

Stručný obsah

Pohled do historie	17
Předmluva	21
Úvod	23
Kapitola 1: Principy a nástroje	27
Kapitola 2: Architektura systému	61
Kapitola 3: Mechanismy systému	109
Kapitola 4: Mechanismy správy	203
Kapitola 5: Spouštění a vypínání	269
Kapitola 6: Procesy, vlákna a úlohy	307
Kapitola 7: Správa paměti	389
Kapitola 8: Bezpečnost	497
Kapitola 9: V/V systém	551
Kapitola 10: Správa úložišť	629
Kapitola 11: Správce mezipaměti	669
Kapitola 12: Souborové systémy	705
Kapitola 13: Práce v síti	805
Kapitola 14: Analýza výpisu paměti při havárii	865
Slovníček pojmů	893
Rejstřík	925

Obsah

Pohled do historie	17
Předmluva	21
Úvod	23
Od autorů	25
Od nakladatelství	26
Od českého vydavatele	26
 Kapitola 1	
Principy a nástroje	27
1.1 Verze operačních systémů Windows	28
1.2 Základní principy a pojmy	29
Rozhraní API systému Windows	29
Služby, funkce a rutiny	30
Procesy, vlákna a úlohy	32
Virtuální paměť	39
Režim jádra versus uživatelský režim	41
Terminálové služby a více relací	46
Objekty a manipulátory	47
Zabezpečení	47

Registr	48
Sada Unicode	49
1.3 Cesta do nitra systému Windows	50
Nástroj Performance (Výkon)	51
Sada Windows Support Tools	52
Sady Windows Resource Kit	52
Ladění jádra	52
Sada Platform Software Development Kit (SDK)	57
Sada Device Driver Kit (DDK)	58
Nástroje sídla Sysinternals	58
1.4 Závěr	59
 Kapitola 2	
Architektura systému	61
2.1 Požadavky a cíle návrhu	62
2.2 Model operačního systému	63
2.3 Přehled architektury	64
Přenositelnost	66
Symetrický multiprocessing	67
Škálovatelnost	72
Rozdíly mezi klientskými a serverovými verzemi	73
Ověřovací sestavení	75
2.4 Klíčové komponenty systému	77
Subsystémy prostředí a knihovny DLL subsystémů	78
Ntdll.dll	87
Výkonná část	88
Jádro	90
Vrstva abstrakce hardwaru	92
Ovladače zařízení	94
Procesy systému	98
2.5 Závěr	108
 Kapitola 3	
Mechanismy systému	109
3.1 Odesílání zachycení	110
Odesílání přerušení	112
Odesílání výjimek	133
Odesílání systémových služeb	142
3.2 Správce objektů	146
Objekty výkonné části	149
Struktura objektů	150
3.3 Synchronizace	171
Synchronizace při vysoké úrovni IRQL	172
Synchronizace při nízké úrovni IRQL	176

3.4 Pracovní vlákna systému	186
3.5 Globální příznaky Windows	188
3.6 Lokální volání procedur	191
3.7 Trasování událostí jádra	194
3.8 Wow64	197
Rozvržení adresového prostoru procesů Wow64	198
Systémová volání	198
Odesílání výjimek	198
Uživatelská zpětná volání	198
Přesměrování systému souborů	199
Přesměrování a zrcadlení registru	199
Požadavky na řízení I/O	200
Aplikace s 16bitovým instalátorem	201
Tisk	201
Omezení	201
3.9 Závěr	201
 Kapitola 4	
Mechanismy správy	203
4.1 Registr	204
Zobrazení a úpravy registru	204
Používání registru	205
Datové typy registru	205
Logická struktura registru	207
Řešení potíží s registrem	212
Vnitřní fungování registru	217
4.2 Služby	232
Aplikace služeb	232
Účty služeb	237
Správce řízení služeb	243
Spouštění služeb	245
Chyby při spouštění	249
Přijetí spuštění a poslední známé dobré verze	250
Selhání služeb	251
Vypnutí služeb	252
Sdílené procesy služeb	253
Programy řízení služeb	255
4.3 Windows Management Instrumentation	256
Architektura WMI	257
Poskytovatelé	258
Společný informační model (CIM) a jazyk formátu spravovaných objektů (MOF)	259
Obor názvů WMI	262
Přiřazování tříd	264
Implementace WMI	265

Zabezpečení WMI	267
4.4 Závěr	268

Kapitola 5

Spouštění a vypínání **269**

5.1 Proces spouštění	270
Počáteční fáze spouštění na x86 a x64	270
Spouštěcí sektor a Ntldr na systémech x86/x64	274
Proces spouštění na architektuře IA64	283
Inicializace jádra a subsystémů výkonné části	284
SMSS, CSRSS a Winlogon	288
Automaticky spouštěné obrazy	291
5.2 Řešení potíží se startem a spouštěním	292
Poslední známá dobrá konfigurace	292
Stav nouze	293
Konzola pro zotavení	297
Řešení obvyklých potíží se spouštěním	299
5.3 Vypnutí	304
5.4 Závěr	306

Kapitola 6

Procesy, vlákna a úlohy **307**

6.1 Vnitřní fungování procesů	308
Datové struktury	308
Proměnné jádra	315
Výkonnostní čítače	315
Příslušné funkce	316
6.2 Tok funkce CreateProcess	318
Fáze 1: Otevření obrazu, který se má vykonat	320
Fáze 2: Tvorba objektu procesu výkonné části Windows	322
Fáze 3: Vytvoření počátečního vlákna a jeho zásobníku a kontextu	326
Fáze 4: Upozornění subsystému Windows na nový proces	327
Fáze 5: Spuštění vykonávání počátečního vlákna	328
Fáze 6: Vykonání inicializace procesu v kontextu nového procesu	328
6.3 Vnitřní fungování vláken	330
Datové struktury	330
Proměnné jádra	337
Výkonnostní čítače	337
Související funkce	338
Zrození vlákna	339
6.4 Průzkum činnosti vláken	339
6.5 Plánování vláken	342
Přehled plánování Windows	342
Úrovně priorit	344

Rozhraní API plánování v systému Windows	346
Příslušné nástroje	347
Priority reálného času	349
Stavy vláken	350
Databáze odesilatele	353
Kvantum	355
Scénáře plánování	359
Přepínání kontextu	362
Nečinné vlákno	362
Zvyšování priority	363
Víceprocesorové systémy	371
Algoritmy plánování vláken na víceprocesorových systémech	380
6.6 Objekty úloh	382
6.7 Závěr	387

Kapitola 7

Správa paměti **389**

7.1 Úvod do správce paměti	390
Součásti správce paměti	390
Interní synchronizace	392
Konfigurování správce paměti	392
Kontrola využití paměti	393
7.2 Služby poskytované správcem paměti	396
Velké a malé stránky	397
Rezervování a svěťování stránek	398
Uzamykání paměti	399
Granularita alokování	400
Sdílená paměť a mapované soubory	400
Chránění paměti	402
Ochrana stránky pomocí zákazu provádění	403
Kopírování při zápisu	407
Správce haldy	408
Rozšíření adresování pomocí okna	413
7.3 Paměťové fondy systému	415
Konfigurování velikostí fondů	416
Sledování využití fondu	419
Vedlejší seznamy	422
Nástroj pro ověřování ovladačů	424
7.4 Členění virtuálního adresového prostoru	428
Rozložení uživatelského adresového prostoru na platformě x86	430
Rozložení systémového adresového prostoru na platformě x86	431
Prostor relace na platformě x86	432
Položky systémové stránkovací tabulky	436
Členění 64bitových adresových prostorů	436

7.5 Překládání adres	437
Překlad virtuálních adres na platformě x86	437
Vedlejší překladová vyrovnávací paměť	448
Rozšíření fyzické adresy (PAE)	449
Překlad virtuálních adres na platformě IA-64	450
Překlad virtuálních adres na platformě x64	451
7.6 Obsluha chyb stránky	452
Neplatné položky PTE	454
Prototypové položky PTE	455
V/V operace při stránkování	456
Kolizní výpadky stránek	457
Stránkovací soubory	458
7.7 Deskriptory virtuální adresy	462
7.8 Objekty úseku	464
7.9 Pracovní sady	470
Stránkování na žádost	471
7.10 Logický systém předběžného načítání	471
Strategie umisťování	475
Řízení pracovní sady	476
Správce vyvážení a vlákno odkládacího mechanismu	479
Pracovní sada systému	480
7.11 Databáze čísel rámců stránek	482
Dynamika seznamů stránek	485
Zapisovač modifikovaných stránek	487
Datová struktura PFN	488
Upozornění při nízkém a vysokém stavu paměti	492
7.12 Závěr	495

Kapitola 8

Bezpečnost

497

8.1 Součásti bezpečnostního systému	501
8.2 Ochrana objektů	505
Kontroly přístupu	506
Bezpečnostní deskriptory a kontrola přístupu	519
8.3 Práva účtu a oprávnění	529
Práva účtu	530
Oprávnění	531
Super oprávnění	537
8.4 Bezpečnostní audit	538
8.5 Přihlášení	541
Inicializace procesu Winlogon	542
Postup přihlašování uživatele	543
8.6 Zásady pro omezení softwaru	547
8.7 Závěr	549

Kapitola 9

V/V systém	551
9.1 Součásti V/V systému	552
Správce V/V	554
Obvyklé zpracování V/V	555
9.2 Ovladače zařízení	556
Druhy ovladačů zařízení	556
Struktura ovladače	562
Objekty ovladače a objekty zařízení	564
Otevírání zařízení	569
9.3 Zpracování vstupu a výstupu	574
Typy V/V	575
Synchronní a asynchronní V/V	575
Pakety V/V požadavků	578
V/V požadavky pro jednovrstvý ovladač	584
V/V požadavky pro vrstvené ovladače	590
Porty ukončení V/V	598
Nástroj pro ověřování ovladačů	602
9.4 Správce Plug and Play (PnP)	603
Úrovně podpory Plug and Play	604
Ovladač a podpora Plug and Play	605
Zavedení, inicializace a instalace ovladače	607
Instalace ovladače	616
9.5 Správce napájení	620
Činnost správce napájení	622
Jak ovladač řídí napájení zařízení	626
9.6 Závěr	626

Kapitola 10

Správa úložišť	629
10.1 Terminologie	630
10.2 Diskové ovladače	630
Zavaděč Ntldr	631
Ovladače třídy disk, port a miniport	631
Ovladače iSCSI	633
Ovladače vícecestného V/V (MPIO)	633
Objekty zařízení typu disk	635
Správce oddílů	636
10.3 Správa svazků	637
Základní disky	638
Dynamické disky	641
Správa víceoddílových svazků	647
Jmenný prostor svazku	653

Přípojně body	654
V/V operace ve svazku	660
Služba virtuálního disku	661
Služba stínové kopie svazku	663
10.4 Závěr	668

Kapitola 11

Správce mezipaměti **669**

11.1 Klíčové vlastnosti správce mezipaměti	670
Jedna centralizovaná mezipaměť systému	670
Správce paměti	671
Soudržnost (koherence) mezipaměti	671
Odkládání virtuálních bloků	673
Odkládání na bázi proudu	673
Podpora zotavitelných souborových systémů	673
11.2 Správa virtuální paměti pro mezipaměť	674
11.3 Velikost mezipaměti	676
LargeSystemCache	677
Virtuální velikost mezipaměti	678
Velikost pracovní sady mezipaměti	679
Fyzická velikost mezipaměti	681
11.4 Datové struktury mezipaměti	683
Celosystémové datové struktury mezipaměti	683
Datové struktury mezipaměti pro jednotlivé soubory	685
11.5 Rozhraní souborového systému	689
Kopírování dat do mezipaměti a nazpět	690
Odkládání do mezipaměti s využitím mapovacího a zachycovacího rozhraní	691
Odkládání do mezipaměti pomocí rozhraní pro přímý přístup do paměti	694
11.6 Rychlý V/V	694
11.7 Dopředné čtení a zápis na pozadí	697
Inteligentní dopředné čtení	697
Zpožděný zápis z mezipaměti a lenivé zapisování	699
Omezení zápisu	702
Systémová vlákna	703
11.8 Závěr	704

Kapitola 12

Souborové systémy **705**

12.1 Formáty souborových systémů Windows	707
CDFS	707
UDF	707
FAT12, FAT16 a FAT32	708
NTFS	711
12.2 Architektura ovladače souborového systému	711

Lokální ovladače FSD	712
Vzdálené ovladače FSD	713
Fungování souborového systému	716
Explicitní souborová V/V operace	717
Ovladače filtru souborového systému	722
12.3 Řešení potíží se souborovým systémem	728
Základní versus pokročilý režim programu Filemon	729
Program Filemon a techniky řešení potíží	729
12.4 Vlastnosti a cíle návrhu systému NTFS	735
Požadavky na špičkový souborový systém	735
Pokročilé vlastnosti systému NTFS	736
12.5 Ovladač souborového systému NTFS	747
12.6 Struktura disku NTFS	749
Svazky	750
Clustery	750
Hlavní souborová tabulka	751
Referenční čísla souborů	757
Souborové záznamy	758
Jména souborů	760
Rezidentní a nerezidentní atributy	763
Komprese dat a řídké soubory	766
Soubor výkazů změn	770
Indexování	771
Identifikátory objektů	773
Sledování kvót	774
Společné zabezpečení	775
Body změny zpracování	777
12.7 Podpora obnovy v systému NTFS	777
Evoluce návrhu souborového systému	778
Protokolování	780
Služba protokolového souboru (LFS)	781
Obnovení	786
Obnova vadných clusterů systémem NTFS	790
12.8 Bezpečnost šifrovacího souborového systému	794
První šifrování souboru	797
Proces dešifrování	802
Zálohování šifrovaných souborů	803
12.9 Závěr	804

Kapitola 13

Práce v síti

805

13.1 Síťová architektura Windows	806
Referenční model OSI	806
Síťové komponenty Windows	807

13.2 Síťová rozhraní API	809
Sokety Windows	810
Vzdálené volání procedury	816
Rozhraní API pro přístup k webu	821
Pojmenovaná propojení a poštovní přihrádky	823
NetBIOS	830
Další síťová rozhraní API	833
13.3 Podpora vícenásobných redirektorů	834
Směrovač pro více síťových prostředí	835
Vícenásobný poskytovatel UNC	838
13.4 Rozklad jmen	839
Systém doménových jmen (DNS)	839
Internetová jmenná služba Windows (WINS)	840
Rozšíření TCP/IP	844
13.5 Ovladače NDIS	847
Variace ovladače miniportu NDIS	852
Ovladače NDIS orientované na spojení	852
Vzdálené rozhraní NDIS	854
QOS	856
13.6 Vazby	857
13.7 Vrstvené síťové služby	858
Vzdálený přístup	859
Služba Active Directory	859
Vyrovnávání zatížení sítě	860
Služba replikování souborů	861
Distribuovaný souborový systém	862
13.8 Závěr	864

Kapitola 14

Analýza výpisu paměti při havárii	865
14.1 Co způsobuje havárie Windows?	866
14.2 Modrá obrazovka	867
14.3 Soubory s výpisem paměti při havárii	870
Generování výpisu paměti při havárii	873
14.4 Hlášení o chybách systému Windows	873
14.5 Přímá analýza havárie	875
14.6 Základní analýza výpisu paměti při havárii	876
Program Notmyfault	876
Základní analýza výpisu paměti při havárii	877
Podrobná analýza	879
14.7 Použití nástrojů pro řešení havárií	881
Přetečení vyrovnávací paměti a speciální fond	881
Přepsání kódu a ochrana systémového kódu před zápisem	884
14.8 Pokročilá analýza výpisu paměti při havárii	886

Poškození zásobníku	886
Zamrzlý nebo nereagující systém	887
Když se žádný výpis při havárii nevytvoří	891
Slovníček pojmů	893
Rejstřík	925

Pohled do historie

Opět jsem vděčný Davidu Solomonovi a Marku Russinovichovi za to, že mi poskytli příležitost napsat několik slov o jejich nejnovějším vydání série knih o vnitřní architektuře Windows (Windows Internals). Poslední kniha vyšla již před třemi lety a za tu dobu se objevily dvě základní věci: podstatná aktualizace klientského systému a další dost důležitá aktualizace serverového systému, která se právě připravuje ke vstupu na trh.

Dva základní problémy, se kterými se autoři této knihy museli vyrovnat, bylo zachytit implementaci vývoje systému Microsoft Windows NT a dokumentovat způsob, kterým zabudování nových rysů ovlivnilo každou verzi. Musím přiznat, že autoři knihy se svého úkolu zhostili velmi dobře a v knize poskytli spoustu příkladů a vysvětlení.

Poprvé jsem se setkal s Davidem Solomonem, když jsem pracoval ve společnosti Digital Equipment Corporation na operačním systému VMS pro VAX; to mu bylo teprve 16. Od té doby se účastnil vývoje operačního systému a školení o vnitřní architektuře operačního systému. S Markem Russinovichem jsem se setkal později, ale o jeho odborných znalostech v oblasti operačních systémů jsem dobře věděl. Podařily se mu úžasné věci, jako například jeho systém NTFS, který pracuje pod Microsoft Win-

dows 98 a jeho „živý“ ladicí program jádra, který lze použít pro nahlížení do spuštěného systému Windows.



(zleva doprava) David Solomon, David Cutler a Mark Russinovich

Windows NT zahájily v říjnu 1988 s cílem vytvořit přenosný systém, který by obsahoval kompatibilitu OS/2, bezpečnost, POSIX, současné zpracování více procesů, integrovanou práci v sítích a spolehlivost. Po příchodu Windows 3.0 a jejich velkém úspěchu se cílem systému stalo obsahovat kompatibilitu Windows přímo a odsunout OS/2 jako subsystém.

Původně jsme si mysleli, že bychom mohli vyprodukovat první systém Windows NT za nějaké dva roky. Nakonec nám to však zabralo čtyři a půl roku a první verze se objevila v létě 1993. Tato verze podporovala procesory Intel i386, Intel i486 a MIPS R400. O šest týdnů později jsme uvedli podporu i pro procesory Alpha Digital.

První verze Windows NT byla větší a pomalejší, než se očekávalo, takže dalším velkým pokrokem byl projekt nazvaný Daytona, pojmenovaný podle dálnice na Floridě. Hlavním cílem této verze bylo zredukovat velikost systému, zvýšit rychlost systému a samozřejmě také zvýšit spolehlivost. Za šest měsíců po uvolnění Windows NT 3.5 na podzim 1994 jsme uvedli Windows NT 3.51, aktualizovanou verzi obsahující podporu pro procesory IBM PowerPC.

Cílem pro další verzi Windows NT bylo aktualizovat uživatelské rozhraní tak, aby bylo kompatibilní s Windows 95 a aby v něm byly začleněny technologie Cairo, které se už ve firmě Microsoft několik let vyvíjely. Vývoj tohoto systému trval další dva roky a byl uveden na trh v létě 1996 jako Windows NT 4.0.

Následující verze NT byla přejmenována na Windows 2000 a byla posledním systémem, pro který byly systémy klienta i serveru uvedeny současně. Tato verze byla vyvíjena na stejné technologii Windows NT jako verze předchozí a měla některé významné nové rysy, jako například aktivní adresář. Vyprodukovat Windows 2000 trvalo tři a půl roku a byla to verze Windows NT, která byla v té době nejvíce testovaná a vyladovaná. Windows 2000 byly kulminací jedenácti roků vývoje a implementací čtyř různých architektur.

Ke konci vývoje Windows 2000 jsme zahájili ambiciózní plán implementovat nové verze klientského a serverového systému, které by obsahovaly nové vylepšené zákaznické rysy a zlepšily schopnosti serveru. Při práci na těchto plánech vyplynulo zcela jasně, že implementace těchto serverových rysů by způsobila zpoždění v implementaci klientských rysů, a proto se uvedení těchto systémů rozdělilo. V srpnu 2002 byla uvedena verze Windows XP Professional a Windows XP Home Edition a o rok později, v březnu 2003 byla uvedena verze Microsoft Windows Server 2003. Kromě architektury Intel x86 obsahovaly tyto systémy také podporu pro Intel IA-64, čímž se Windows NT poprvé posunuly k 64bitovému zpracovávání.

Tato kniha je konečnou prací o vnitřních strukturách a práci Windows XP a Windows Server 2003. Mimo to však také nabízí pohled do budoucnosti Windows – k posunu do 64bitového zpracovávání tím, že se věnuje architektuře x64 (AMD64) uvedené v roce 2003 a ohlašované podpoře Intelu (EM64T) v únoru 2004. Verze klienta i serveru plně podporující x64 se plánuje na první polovinu roku 2005 a tato kniha obsahuje mnoho zajímavých pohledů do detailů jeho implementace.

Architektura x64 je počátkem nové éry pro Windows NT v době, kdy architektura x86 už jeví známky stárnutí. Tato architektura nabízí kompatibilitu 32bitové x86 při rychlosti takové, aby chránila starší investice do softwaru, a poskytuje schopnosti 64bitového adresování pro ty nejnovější aplikace. Tím se ochrání investice do 32bitového softwaru, ale zároveň dostanou Windows NT zbrusu nový rys, který jim pomůže přežít v dalším desetiletí i potom.

Ačkoli systém Windows NT prošel za posledních pár let několika změnami, zůstává zcela založen na základně kódu Windows NT. S tím, jak šel čas a vynalézaly se stále nové a nové věci, změnila se implementace mnoha vnitřních rysů dost zásadně. Autoři odvedli výbornou práci, když asimilovali detaily z kódové základny Windows NT a jejich různé implementace od verze k verzi a od platformy k platformě a při výběru příkladů a nástrojů, které čtenářům umožní pochopit, jak to všechno pracuje. Každý vývojář operačních systémů, který svou práci bere vážně, by měl tuto knihu mít na stole.

David N. Cutler
samostatný programátor
Microsoft Corporation

Předmluva

Microsoft Windows stály v centru mého života celých posledních 14 let. V tuto dobu se operační systém od verze k verzi neustále vyvíjel do šířky i do hloubky. Vývoj Windows je v dnešním světě jedním z nejdůležitějších a nejkompexnějších projektů. Na vývoji Windows pracuje kolem 5 000 inženýrů. V téměř všech kulturách tvoří uživatelé Windows celé spektrum od těch nejdůležitějších průmyslových odvětví až po ty nejmenší děti. Uživatelé Windows vyžadují neustálá vylepšení v téměř každém ohledu – od schopnosti zvládat ty největší servery až po schopnost být tak jednoduché, aby je mohly používat i předškolní děti. Windows zahrnují verze mnoha tvarů a velikostí, od zapouzdřených verzí až po správu datových center. Všechny tyto produkty používají stejné vnitřní struktury jádra Windows, které se vyvíjejí a vylepšují s každou novou verzí.

Toto je ta nejuplněnější kniha o vnitřní architektuře jádra Windows. Chcete-li se dozvědět, jak Windows pracují uvnitř, a to co nejrychleji, pak je tato kniha pro vás. Snažit se pochopit, jak všechny součásti tak obrovského produktu fungují, je nadmíru těžký úkol. Ale když začnete u koncepcí jádra systému a odsud budete postupovat dále, je ta skládačka mnohem jednodušší. Stejně tak jak se vyvíjely Windows samotné, vyvíjela se i povaha této knihy, která vychází již ve čtvrtém vydání. Celá léta jsme užívali dřívější vydání této knihy ke školení nových zaměstnanců firmy Microsoft, takže tento materiál je opravdu vyzkoušený a funguje.

Pokud jste jako já, rádi zjišťujete, jak věci fungují. Mně osobně nikdy nestačily knihy, které jen popisují, jak něco pracuje, nebo nabízejí „tipy a triky“. Když pochopíte,

jak něco pracuje uvnitř, víte, jak to lépe používat, umíte zlepšit výkon a bezpečnost, dokážete odhalit příčiny selhání a taky je to mnohem zábavnější. Pokud jste jako já a chcete vidět Windows „svlečené z kůže“, pak jste na správném místě.

Dave a Mark odvedli při podrobném popisu detailů vnitřní struktury Windows výbornou práci. Nástroje, které popisují, jsou skvělým zdrojem pro práci při výuce i diagnostikování. Až si tuhle knihu přečtete, budete mnohem lépe rozumět tomu, jak zapadají operační systémy dohromady, jaká jsou v systému nejnovější vylepšení a jak z nich získat co nejvíc.

Ta cesta byla dlouhá – a ještě stále pokračuje. Tak se dejte do čtení a ponořte se do hlubin jednoho z nejúžasnějších operačních systémů, který byl kdy vytvořen.

Jim Allchin
viceprezident, Platforms
Microsoft Corporation

Úvod

Kniha *Vnitřní architektura Microsoft Windows*, jež je překladem čtvrtého vydání anglického originálu *Microsoft Windows Internals*, je určena pokročilým počítačovým profesionálům (vývojářům i správcům systémů), kteří chtějí pochopit, jak pracují vnitřní součásti jádra operačních systémů Microsoft Windows 2000, Windows XP a Microsoft Windows Server 2003. S těmito znalostmi mohou vývojáři lépe rozumět důvodům pro konkrétní rozhodnutí při výstavbě aplikací pro platformu Windows. Tyto znalosti mohou také vývojářům pomoci řešit komplexní problémy. Správci systémů mohou tyto informace využít také, protože když pochopí, jak operační systém funguje „uvnitř“, bude jim jasnější chování a výkonnost systému a snadněji se jim budou hledat příčiny problémů. Jestliže si tuto knihu přečtete, lépe pochopíte, jak Windows fungují a proč se chovají tak, jak se chovají.

Struktura knihy

První dvě kapitoly (Principy a nástroje a Architektura systému) pokládají základy vysvětlením pojmů a popisem principů, které se vyskytují v celé knize. Následující tři kapitoly – Mechanismy systému, Mechanismy správy a Spouštění a vypínání – popisují klíčové základní mechanismy systému. Další osm kapitol vysvětluje komponenty jádra operačního systému. Poslední kapitola se týká analýzy výpisu paměti při havárii.

Historie knihy

Toto je čtvrté vydání knihy, která se původně jmenovala *Inside Windows NT* (Microsoft Press, 1992) a napsala ji Helen Custerová (ještě před prvním vydáním Microsoft Windows NT 3.1). *Inside Windows NT* byla první knihou publikovanou o Windows NT a poskytovala základní vhled do architektury a návrhu systému. Druhé vydání této knihy (Microsoft Press 1998) napsal David Solomon a v českém překladu ji vydal Computer Press pod názvem *Windows NT pro administrátory a vývojáře*. Bylo aktualizováno, aby obsahovalo Windows NT 4.0 a bylo mnohem podrobnější. *Inside Windows 2000*, třetí vydání (Microsoft Press 2000) napsali David Solomon a Mark Russinovich. Obsahovalo nová témata, jako spouštění a vypínání, vnitřní architekturu služeb, vnitřní architekturu registru, ovladače systému souborů a práci v síti a změny jádra ve Windows 2000, jako třeba Windows Driver Model (WDM), Plug and Play, správu napájení, Windows Management Instrumentation (WMI), šifrování, objekty úloh a terminálové služby.

Změny ve čtvrtém vydání

Toto poslední, čtvrté vydání, nyní v originále nazvané *Microsoft Windows Internals* bylo aktualizováno tak, aby obsahovalo změny jádra učiněné ve Windows XP a Windows Server 2003, včetně podpory 64bitového systému. Byla aktualizována část experimentů tak, aby odrážela změny v nástrojích a byly dodány nové experimenty, jež využívají nových nástrojů, které nebyly ještě k dispozici v době třetího vydání.

Jelikož úroveň změn jádra od Windows 2000 do těchto verzí byla relativně malá (ve srovnání se změnami mezi Windows NT 4.0 a Windows 2000), velká většina tohoto textu je platná pro Windows 2000, Windows XP a Windows Server 2003. Proto pokud není specifikováno jinak, všechno platí pro všechny tyto tři verze.

Experimenty

I bez přístupu ke zdrojovému kódu se dá dozvědět hodně o vnitřní struktuře Windows z nástrojů, které máme k dispozici, jako například debugger jádra. Když je možné použít nějaký nástroj pro odhalení nebo demonstrování nějakých aspektů chování vnitřních struktur Windows, jsou kroky pro vyzkoušení nástroje popsány v odstavečcích nazvaných Experimenty. Ty se vyskytují po celé knize a my vám doporučujeme si je vyzkoušet při četbě knihy – viditelné důkazy toho, jak Windows uvnitř fungují, vám přiblíží celou problematiku názorněji než jen četba.

Témata, kterými se nezabýváme

Windows jsou obrovský a složitý operační systém. Tato kniha nepokrývá všechno důležité pro vnitřní strukturu Windows, ale místo toho se soustředí na komponenty základny systému. Například zde nepopisujeme COM+, infrastrukturu objektově orientovaného programování Windows, ani .NET Frameworking, základnu další generace aplikací s řízeným kódem.

Protože toto je kniha o vnitřní struktuře, nejedná se o uživatelskou příručku nebo příručku pro správce, nepopisuje, jak Windows používat, konfigurovat nebo v nich programovat.

Varování a upozornění

Protože tato kniha popisuje nedokumentované chování vnitřní architektury a činnost operačního systému Windows (např. vnitřní struktury jádra a funkce), podléhá tento obsah změnám ve verzích. (Externí rozhraní, jako například Windows API, nepodléhají nekompatibilním změnám.)

„Podléhání změnám“ nemusí znamenat, že detaily popsané v knize budou u různých verzí jiné, ale nelze se spoléhat na to, že se měnit vůbec nebudou. Jakýkoli software, který pracuje na těchto nedokumentovaných rozhraních, nemusí nutně pracovat v budoucích verzích Windows. A co je ještě horší, software, který běží v režimu jádra (jako ovladače zařízení) a používá nedokumentovaná rozhraní, může zkolabovat, když jej spustíte na novější verzi Windows.

Podpora

Všechny informace v této knize by měly být přesné. Kdybyste přece jen narazili na problém, obraťte se na zdroje, které uvádíme dále.

Od autorů

Tato kniha není dokonalá. Bezpochyby se v ní nalézají nějaké nepřesnosti, nebo jsme možná vynechali nějaká témata, kterými jsme se zabývat měli. Pokud najdete něco, o čem si myslíte, že je to nesprávné, nebo si myslíte, že by zde měl být materiál, který tu není, neváhejte a napište nám na windowsinternals@systinternals.com. Aktualizace a opravy budou k dispozici na stránce www.sysinternals.com/windowsinternals.

Od nakladatelství

Microsoft také poskytuje opravy pro knihy na Internetu na následující adrese:

<http://www.microsoft.com/learning/support>

Pro připojení přímo ke službě Microsoft Learning Knowledge Base a pro zadání dotazu týkajícího se problému, se kterým jste se setkali, si najděte

<http://www.microsoft.com/learning/support/search.asp>.

Kromě toho, že zašlete reakce a poznámky přímo autorům, můžete také svůj komentář, dotazy nebo nápady týkající se prezentace nebo používání této knihy zaslat do nakladatelství Microsoft:

poštovní adresa:
Microsoft Press
Attn.: Windows Internals Editors
One Microsoft Way
Redmond, WA 98052-6399
e-mail:
mspinput@microsoft.com

Podpora produktu se na výše zmíněných adresách neposkytuje. Informace týkající se podpory Microsoft Windows naleznete na stránkách www.microsoft.com/windows. Můžete také využít telefonické služby standardní podpory na čísle (425) 635-7011 ve všední dny od 6 do 18 hodin (tichomořského času) nebo podpory online na support.microsoft.com/support.

Od českého vydavatele

Také nakladatelství Computer Press, které pro vás tuto knihu přeložilo, stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

Computer Press
redakce počítačové literatury
náměstí 28. dubna 48
635 00 Brno-Bystrc
nebo
knihy@cpres.cz.

Další informace a případné opravy českého vydání knihy najdete v budoucnu na adrese <http://knihy.cpress.cz/k1190>. Prostřednictvím uvedené adresy můžete též naší redakci zaslat komentář nebo dotaz týkající se knihy. Na vaše reakce se srdečně těšíme.