Stručný obsah

Obsah

KAPITOLA 2

Architektura rodiny operačních systémů Windows NT 45

OKAPITOLA 3

Vývoj ovladačů jádra 65

KAPITOLA 4

Synchronizace 113

KAPITOLA 5

Výjimky, přerušení a systémová volání 147

KAPITOLA 7

Procesy a vlákna 259

KAPITOLA 8

Správce vstupně/výstupních operací 305

KAPITOLA 9

Správa paměti 327

Úvod

Tato kniha v jedenácti kapitolách pojednává o různých aspektech jádra operačních systémů rodiny Windows NT. Neklade si však za cíl toto téma zpracovat do nejmenších podrobností; spíše se čtenáři snaží vštípit základní informace a obohatit jej o některé zajímavosti, na něž může při průzkumu jádra narazit.

Kniha se snaží postupy a algoritmy používané v jádře Windows uvést do širších souvislostí teorie operačních systémů. Z tohoto důvodu jsou některé kapitoly rozděleny na dvě části – první se věnuje dané problematice (například synchronizaci či správě paměti) obecně a druhá ukazuje, jaké poznatky a algoritmy se vývojáři a návrháři jádra Windows rozhodli použít. Tímto uspořádáním se kniha snaží ukázat, že mnohé postupy si Microsoft nevymyslel na „zelené louce", ale vychází z teoreticky podložených faktů. Varianty některých zde popsaných algoritmů se nacházejí i v jádrech jiných operačních systémů, například těch založených na Unixu.

Dalším a posledním cílem knihy je naučit čtenáře (pokud bude chtít) pohybovat se v jádře a samostatně zkoumat jeho vnitřní mechanismy a zákonitosti. Z tohoto důvodu kniha zahrnuje i popis v tomto ohledu užitečných nástrojů a snaží se poskytnout neformální základy programování ovladačů. Za tímto účelem spolu s touto publikací vzniká webová stránka *http://www.jadro-windows.cz*, na které naleznete okomentované zdrojové kódy ovladačů jádra, jež prakticky ukazují některé aspekty probírané v jednotlivých kapitolách. Na části těchto zdrojových kódů narazíte i v textu knihy formou výpisů. Dále na zmíněném webu naleznete materiály vhodné pro další rozšiřování znalostí a užitečné nástroje.

Zdrojové kódy projektů

Konkrétně na webové stránce *jadro-windows.cz* naleznete zdrojové kódy následujících projektů:

- **Dllhide** – program demonstruje, jak lze manipulací s interními datovými strukturami procesu skrýt knihovny DLL, které používá.
- **Drv** – tento program na základě argumentů příkazového řádku dokáže načítat a odstraňovat ovladače jádra. Ukazuje, jak tyto operace provádět různými způsoby.
- **Filemaptest** – ukazuje, jakým způsobem je možné využít sdílené paměti vytvořené pomocí paměťově mapovaného souboru a přenášet data mezi dvěma procesy.
- **Hello** – velmi jednoduchý ovladač, který pouze vypíše několik oznámení do debuggeru jádra. Ačkoliv neprovádí prakticky žádné operace, jeho zdrojový kód ukazuje, co musí každý ovladač minimálně umět.
- **Intcount** – ovladač a aplikace, které si kladou za cíl zjistit statistiku vykonávání jednotlivých přerušení. Cílem této ukázky je demonstrovat práci s tabulkou vektorů přerušení a synchronizaci více procesorů.
- **Keyedevent** – jádro Windows implementuje zajímavá synchronizační primitiva, která jsou v této knize označována jako události na klíč (keyed events). Ačkoliv je mohou používat i normální aplikace, příslušné rozhraní není dokumentováno. Projekt `keyedevent` práci s tímto rozhraním zjednodušuje a dokumentuje jej.

- **Listdll** – tento program tvoří protipól k projektu `dllhide`. Na základě argumentů příkazového řádku se snaží zjistit seznam knihoven DLL používaných cílovým procesem. Ukazuje různé způsoby, jak tyto informace zjistit.
- **Logptm** – projekt ukazuje, jak pomocí relativně jednoduchého ovladače jádra monitorovat spouštění a ukončování procesů a vláken a načítání knihoven DLL a dalších spustitelných souborů do paměti. Ovladač k tomuto účelu využívá velmi staré a dokumentované rozhraní.
- **Ntqueryobject** – jednoduchý program, který demonstruje použití nativní funkce `NtQueryObject` ke zjištění různých zajímavých informací.
- **Obinit** – tento projekt ukazuje, jak pomocí techniky DKOH (Direct Kernel Object Hooking) monitorovat přístupy k různým objektům operačního systému (souborům, klíčům registru, procesům, vláknům a dalším).
- **Objview** – projekt, který ukazuje, jakým způsobem je možné implementovat funkce, kterými disponuje utilita `WinObj` ze serveru *www.sysinternals.com*. Jedná se o prohlížeč pojmenovaných objektů existujících v jádře operačního systému.
- **Pproc** – Windows Vista mimo jiné zavádí nový druh procesů – tzv. *chráněné procesy* (protected processes). Cílem projektu `pproc` je umožnit vám libovolný proces označit jako chráněný a opačně. Dále projekt také obsahuje testovací program, který prakticky demonstruje, jaké možnosti a omezení chráněné procesy s sebou přináší.
- **Registrymon** – projekt ukazuje, jak implementovat funkcionalitu podobnou aplikaci `Regmon`, kterou jste mohli dříve nalézt na serveru *www.sysinternals.com*, tedy monitorování operací nad Registrem Windows.
- **SSDTInfo** – systémová volání patří k jednomu z nejdůležitějších mechanismů ve Windows. Projekt `SSDTInfo` ukazuje, jak zjistit zajímavé informace o interních datových strukturách, které implementace tohoto mechanismu používá.
- **Syscallmon** – projekt ukazuje, jakým způsobem lze monitorovat systémová volání.
- **Vad** – bloky alokované a rezervované paměti procesu reprezentuje jádro Windows pomocí struktur VAD (Virtual Address Descriptor). Projekt `vad` demonstruje, jak s těmito strukturami pracovat a získat z nich užitečné informace.

Všechny zdrojové kódy jsou psány v programovacích jazycích C a Object Pascal a vývojových prostředích Delphi XE 2010 a Microsoft Visual Studio. Jednotlivé programy a ovladače, až na výjimky, fungují na 32bitových i 64bitových verzích Windows XP, Windows Server 2003, Windows Vista a Windows 7. Delphi je použito převážně z důvodu snadné tvorby grafického uživatelského rozhraní.

Co v knize najdete

První tři kapitoly knihy tvoří úvod do problematiky operačních systémů rodiny Windows NT. První kapitola nejprve vysvětluje základní pojmy, jako je proces, vlákno, systémové volání či handle. Dále pokračuje stručným popisem jednotlivých verzí Windows; od Windows 1 až po současná Windows 7. Ve své třetí části kapitola popisuje základní datové struktury, mezi které patří pole, spojový seznam, fronta či zásobník a které jádra operačních systémů často využívají k uchovávání různých informací.

Druhá kapitola již trochu sestupuje z teoretických výšin kapitoly první a obecně pojednává o jednotlivých částech jádra Windows a dalších komponentách, bez kterých by operační systém nefungoval. Dočtete se v ní také o službách – programech (a ovladačích), jejichž posláním je vykonávat důležité činnosti na pozadí.

Třetí kapitola popisuje některé postupy a principy programování ovladačů jádra. Dozvíte se, jaké nástroje potřebujete a jak ovladač načíst do paměti jádra. V závěrečné části je popsána struktura ovladače `logptm.sys`. Kapitola se informace snaží podávat méně formálním způsobem; kterým se autor této knihy učil poznávat zákoutí jádra Windows.

Další kapitoly se již věnují jednotlivým aspektům operačního systému, i když u některých nechybí obecný úvod. Ve čtvrté kapitole se dočtete o způsobech řízení přístupu více aplikací (vláken) ke sdíleným prostředkům. Pátá kapitola popisuje mechanismy obsluhy přerušení, odloženého volání procedur a systémových volání. Následující kapitola pojednává o tom, jak jádro Windows využívá principů objektově orientovaného programování.

Sedmá kapitola se věnuje procesům, vláknům a jejich plánování. V osmé se dočtete o způsobech předávání dat mezi aplikací a ovladačem a mezi ovladači navzájem. Jedná se o rozšíření poznatků neformálně sdělených ve třetí kapitole. Devátá kapitola se zabývá správou paměti. Popisuje jak různé operace s virtuální pamětí, které jádro Windows podporuje, tak dává lehce nahlédnout i do interních datových struktur, které správce paměti používá.

Desátá a jedenáctá kapitola popisují formáty, které Windows používají pro ukládání dat na externí média, například pevné disky. Desátá kapitola se věnuje Registru, struktuře určené ukládání nastavení aplikací a celého operačního systému. Popisuje tento formát z hlediska programátora a uživatele. Její podstatná část pojednává i o tom, jak je tato „databáze“ fyzicky uložena na pevném disku. Jedenáctá kapitola popisuje interní datové struktury dvou na Windows nejrozšířenějších souborových systémů – FAT a NTFS.

Zpětná vazba od čtenářů

Nakladatelství a vydavatelství Computer Press stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

redakce PC literatury
Computer Press
Spielberk Office Centre
Holandská 3
639 00 Brno

nebo

sefredaktor.pc@cpress.cz

Zdrojové kódy ke knize

Z adresy *http://knihy.cpress.cz/K1741* si po klepnutí na odkaz Soubory ke stažení můžete přímo stáhnout archiv s ukázkovými kódy.

Errata

Přestože jsme udělali maximum pro to, abychom zajistili přesnost a správnost obsahu, chybám se úplně vyhnout nelze. Pokud v některé z našich knih najdete chybu, ať už v textu nebo v kódu, budeme rádi, pokud nám ji nahlásíte. Ostatní uživatele tak můžete ušetřit frustrace a pomoci nám zlepšit následující vydání této knihy.

Veškerá existující errata zobrazíte na adrese *http://knihy.cpress.cz/K1741* po klepnutí na odkaz Soubory ke stažení.