 - Driver Verifier, 606
 - instalowanie ogólnego sterownika, 631
 - kolejkowanie asynchronicznego żądania, 586
 - kolejkowanie pakietów IRP, 588
 - komponenty systemu, 529
 - kończenie przetwarzania pakietów IRP, 588
 - menedżer, 531
 - określanie priorytetu, 599
 - pakiety żądań IRP, 563
 - podnoszenie priorytetu, 603
 - położenia stosu, 565
 - porównanie przepustowości, 603
 - porty ukończenia, 594, 596
 - powiadomienia kontenerów, 606
 - przepływ operacji, 642
 - przetwarzanie, 532, 559
 - realizowanie warstwowego żądania, 587
 - rezerwacja przepustowości, 605
 - sterowniki urządzeń, 539
 - strategie określania priorytetów, 599
 - stronicowanie, 425
 - synchroniczne, 560
 - szybkie, 560
 - środowisko KMDF, 641
 - unikanie inwersji priorytetów, 602
 - wyliczanie urządzeń, 615
 - z mapowaniem plików, 562
 - z techniką rozrzucania/zbierania, 562
 - żadne, 582
 - żądania, 574, 586
- oprogramowanie sprzętowe, 49
- osłabianie
 - exploitów, 801
 - procesów, 803
- otwieranie
 - obrazu, 162
 - urządzeń, 555

P

- PAE, Physical Adress Extension, 409
- pakiet
 - IRP, 532, 564, 571
 - Kerberos, 778, 779
 - MCM, 306
 - MSV1_0, 778
- pakiety
 - pochodzenie, 752
 - uwierzytelniania, 667
 - znaczniki, 753
- pamięć, 337–527
 - ACL, 356
 - architektura kompresji, 495
 - asocjacyjna, 415
 - blokowanie, 350
 - buforowana, 342
 - deklarowanie, 348
 - dostępna, 342
 - enklawy, 510
 - fizyczna, 337
 - ograniczenia, 488
 - Kompozycja pamięci, 342
 - kompresja, 491, 497
 - liczniki wydajności, 341
 - likwidowanie wycieku, 368
 - limity, 489
 - ładunek deklaracji, 350
 - mechanizm AWE, 362
 - ochrona, 354

- opcje zabezpieczenia, 355
- partycje, 498
- plik stronicowania, 352
- proaktywne zarządzanie, *Patrz* SuperFetch
- przydzielanie, 346, 347
- podręczna, 387
- Pula niestronicowana, 342, 363
- Pula stronicowana, 342
- rezerwowanie, 348
- rodzaje alokacji, 433
- rozmiary pul, 363
- scalanie, 501
- stronicowanie, 337
- strony, 339
 - deklarowane, 348
 - rezerwowane, 348
- synchronizacja wewnętrzna, 344
- systemowe pule, 363
- tabela stron, 424
- W użyciu, 342
- wirtualna, 40, 337
- Wolna, 342
- współdzielona, 351
- Wykorzystanie pamięci, 342
- Zadeklarowana, 342
- zwalnianie, 346
- partycja systemowa, 499
- partycje pamięci, 498
- PatchGuard, 835
- PCR, Processor Control Region, 330
- PEB, 194
- PEP, Platform Extension Plug-in, 659
- personalizacja, 680
- personifikacja, 702
- PFN, 426, 482–484
- piaskownica, 215, 498
- Pico, 145
- pikodostawcy, 91
- planista
 - bezczynności, 300
 - skalowalność, 307
- planowanie, 283
 - DFSS, 317
 - dynamiczne ze sprawiedliwym udostępnianiem, 323
 - heterogeniczne wątków, 320
 - oparte na grupach, 322
 - generacja, 322
 - udział, 322
 - waga, 322
 - terminowe, 285
 - wątków, 243
 - baza danych dyspozytora, 258
 - głębokie zamrożenie, 296
 - heterogeniczne, 320
 - kwant, 260
 - poziomy priorytetów, 245
 - przełączanie kontekstu, 286
 - stany, 252
 - systemy wieloprocesorowe, 300, 316
 - warianty, 288
 - wstrzymanie, 296
 - wyбір procesora, 317
 - wyбір wątku, 298
 - zwiększanie priorytetu, 268
 - ze sprawiedliwym przydziałem, 322
- platforma
 - ARM
 - tłumaczenie adresów wirtualnych, 419
 - układ przestrzeni adresowej, 394
 - filtrowania systemu, 838
 - OneCore, 22
 - x64
 - ograniczenia adresowania wirtualnego, 396
 - tłumaczenie adresów wirtualnych, 418
 - układ przestrzeni adresowej, 394
 - x86
 - przebieg sesji, 391
 - tłumaczenie adresów wirtualnych, 409
 - układ przestrzeni adresowej, 388, 391
- plik
 - afd.sys, 217
 - audiodg.exe, 137
 - Bash.exe, 92
 - bioiso.exe, 151
 - Chkdisk.exe, 389
 - Ci.dll, 104
 - cmd.exe, 90, 164
 - Conhost.exe, 88, 90
 - Csrss.exe, 87, 112
 - Dllhst3g.exe, 389
 - Dwm.exe, 88
 - Dxgkrnl.sys, 129
 - explorer.exe, 227
 - fsiso.exe, 151
 - Halmacpi.dll, 103
 - Hvix64.exe, 71
 - Inetinfo.exe, 389
 - Keyboard.inf, 628

plik

LogonUI.exe, 123, 667
 LsaIso.exe, 112, 119, 669, 673
 Lsass.exe, 112, 123, 389, 669
 Lxcore.sys, 91
 Lxss.sys, 91
 Mmc.exe, 799
 msinfo32.exe, 544
 msmtpeng.exe, 144
 Msrpc.sys, 104
 nissvc.exe, 144
 Npfs.sys, 93
 notmyfault.exe, 592
 Ntoskrnl.exe, 71, 88, 100, 340
 ntvdm.exe, 164
 onedrive.exe, 193
 PowerShell.exe, 833
 Procexp.exe, 113
 Pstat.exe, 113
 securekernel.exe, 82
 Services.exe, 112, 119
 Ssms.exe, 112, 115, 215, 389, 428
 sppsvc.exe, 141
 Srv2.sys, 114
 Svchost.exe, 122
 swapfile.sys, 432
 Tasklist.exe, 113
 Tlist.exe, 113
 Userinit.exe, 123
 wcifs.sys, 215
 Win32k.sys, 71, 88, 89
 Win32kBase.sys, 89
 Win32kFull.sys, 89
 Win32kMin.sys, 89
 Wininit.exe, 112, 119
 Winlogon.exe, 112, 122, 667
 wymiany, swap file, *Patrz* pliki stronicowania

pliki

.sys, 71
 INF, 531, 628
 mapowane, 351
 sterowników dla Direct X, 71
 stronicowania, 352, 422, 427, 431

- obliczanie rozmiaru, 429
- rezerwacja, 485
- sprawdzanie poziomu użycia, 436
- wirtualne, 432
- zalecane rozmiary, 430

systemu Windows, 71
 wykazu, 629
 PLM, Process Lifecycle Manager, 429
 PMP, Protected Media Path, 137
 pobieranie z wyprzedzeniem, 453
 podgląd zdarzeń, 830
 podnoszenie uprawnień, 798

- automatyczne, 799

 podrzucanie binariów, 189
 podsystem

- POSIX, 91
- środowiskowy, 84
- Windows, 87, 112
 - dla systemu Linux, 91

 podwyższanie uprawnień, 794
 pola

- rejestru Win32PrioritySeparation, 266

 struktury

- CSR_THREAD, 235
- KTHREAD, 225
- PEB, 134
- procesów jądra, 131
- TEB, 231
- W32THREAD, 236
- wykonawczej procesu, 130

 polecenie

- !devobj, 552
- !drvobj, 552, 561
- !handle, 132
- !heap, 379
- !irp, 592
- !object, 550
- !peb, 196
- !pocaps, 655
- !process, 132, 592
- !silo, 217
- !teb, 231
- !thread, 227, 568
- powercfg, 655
- System Information, 365
- tlist, 229

 POSIX, 91
 powiadomienia

- filtra rejestru, 838
- kontenerów, 606
- o stanie pamięci, 463
- procesu, 838

 poziom podniesienia uprawnień, 798

- poziomy
 - integralności, 688, 702
 - identyfikatorów SID, 688
 - obiektów, 692
 - procesów, 689
 - klas TCSEC, 664
 - personifikacji, 704
 - priorytetów wątków, 245
 - żądań przerwania, 535
- PPL, Protected Process Light, 115, 138, 143
- prawa
 - dostępu, 724, 725
 - konta, 732
 - użytkownika, 733–736
 - właścicielskie, 723
- PRCB, Processor Control Block, 258, 330
- prefetcher, 453, 455
- priorytet
 - strony, 477, 520
 - wątku, 245, 268–286
- priorytety
 - czasu rzeczywistego, 248
 - operacji wejścia-wyjścia, 599
- proaktywne zarządzanie pamięcią, *Patrz* SuperFetch
- procedura
 - MiCheckReservePageFileSpace, 486
 - MiCombineIdenticalPages, 502
- procedury
 - instrumentacji zarządzania systemu, 97
 - pomocnicze WHEA, 98
 - wymiany procesu, 338
- proces, 39, *Patrz także* plik
 - LogonUI, 122
 - LSAlso, 666
 - Lsass, 666
 - Memory Compression, 495
 - System, 112, 113
 - Userinit, 122
 - UWP, 751, 753
 - Winlogon, 122, 776
- procesor
 - dynamiczne dodawanie i usuwanie, 330
 - idealny, 310
 - logiczny, 305
 - następny, 310
 - ostatni, 310
- procesy, 27, 125–206
 - bezczynności, 112, 292
 - bezpieczeństwa systemu, 112, 115
 - bezpieczne, 147
 - chronione, 137
 - certyfikacji WHQL, 44
 - etapy tworzenia, 156, 162, 165, 171, 174, 176
 - funkcja CreateProcess, 155
 - hosta konsoli, 88
 - inicjalizacyjne, 119
 - kompresji pamięci, 112, 115
 - kończenie, 183
 - logowania, 112
 - menedżera sesji, 116
 - minimalne, 144
 - nadrzędne, 31
 - Pico, 144
 - programu Trustlet, 147
 - serwera podsystemu środowiskowego, 70
 - systemowe, 70, 112
 - tworzenie, 125
 - usługowe, 70
 - użytkownika, 70
 - wczesna inicjalizacja, 186
 - wewnętrzne elementy, 129
 - zasady osłabiania, 803
- program, 26
 - ładujący
 - flagi wpisów tabeli danych, 198
 - obrazy, 184, 185
 - poła wpisu tabeli danych, 195
 - wymiany, 461
- programowalny kontroler przerwania, 103
- projektowanie sterowników, 634
- protokoły uwierzytelniania, 783
- protokół
 - Kerberos, 675
 - NTLM, 674
- przechwytywanie NDIS, 838
- przedrostki, 110, 111
- przeoglądanie
 - atrybutów tokenowych, 756
 - atrybutów zabezpieczeń kontenera aplikacji, 759
 - bazy danych PFN, 468
 - deskryptorów adresów wirtualnych, 442
 - filtrowanych tokenów, 706
 - identyfikatorów SID, 686
 - masek dostępu, 683
 - możliwości kontenera aplikacji, 765
 - obszarów sterowania, 448
 - partycji pamięci, 500

- przeglądanie
 - plików stronicowania, 429
 - sesji, 392
 - tabeli atomów kontenera aplikacji, 761
 - tokenów dostępowych, 696
 - tokenu kontenera aplikacji, 755
 - wpisów PFN, 484
 - wykorzystania przestrzeni sesyjnej, 393
 - zaufanych identyfikatorów SID, 719
 - zawartości deskryptora zabezpieczeń, 715
 - przejścia stanów zasilania urządzenia, 651
 - przekierowywanie
 - .LOCAL, 191
 - bibliotek DLL, 191, 192
 - mechanizmu API Set, 191
 - rozszerzenia Fusion, 192
 - przełączanie
 - kontekstu, 244, 286
 - użytkowników, 519
 - przenośność, 67, 72
 - przepływ
 - operacji wejścia-wyjścia, 642
 - pakietu IRP, 569
 - sterowania, 808
 - ochrona, 809
 - przerwania
 - IRQL, 535
 - międzyprocesorowe, 426
 - przestrzeń
 - adresowa
 - analiza, 403
 - hiperprzestrzeń, 387
 - jądra, 407
 - kod systemowy, 387
 - lista zestawów roboczych, 387
 - ogólnosystemowa wirtualna, 402
 - pamięć podręczna, 387
 - przydziały, 402
 - użytkownika, 403
 - nazw obiektów, 767
 - sesji, 391
 - przetwarzanie
 - operacji wejścia-wyjścia, 559
 - pakietów IRP, 642
 - przydziały
 - systemowej wirtualnej przestrzeni
 - adresowej, 402
 - użytkowników, 402
 - przydzielanie pamięci, 347
 - przypisywanie procesorów do grupy, 304
 - przywilej, 732–740
 - Debuguj programy, 739
 - Działanie jako część systemu operacyjnego, 740
 - Ładuj i zwalnij sterowniki urządzeń, 740
 - Obejdź sprawdzanie przy przechodzeniu, 738
 - Przejmij na własność, 739
 - Przywracaj pliki i katalogi, 740
 - SeTimeZonePrivilege, 737
 - Utwórz obiekt tokenu, 740
 - PSM, Process State Manager, 751
 - PTE, Page Table Entry, 409, 416, 423, 447, 466, 482
 - pula
 - niestronicowana, 363
 - stronicowana, 363
 - pule wątków, 332
- ## R
- ramka wyjątków, 185
 - randomizacja
 - obrazu, 405
 - sterty, 407
 - stosu, 406
 - raportowanie błędów systemu, 525
 - region PCR, 330
 - reguła
 - No-Execute-Up, 691
 - No-Read-Up, 691
 - No-Write-Up, 691
 - reguły
 - AppLockera, 828
 - licencjonowania, 78
 - uwierzytelniania, 675
 - rejestr, 53, 531
 - ProductType, 78
 - rezerwacja pliku stronicowania, 485, 486
 - RID, Relative Identifier, 684
 - rodzaje alokacji pamięci, 433
 - rozmiar
 - pliku stronicowania, 428, 435
 - zestawu roboczego, 458
 - rozpoznawanie linii papilarnych, 784
 - rozszerzalność, 67
 - rozszerzenia
 - HAL, 103
 - obiektu pliku, 557
 - adresu fizycznego, 409

rozwiązywanie nazw bibliotek DLL, 189
 RVA, Relative Virtual Address, 810
 ryzyko ataku, 803–807

S

SACL, 711, 713
 SAM, Security Accounts Manager, 123, 666
 SAS, Secure Attention Sequence, 665
 scalanie pamięci, 501, 504, 507
 etap klasyfikacji, 503
 etap scalania stron, 504
 etap wyszukiwania, 502
 konwersja wpisu PTE, 505
 zwalnianie stron scalonych, 506
 schemat
 korzystania z TLB, 416
 mechanizmu SuperFetch, 517
 procesu tłumaczenia adresów, 410
 SCM, Service Control Manager, 119, 544
 SDK, Software Development Kit, 64
 segment stanu zadania, 100
 sekcje, 352
 oparte na pliku stronicowania, 352
 sekwencja SAS, 777
 sekwencyjny dostęp do katalogu, 522
 separacja priorytetu, 266
 serwer, 106
 Active Directory, 667
 FTH, 385
 informacji internetowych, 389
 plików, 114
 uwierzytelniania zabezpieczeń lokalnych, 112
 sesje
 0 inicjalizacji, 112
 logowania, 667
 SID, Security Identifiers, 684
 ograniczone, 705
 silnik podkładki jądra, 98
 silosy serwerowe, 213
 granice izolacji, 216
 izolacja, 214
 konteksty, 218
 monitory, 218
 tworzenie, 219
 skalowalność, 75
 planisty, 307
 składniki podsystemu Windows, 87
 skrót pliku, 828
 skrzynki pocztowe, 153

SLAT, Second Level Address Translation, 83
 SLS, Silo Local Storage, 217
 SoC, System on a Chip, 659
 solidność, 68
 sprawdzanie
 aktywności wątków, 237
 dostępu, 681
 funkcji rozdzielania sterownika, 567
 obiektów urządzeń, 550
 pakietów IRP, 571
 pliku INF sterownika, 628
 poziomu integralności procesu, 689
 poziomu IRQL, 611
 praw dostępu, 725
 priorytetów procesów, 249
 priorytetów wątków, 249
 puli wątków, 334
 typu podsystemu, 85
 wykorzystania pamięci, 341
 wykorzystania stosu jądra, 440
 zabezpieczenia DEP, 359
 zaległych pakietów IRP wątku, 568
 sprawiedliwe udostępnianie, 323
 SQOS, security quality of service, 704
 SRM, Security Reference Monitor, 217, 666
 grupy, 711
 SRP, Software Restriction Policies, 832
 SSPI, Security Support Provider Interface, 703
 stan
 Connected Standby, 652
 Modern Standby, 652
 procesora logicznego, 306
 strony, 347, 466
 wątku
 gotowość, 252
 oczekujący, 253
 odroczone gotowość, 252
 przejście, 253
 uruchomiony, 253
 w pogotowiu, 252
 zainicjowany, 253
 zakończony, 253
 zasilania systemu, 648, 650, 653
 zasilania urządzenia, 653
 standard ACPI, 648
 sterownik, 530
 instalacja, 633
 ładowanie, 631
 zasada zasilania, 653

sterowniki

- drukarek, 539
- filtrów, 107, 540
- funkcji, 107, 540
- jądra, 106
- klas, 541
- KMDF, 635
 - funkcja dodawania urządzenia, 636
 - funkcja inicjalizacji, 636
 - funkcje EvtIo*, 636
- magistrali, 107, 540
- miniklas, 541
- miniportów, 542
- oprogramowania, 106
- portów, 542
- programowe, 633
- protokołów, 106
- przekierowania sieciowego, 106
- serwera plików, 114
- skanera biometrycznego, 785
- strumieniowe jądra, 106
- systemowe, 544
- systemu plików, 106, 540
- UMDF, 539, 644
 - aplikacje, 646
 - architektura modelu, 646
 - jądro systemu, 646
 - menedżer, 646
 - proces hosta, 647
 - reflektor, 646
- uniwersalne, 108
- urządzeń, 71, 105, 539
 - funkcja anulowania operacji
 - wejścia-wyjścia, 547
 - funkcja dodawania urządzenia, 546
 - funkcja inicjalizacji, 546
 - funkcja obsługi przerwania ISR, 546
 - funkcja powiadamiania o zamykaniu systemu, 548
 - funkcja rozpoczynania operacji
 - wejścia-wyjścia, 546
 - funkcja ukończenia operacji
 - wejścia-wyjścia, 547
 - funkcja usuwania z pamięci, 548
 - funkcja wywołań DPC, 547
 - funkcje rejestrowania błędów, 548
 - funkcje szybkiego rozdzielania, 547
 - graficznych, 88
 - obiekty, 548

- otwieranie, 555
- sprzętowych, 106
- struktura, 545
- trybu jądra, 88
- typy, 539
- zabezpieczenia, 667
- zestaw funkcji rozdzielania, 546
- WDF, 634
- WDM, 540
- z obsługą technologii Plug and Play, 540, 627
- z warstwami, 586
- zainstalowane, 109

sterta, 363, 370

- bezpieczeństwo, 379
- funkcje bezpieczeństwa, 380
- funkcje debugowania, 380
- NT, 372
- o małej fragmentacji, 372, 373
- odporna na błędy, 385
- procesu, 371
- randomizacja, 407
- segmentowa, 374
- synchronizacja, 373

stos

- DPC, 440
- jądra, 439
- randomizacja, 406
- urządzeń, 571, 618
- użytkownika, 438

stronicowanie, 337

- danych, 40
- na żądanie, 452
- plik, 427
- strategia rozmieszczania, 456
- strategia zamiany, 456

strony

- adres PTE, 481
- licznik odwołań, 481
- deklarowane, 348
- duże, 339
- małe, 339
- objęte klastrem, 487
- oczekujące, 471
- PFN, 482
- priorytet, 520
- PTE, 482
- ramki, 469
- rezerwowane, 348
- stany, 347, 466

- typ, 481
- wolne, 470
- współużytkowane, 424
- wyzerowane, 469, 470
- zmapowane, 479
- zmodyfikowane, 471, 479
- znaczniki, 481, 482
- struktura
 - CSR_PROCESS, 135, 235
 - CSR_THREAD, 235
 - EPROCESS, 129, 131
 - ETHREAD, 224
 - IO_STACK_LOCATION, 565
 - KLDR_DATA_TABLE_ENTRY, 197
 - KPCR, 100
 - KPRCB, 100
 - KSCB, 323
 - KSHARED_READY_QUEUE, 259
 - KTHREAD, 226
 - LDR_DATA_TABLE_ENTRY, 196
 - PEB, 133, 134, 170, 194, 224
 - PEB_LDR_DATA, 196
 - PRCB, 258
 - PROCESS_INFORMATION, 127
 - SECS, 513
 - STARTUPINFO, 127
 - TEB, 224
 - pola, 231
 - sprawdzanie, 231, 233
 - W32THREAD, 235
- struktury
 - danych
 - PFN, 481
 - w magazynie, 496
 - kontroli wątku, 515
 - pakietów IRP, 564
 - programu Trustlet, 148
 - sterownika, 545
 - dla trybu jądra, 108
 - dla trybu użytkownika, 108
 - KMDF, 635
 - VAD procesu, 441
 - wątku jądra, 225
 - wewnętrzne sekcji, 447
 - zabezpieczeń procesów i wątków, 741
- SuperFetch, 515
 - agenty, 516
 - dublowanie procesu, 525
 - funkcja Ready Boost, 523
 - funkcja Ready Drive, 524
 - komponenty, 516
 - menedżer scenariuszy, 516
 - moduł ponownego bilansowania, 517
 - moduł śledzenia, 516
 - moduł zbierający, 516
 - niezawodność działania, 522
 - ponowne bilansowanie, 520
 - priorytet strony, 520
 - rejestrowanie, 518
 - scenariusze, 519
 - schemat mechanizmu, 517
 - śledzenie, 518
 - superprzywileje, 739
 - SwitchBack, 201
 - działanie technologii, 203
 - identyfikatory GUID, 201
 - tryby zgodności, 202
 - SxS, Side-by-Side, 184
 - symbole globalne, 96
 - synchronizacja sterty, 373
 - system
 - heterogeniczny, 321
 - NUMA, 301
 - operacji wejścia-wyjścia, 529–662
 - plików
 - NTFS, 92, 466
 - VFS, 92
 - wieloprocessorowy, 73, 300, 316
 - working set, 462
 - zabezpieczeń, 666
 - systemowa przestrzeń adresowa, 398
 - hiperprzestrzeń, 387
 - lista zestawów roboczych, 387
 - pamięć podręczna, 387
 - pula stronicowana, 387
 - warstwa HAL, 387
 - zrzut awarii, 387
 - systemowe
 - wpisy tabeli stron, 393
 - zestawy robocze, 462
 - systemowy limit deklaracji, 432
 - szablon kontenera, 221
 - szeregowanie wątków, 75
 - szybkie przełączanie użytkowników, 50, 519

Ś

ścieżka katalogu, 828

śledzenie

- uruchamiania procesu, 178
- zdarzeń systemu, 98, 149, 838

środowisko

- .NET Framework, 25
- AppContainer, 757
- KMDF, 634, 635
 - atrybuty obiektów, 641
 - hierarchia obiektów, 640
 - obsługa żądań, 644
 - operacje wejścia-wyjścia, 641
- UMDF, 634, 644
- WDF, 634
- zarządzania zasilaniem, 658

T

tabela

- ACPI SRAT, 306
- atomów kontenera aplikacji, 761
- danych programu ładującego, 194
- GDT, 330
- IAT, 184
- importu, 184
- rozdziału przerw, 100
- stron, 409, 412, 424, 467

tablica SLS, 217

TCB, Trusted Computing Base, 141

TCS, Thread Control Structure, 515

TEB, Thread Environment Block, 224

technologia

- PnP, 530, 614
 - instalacja sterownika, 627
 - ładowanie sterowników, 620
 - sterowniki, 625
 - wyliczanie urządzeń, 615
- SGX, 510
- SwitchBack, 201

TLB, Translation Lookaside Buffer, 339, 415

TLS, Thread Local Storage, 184

tłumaczenie adresów, 410, 416

- wirtualnych, 411
 - platforma ARM, 419
 - platforma x64, 418
 - platforma x86, 409

token, 692, 694

- administracyjny, 705
 - dostępowy procesów i wątków, 740
 - dostępu, 40
 - kontenera aplikacji, 755
 - ograniczony, 705
 - procesu UWP, 695, 751
- translacja adresów, 415
- drugiego poziomu, 83
- Trustlet, 83, 148
- atrybuty, 150
 - LSA, 119
 - metadane zasad, 149
 - opcje zasad, 149
 - struktura programu, 148
 - tożsamość programów, 151
 - wbudowane programy, 151
 - wywołania systemowe, 153

tryb

- jądra, 43, 68
 - centrum wykonawcze, 71
 - jądro, 71
 - okienka i grafika, 71
 - sterowniki urządzeń, 71
 - warstwa abstrakcji sprzętowej, 71
 - warstwa hipernadzorczy, 71
- użytkownika, 43, 68
 - izolowany, 81
 - procesy serwera podsystemu
 - środowiskowego, 70
 - procesy systemowe, 70
 - procesy usługowe, 70
 - procesy użytkownika, 70

tryby powiadamiania portu ukończenia, 598

TSS, Task State Segment, 100

tworzenie

- fabryki wątków roboczych, 333
- obiektu procesu wykonawczego, 165
- obszaru adresów procesu, 168
- początkowego wątku, 171
- procesu, 125
- procesu nowoczesnej aplikacji, 128
- rozszerzeń HAL, 103
- silosu serwerowego, 219
- sterowników, 529
- struktury procesu jądra, 168
- wątków, 223
- zrzutu drzewa urządzeń, 617

typy

- obiektów KMDF, 638
- procesów, 147

U

UAC, User Account Control, 123, 680, 692, 787
wartości rejestrów, 802

UAP, Universal Application Platform, 748

uchwyty

- kontenera aplikacji, 769
- zapisane w tokenie, 770

UDDI, Universal Device Driver Interface, 662

udział procesu w pliku stronicowania, 433

UEFI, Unified Extensible Firmware Interface,
648, 674

UIPI, User Interface Privilege Isolation, 680, 721

układ

- platformy Windows, 750
- przestrzeni adresowej, 42, 388, 394
- systemowej, 391
- użytkownika, 403
- struktury SECS, 513

UMDF, User-Mode Driver Framework, 108,
634, 644

Unicode, 53

unikatowy identyfikator globalny, 149

uniwersalna platforma Windows, 371

uprawnienia, 693, 702, 749, 794

- administracyjne, 795

uprzywilejowana kontrola dostępu, 52

uruchamianie podsystemu, 86

usługi, 26, 120

- Active Directory, 667
- biometryczne, 784
- HVCI, 676
- izolowanego trybu użytkownika, 152
- kryptograficzne, 153
- logowania sieciowego, 667
- LSA, 669
- menedżera pamięci, 345
- MMCSS, 284, 285
- PEP, 659
- Superfetch, 453, 455
- systemu Windows, 26
- terminalowe, 49
- uwierzytelniania zabezpieczeń lokalnych, 112
- WMI, 530, 531
- zainstalowane, 121

ustawienia

- funkcji Kontrola konta użytkownika, 800
- zabezpieczeń, 726
- zasilania, 655

usuwanie

- bibliotek DLL, 184
 - procesorów, 330
- uwierzytelnianie, 675, 778
- wzmocnione, 783
 - zabezpieczeń, 389
 - zabezpieczeń lokalnych, 119

UWP, Universal Windows Platform, 184, 371,
751

uznaniowa kontrola dostępu, 52, 679

V

VAD, Virtual Address Descriptor, 348, 423, 441

VBS, Virtualization-Based Security, 48, 98

VDM, Virtual DOS Machine, 87

VFS, Virtual File System, 92

VSM, Virtual Secure Mode, 81, 461

VTL, Virtual Trust Level, 48, 81

W

warianty planowania wątków, 288

warstwa, 529

- abstrakcji HAL, 531
- abstrakcji sprzętowej, 71, 102
- hipernadzorcy, 71
- sterownika systemu plików, 542
- sterowników, 541

warstwowa budowa systemu, 72

wartości ochrony procesów, 139

wątek, 37, 223–336

- baza danych dyspozytora, 258
- bezczynności, 292
- chronionych procesów, 242
- cykl istnienia, 236
- dereferencji segmentu, 339
- dynamiczne dodawanie procesorów, 330
- fabryki wątków roboczych, 333
- głębokie zamrożenie, 296
- kwant, 260
- lekki, 38
- pierwszoplanowy, 274

- wątek
 - planowanie, 243
 - heterogeniczne, 320
 - warianty, 288
 - poziomy priorytetów, 245
 - priorytety czasu rzeczywistego, 248
 - sprawdzanie aktywności, 237
 - stany, 252
 - struktury danych, 224
 - systemowy, 113
 - tworzenie maksymalnej liczby, 438
 - UMS, 39
 - w systemach wieloprocesorowych, 316
 - wstrzymanie, 296
 - wybór procesora, 317
 - zerowania stron, 339, 469
 - zwiększanie priorytetu, 268
- wczesna inicjalizacja procesu, 186
- WDF, Windows Driver Foundation, 108, 634
- WDI, Windows Diagnostic Infrastructure, 98, 525
- wejście-wyjście pliku mapowanego, 444
- WER, Windows Error Reporting, 525
- wersja systemu, 20
 - Checked build, 79
 - kliencka, 76
 - serwerowa, 76
- weryfikator sterowników, 98
- węzeł, 74
 - urządzeń, 619
- WHQL, Windows Hardware Quality Labs, 44
- widoki, 387
- wieloprocesorowość
 - heterogeniczna, 74
 - symetryczna, 73
- wiersz polecenia, 833
- Windows Driver Kit, 64
- Windows Hello, 786
- Windows Runtime, 24
- Windows Software Development Kit, 64
- Windows System Resource Manager, 252
- windowsowy model sterowników, 97
- WinTCB, Windows Trusted Computer Base, 139
- wirtualizacja, 669, 787
 - mechanizmy bezpieczeństwa, 81
 - rejestr, 788, 793
 - systemu plików, 788–791
 - UAC, 790
- wirtualna przestrzeń adresowa, 337, 386, 397, 402
- wirtualne
 - konta usług, 706
 - poziomy zaufania, 81
- wirtualny
 - plik stronicowania, 432
 - rejestr, 215
 - system plików, 215
 - tryb bezpieczny, 461
 - tryb chroniony, 81
- właściciel obiektu, 723
- włączanie
 - przywileju, 737
 - globalnych zasad inspekcji, 746
- włókna, 38
- WMC, Windows Media Certificate, 137
- WMI, Windows Management Instrumentation, 207, 530
- wpis
 - ACE, 714
 - warunkowy, 730
 - zaufany, 718
 - katalogu stron, 412
 - MDL, 426
 - PFN, 484
 - PTE, 393, 447, 466
 - programowy, 422
 - prototypowy, 423
 - prywatny, 505
 - współdzielony, 505
 - tabeli stron, 393, 409–413
- WPP, Windows PreProcessor, 81
- WSK, Windows Sockets for Kernel, 92
- wskaźnik
 - złych odrzuceń, 786
 - złych zezwoleń, 786
- wskaźniki obiektu sekcji, 447
- współdzielenie pamięci, 352
- wstrzymanie wątków, 296
- wybór
 - procesora, 317
 - wątku, 298
 - w systemach wieloprocesorowych, 316
- wyciek pamięci, 368
- wydajność, 68
- wykorzystanie
 - pamięci, 341
 - procesora, 327
 - stosu jądra, 440
 - systemowej przestrzeni adresowej, 398

- wymuszenie zasad SRP, 833
 - wrażenia warunkowe, 730
 - wyświetlanie
 - chronionych procesów, 142
 - dojść do urządzeń, 557
 - drzewa procesów, 31
 - formatu struktury, 131
 - gotowych wątków, 259
 - informacji o procesorach, 301
 - informacji o sterownikach KMDF, 636
 - informacji o systemie NUMA, 302
 - informacji o wątkach, 229, 242
 - informacji o węzle urządzeń, 624
 - koligacji procesu, 308
 - listy struktur jądra, 61
 - listy zainstalowanych sterowników, 109, 544
 - listy zainstalowanych usług, 121
 - mapowań zasilania, 654
 - obiektów sterowników, 552
 - obiektów urządzeń, 552
 - obiektu zadania, 211
 - plików wykazu, 629
 - stosu urządzeń, 571
 - stosu wątku, 239, 240
 - struktur wątków, 292
 - struktury ETHREAD, 226
 - szczegółów procesu, 35
 - wyeksportowanych funkcji, 54
 - zasad zasilania, 655
 - żądań dostępności zasilania, 661
 - wyłączanie, 289
 - wywołania
 - ALPC, 288
 - DPC, 535, 537
 - procedur zróżnicowanych, 440
 - synchroniczne RPC, 288
 - zdalne COM, 288
 - względne adresy wirtualne, 810
- Z**
- zabezpieczanie pamięci, 355
 - zabezpieczenia, 51
 - ASLR, 408
 - procesów i wątków, 741
 - VBS, 48
 - zaciemnianie kodu, 834
 - zadania, 40, 206–222
 - hierarchia, 210
 - limity, 207
 - tworzenie, 209
 - zagnieżdżone, 209
 - zainstalowane
 - sterowniki, 109
 - usługi, 121
 - zamrożenie, 296
 - zapobieganie wykonywaniu danych, 356, 358
 - zarządzanie
 - mechanizmami zaufanymi, 665
 - oknami konsolowymi, 90
 - pamięcią, 337–527
 - prawami cyfrowymi, 44
 - proaktywne pamięcią, *Patrz* SuperFetch
 - stanami wydajności, 659
 - systemową wirtualną przestrzenią adresową, 397
 - zasilaniem, 530, 625, 658
 - zestawami roboczymi, 457
 - zasada, 149
 - Wymuszanie, 832
 - Wyznaczone typy plików, 832
 - Zaufani wydawcy, 832
 - zasady
 - inspekcji, 741
 - globalne, 745
 - ustawienia, 747
 - KMCS, 44
 - ograniczeń oprogramowania, 832
 - osłabiania procesów, 803
 - zabezpieczeń lokalnych, 741
 - zasilanie, 648
 - systemu
 - stan Connected Standby, 652
 - stan Modern Standby, 652
 - stany, 648, 650, 653
 - urządzenia, 657
 - stany, 653
 - zasoby procesu, 39
 - zaufana baza obliczeniowa, 141
 - zdarzenia
 - dyspozytora, 268
 - ETW, 312
 - planisty, 268

zdarzenie

- HighCommitCondition, 464
- HighMemoryCondition, 464
- HighNonPagedPoolCondition, 464
- HighPagedPoolCondition, 464
- LowCommitCondition, 464
- LowMemoryCondition, 464
- LowNonPagedPoolCondition, 464
- LowPagedPoolCondition, 464
- MaximumCommitCondition, 464
- MemoryErrors, 464

zestaw

- Debugging Tools for Windows, 59
- SMT, 300
- Windows Software Development Kit, 64

zestawy

- procesorów, 311, 312
- robotyczne, 337
 - menedżer, 457
 - procesowe, 452
 - przeglądanie listy, 460
 - przycinanie, 461
 - rozszerzanie, 461
 - sesyjne, 452
 - systemowe, 452, 462
 - zarządzanie, 457

ziarnistość alokacji, 351

zmiany stanów planowania wątków, 254

znaczniki

- ochrony przepływu sterowania, 818
- pakietu, 753
- PTE, 416
- wirtualizacji rejestru, 793

zrzut

- awaryjny trybu jądra, 834
- bazy danych załadowanych modułów, 196
- drzewa urządzeń, 617
- kontekstu silosu monitora SRM, 217
- metadanych zasad, 153
- po awarii, 149
- struktury PEB, 134
- tabeli dojsć procesów, 132
- zwiększanie priorytetu wątku, 268–286

Z

żądania

- dostępności zasilania, 660
- przerwań IRQL, 535
- uprawnień administracyjnych, 797
- WMI, 207

PROGRAM PARTNERSKI

— GRUPY HELION —

1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion

Windows

od podszewki — poznaj i zrozum!



Systemy operacyjne Windows 10 i Windows Server 2016 zdecydowanie różnią się od swoich poprzedników.

Są bardziej złożone, a niektóre zastosowane rozwiązania można określić jako zaawansowane i wysublimowane.

Zwłaszcza znajomość wewnętrznych mechanizmów systemu, architektury jądra i systemowego modelu bezpieczeństwa okazuje się niezwykle istotna dla programistów i inżynierów odpowiadających za bezpieczeństwo. Bez tej wiedzy trudno mówić o prawdziwie niezawodnej pracy oprogramowania tworzonego dla maszyn pracujących pod kontrolą najnowszych wersji systemu Windows.

Ta książka jest pierwszym tomem klasycznego przewodnika po wewnętrznych mechanizmach podstawowych komponentów systemu Windows. Omówiono w niej jego architekturę, sposoby implementowania i modyfikacji procesów, przetwarzania wątków oraz korzystania z pamięci fizycznej i wirtualnej. Sporo miejsca poświęcono operacjom wejścia-wyjścia oraz integracji ze sterownikami poszczególnych urządzeń. Szczegółowo przedstawiono zabezpieczenia wbudowane w system. Projektanci oprogramowania, specjaliści do spraw bezpieczeństwa oraz administratorzy systemów informatycznych znajdą tu wiele ważnych informacji, dzięki którym dogłębnie zrozumieją sposób działania systemu, co pozwoli im na podejmowanie lepszych decyzji.

Najważniejsze zagadnienia:

- wprowadzenie do wewnętrznych mechanizmów systemu Windows
- omówienie komponentów architektury systemu
- procesy, zadania, wątki
- funkcjonowanie menedżera pamięci i sposoby jej modyfikacji
- operacje wejścia-wyjścia i obsługa urządzeń peryferyjnych
- mechanizmy zabezpieczeń i zwalczanie złośliwego oprogramowania

Pavel Yosifovich specjalizuje się w technikach i narzędziach stosowanych przez Microsoft. Otrzymał tytuł Microsoft MVP. Programowanie jest jego pasją już od czasu komputerów 8-bitowych.

Alex Ionescu jest niekwestionowanym autorytetem w dziedzinie niskopoziomowego programowania systemów operacyjnych, udoskonalania zabezpieczeń i inżynierii wstecznej.

Mark E. Russinovich jest wybitnym specjalistą w dziedzinie systemów rozproszonych. W Microsoftzie zajmuje się chmurową platformą Azure.

David A. Solomon jest autorem wielu książek o systemie Windows. O jądrze tego systemu operacyjnego wie chyba wszystko. W latach 1993 i 2005 otrzymał tytuł Microsoft MVP.

Helion



helion.pl



HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

Microsoft

KOD KORZYŚCI
Sięgnij po więcej! ▶



ISBN 978-83-8322-554-8



9 788383 225548

Cena: 149,00 zł