Devid Espenschied

Systemprogrammierung mit Delphi

Hardwarezugriff über Windows-API und Windows-Kernelmodus-Treiber

Springer Vieweg

Systemprogrammierung mit Delphi

Devid Espenschied

Systemprogrammierung mit Delphi

Hardwarezugriff über Windows-API und Windows-Kernelmodus-Treiber

Springer Vieweg

Devid Espenschied
Berlin, Deutschland

ISBN 978-3-658-43454-0 ISBN 978-3-658-43455-7 (eBook)
https://doi.org/10.1007/978-3-658-43455-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Planung/Lektorat: David Imgrund
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Das Papier dieses Produkts ist recycelbar.

Vorwort

Liebe Leserinnen und Leser,

der Begriff Systemprogrammierung tauchte bereits vor mehreren Jahrzehnten unter dem Gesamtbegriff der Softwareentwicklung auf und beschreibt eine software- und hardwarenahe Entwicklung, die als systemnah bezeichnet werden kann. Auch wenn diese Thematik viel Wissen über die Hardware und deren Schnittstellen erfordert, wird man früher oder später damit konfrontiert – spätestens dann, wenn eine Windows API-Funktion benötigt wird (von denen wirklich sehr viele existieren). Embarcadero's Delphi bietet hierfür eine gute bis sehr gute API-Integration und liefert entsprechende Object Pascal-Implementierungen mit, die man leicht nutzen kann. Die dazugehörige Dokumentation stammt gleichzeitig von Microsoft's sehr umfangreichen Internet-Dokumentationsseiten.

Meine Motivation für dieses Buch ist tatsächlich die über 30jährige Erfahrung in diesem Bereich (damals noch unter DOS) und die Faszination, Hardware direkt mit Software anzusprechen – auf einer der untersten möglichen Zugriffsebenen. Gleichzeitig gab es den Wunsch, diese Art und Weise der Entwicklung dem Leser über verständliche Didaktik zu vermitteln. Ich habe mich bemüht, einige der häufig als trocken und extrem techniklastig bezeichneten Themenblöcke transparent mit flüssigem Schreibstil darzustellen und hoffe, dass mit diesem Wissen und der gleichzeitig entwickelten Beispielapplikation *PC Analyser* eine praxisnahe Umsetzung als Bereicherung für eigene Aufgaben und Projekte ermöglicht wird.

Trotzdem ist mir natürlich bewusst, dass der IT-Markt rasant fortschreitet und die mit diesem Buch aktuelle Speichertechnologie DDR5 bspw. bald durch eine neue Generation ersetzt wird. Deswegen könnte ich einer möglichen Neuauflage in ein paar Jahren sehr wahrscheinlich nicht abgeneigt sein.

Einen großen Dank möchte ich an Matthias Eißing von Embarcadero Deutschland richten, der mir viele Fragen beantwortet und mit seinem Wissen dieses Buch abgerundet hat, sowie eine unterstützende Hilfe während des Schreibprozesses war. Leider hat er die Veröffentlichung nicht mehr erleben dürfen, da er am 14. Februar 2024 plötzlich und unerwartet im Alter von 53 Jahren von uns gegangen ist. Herr Eißing war seit 1997 für Borland/Inprise/CodeGear/Embarcadero tätig und hat Delphi seit Version 1 begleitet.

Dass sein Todestag auf den Valentinstag und damit auf den 29. Geburtstag von Delphi fiel, ist bezeichnend, denn sein Wissen über Delphi hat ihm in der Delphi-Community den Status einer Legende eingebracht.

Für dieses Buch sind Ihre Meinung und Feedback sehr wichtig, weil es mir hilft, neue Auflagen entsprechend noch kundenorientierter zu verfassen. Für eine Kommunikation schreiben Sie mir daher gerne an meine E-Mail-Adresse:

d.espe@gmx.de

und besuchen Sie auch gerne meine Homepage, auf der ich weitere Details zum Buch zusammengestellt habe:

www.pcanalyser.de

Den Quellcode für die begleitende Beispielapplikation ist in meinem GitHub-Repository verfügbar:

https://github.com/DevidEspe/PCAnalyser

Und abschließend folgen einige wenige und wahrscheinlich die einzigen emotionalen Worte in diesem Buch. Dieses Buch widme ich meiner Tochter Catharina als Dank für alles, was ich mit ihr bisher erleben durfte und mich noch möglichst viele Jahre meines Lebens begleiten wird. Du bedeutest mir alles.

Berlin Devid Espenschied
im Juni 2024

Inhaltsverzeichnis

Teil IV Hardwarezugriffe über den Kernelmodus-Treiber

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung (Beschreibung)
ACE	Access Control Entry (Eintrag einer Tabelle, der den Zugriff auf ein Objekt kontrolliert oder überwacht und Bestandteil der ACL ist)
ACL	Access Control List (Tabelle, die Windows mitteilt, welche Zugriffsrechte jeder Anwender auf bestimmte Systemobjekte hat)
ACPI	Advanced Configuration and Power Interface (Industriestandard und Schnittstelle für Energieverwaltung)
ADK	Assessment and Deployment Kit (Paketsammlung von Microsoft, um Windows automatisch installieren zu lassen)
AGP	Accelerated Graphics Port (Anschlussnorm auf Hauptplatinen zur direkten Verbindung zwischen Grafikkarte und dem Chipsatz bzw. dessen Northbridge)
ANSI	American National Standards Institute (Private, gemeinnützige und amerikanische Organisation zur Koordinierung der Entwicklung freiwilliger Normen in den Vereinigten Staaten. Der Sitz der Non-Profit-Organisation ist Washington, D.C.)
API	Application Programming Interface (Synonym für eine beliebige Programmierschnittstelle)
APIC	Advanced Programmable Interrupt Controller (Kontroller für die Verteilung von Interrupts)
BCD	Boot Configuration Data (Firmware-unabhängige Datenbank für Konfigurationsdaten, die während des Bootens benötigt werden. Sie ersetzt die Datei „boot.ini“, die ursprünglich vom NT-Loader genutzt wurde)
BIOS	Basic Input/Output System (Firmware für PCs, die während des Kaltstarts die Hardware konfiguriert, über eine GUI die Konfiguration ermöglicht und die Kontrolle ans Betriebssystem abgibt)
BIST	Built In Self Test (Gerätespezifischer Selbsttest, der nach der PCI-Spezifikation ausgelöst und ausgewertet werden kann, wenn das PCI-Gerät diesen Test unterstützt)

BKGD	BIOS and Kernel Developer's Guide (AMD-Dokumentation mit enthaltenen CPUID-Funktionen und Modell-spezifischen Registern (MSR))
CAS	Column Address Strobe (Speicherlatenz die benötigt wird, um eine Spalte im Hauptspeicher des Rechners zu adressieren)
CSIDL	Constant Special Item ID List (Vordefinierte Konstanten für die Ermittlung spezieller Ordner (etwa mit unterschiedlichen Namen und Speicherorten auf unterschiedlichen Systemen))
CPU	Central Processing Unit (Allgemeine Bezeichnung für den Zentralprozessor)
CPUID	Central Processing Unit Identification (Prozessorbefehl zur Ermittlung von Prozessoren mit vielen seiner Eigenschaften)
DDK	Driver Development Kit (Toolsammlung von Microsoft, die eine Entwicklung von Gerätetreibern für die Windows-Plattform ermöglicht. Die Sammlung umfasst Dokumentationen, Beispiele, Build-Umgebungen und Tools für Treiberentwickler)
DDR5	Double Data Rate 5 (Speichertechnologie in der 5. Generation, die im Vergleich zu DDR4 weniger Strom verbraucht und die Bandbreite erhöht)
DIMM	Dual Inline Memory Module (Doppelreihiges Speichermodul, das auf beiden Seiten Signale und Speicherbausteine enthält)
DMI	Desktop Management Interface (Standardverfahren zur Erkennung und Verwaltung von Rechnerkomponenten, das von der Distributed Management Task Force (DMTF) entwickelt wurde)
DMTF	Distributed Management Task Force (Normungsorganisation von Unternehmen der IT-Industrie, der eine Vielzahl von namhaften Unternehmen angehören)
DTS	Digital Thermal Sensor (Digitaler Temperatursensor auf einem Intel Prozessor-Chip, der eine Überwachung ermöglicht. Damit lässt sich erkennen, wie nah das System an der Temperaturgrenze ist, ohne zerstörerische Tests durchzuführen)
ECC	Error Correcting Code (Methode zur Erkennung von Hauptspeicherfehlern, wobei ein Hashwert über die 64 Bits einer Speicherzelle berechnet und in zusätzlichen Bits abgelegt wird)
EMS	Emergency Management Services (Dienstleistungen, die im Zusammenhang mit dem Katastrophenschutz stehen)
GPU	Graphics Processing Unit (Grafikprozessor mit Nutzung von Grafikspeicher und Bildschirmausgabe)
GUID	Globally Unique Identifier (Eindeutiger 16 Byte-Zahlenwert (128 Bit) zur Identifizierung in Computersystemen)
HKCU	HKEY Current User (Windows-Registrierungsschlüssel mit benutzerspezifischen Inhalten)

HKLM	HKEY Local Machine (Windows-Registrierungsschlüssel mit maschinenspezifischen Inhalten)
HWCR	Hardware Configuration Register (Weit verbreitetes AMD MSR mit allgemeinen Details zur Hardware-Konfiguration)
IOCTL	Input/Output Control (Systemaufruf für gerätespezifische Ein- und Ausgabeoperationen)
IRP	I/O Request Package (Kernelmodusstrukturen, die vom Windows-Treibermodell und von Windows NT-basierten Gerätetreibern verwendet werden, um miteinander und mit dem Betriebssystem zu kommunizieren)
KMDF	Kernel-Mode Driver Framework (Microsoft Treiber-Framework, um Treiberentwicklern beim Erstellen und Verwalten von Gerätetreibern im Kernelmodus für Windows 2000 und höher zu helfen)
MDL	Memory Descriptor List (I/O-Puffer, der sich über einen Bereich zusammenhängender virtueller Speicheradressen erstreckt, und über mehrere physische Seiten verteilt sein kann, die nicht zusammenhängend sein müssen. Das Betriebssystem verwendet eine MDL, um das physische Seitenlayout für einen virtuellen Speicherpuffer zu beschreiben)
MMX	Multi Media Extension (Von Intel in 1997 entwickelte Erweiterung des Prozessor-Befehlssatzes)
MSR	Model-specific Register (Modell-spezifische Prozessorregister, die auf Kernel-Ebene des Betriebssystems ausgeführt werden und weitreichende Details liefern bzw. Einstellungen ermöglichen)
Mutex	Mutual Exclusion Object (Methode für die Synchronisierung von Datenzugriffen zwischen mehreren Prozessen)
NDA	Non-Disclosure Agreement (Vertraulichkeitsvereinbarung, die Hersteller mit Geschäftspartnern abschließen, um vertraulichen Informationsfluss zu steuern)
PCH	Platform Controller Hub (Intel-Bezeichnung für Chipsätze und die Anbindung zwischen Northbridge und Southbridge an das System)
PCI	Peripheral Component Interconnect (Bus-Standard zur Verbindung von Peripheriegeräten mit dem Chipsatz eines Prozessors – es existieren zahlreiche Varianten und Einsatzgebiete des Standards)
PEC	Packet Error Checking (Gepackter Fehlercode, der an das Ende einer Transaktion angehangen und berechnet wird)
POST	Power On-Self Test (Initialisierungsprozess des BIOS, bei dem die Hardware angesteuert und konfiguriert wird, und dem Betriebssystem bzw. dem dazugehörigen Bootloader die Kontrolle übergeben wird)
PPR	Processor Programming Reference (AMD-Dokumentation mit enthaltenen CPUID-Funktionen und Modell-spezifischen Registern (MSR))

PSIG	PCI Special Interest Group (Konsortium der Elektronikindustrie, das für die Spezifizierung der Peripheral Component Interconnect-, PCI-X- und PCI Express-Computerbusse verantwortlich ist. Es hat seinen Sitz in Beaverton, Oregon)
SBA	SMB Base Address (SMBus-Basisadresse, die aus dem Konfigurationsbereich des PCI-Gerätes für den SMBus-Kontroller gewonnen wird und die Basis für die SMBus-Kommunikation (inkl. der Ermittlung von Speichermodulen über SPD EEPROM) darstellt)
SDK	Software Development Kit (Toolsammlung von Microsoft, die Dokumentationen, Headerdateien, Kompiler, Programmbibliotheken, Beispiele und Programmierwerkzeuge für die Entwicklung von Microsoft Windows und dem .NET-Framework enthält)
SDRAM	Synchronous Dynamic Random Access Memory (Halbleiterbasierte Speichervariante, bei der sich der Speicher mit dem Systemtakt des PCs synchronisiert)
SID	Security Identifier (Eindeutiger Sicherheits-Identifikator, den Windows automatisch vergibt, um jedes System, jeden Benutzer und jede Gruppe dauerhaft zu identifizieren)
SMART	Self-Monitoring, Analysis and Reporting Technology (Industriestandard zur Überwachung von Festplatten und SSDs mit einer Vorhersagemöglichkeit für einen potenziellen bevorstehenden Ausfall (Fitnesswerte))
SMBIOS	System Management BIOS (Industriestandard zur Erkennung und Verwaltung von Rechnerkomponenten, der von der Distributed Management Task Force (DMTF) entwickelt wurde)
SMBus	System Management Bus (Zweileiterbus für die Kommunikation mit Baugruppen, etwa Sensor-Chips und Konfigurationsdaten von Speichermodulen)
SPD-EEPROM	Serial Presence Detect -Electrically Erasable Programmable Read-Only Memory (Verfahren zur automatischen Konfiguration von Speichermodulen auf einem Nur-Lese-Speicher, der elektrisch gelöscht werden kann)
SPDWD	Serial Presence Detect Write Disable (Intel-Schutzmechanismus ab DDR4-Speichermodulen, bei denen jeder Schreibzugriff auf die Speichermodule bzw. deren Basisadressen 50h–57h unterbunden wird)
SSE	Streaming SIMD Extensions (Von Intel in 1999 entwickelte Erweiterung des Prozessor-Befehlssatzes)
TPM	Trusted Platform Module (Chip auf der Hauptplatine, der einen Computer oder ähnliche Geräte um grundlegende Sicherheitsfunktionen erweitert)

TSC	Time Stamp Counter (Hochauflösende Zeitquelle in Prozessoren, die in einem 64 Bit-Register die Anzahl der Prozessorzyklen seit dem letzten Reset hochzählen)
UAC	User Account Control (Windows-Benutzerkontensteuerung)
UEFI	Unified Extensible Firmware Interface (Neuartige Rechnerfirmware als Nachfolger des BIOS mit Sicherheitsfunktionen wie SecureBoot)
USB	Universal Serial Bus (Datenübertragungstechnologie zur Verbindung von Rechnern mit externen Geräten)
WBEM	Web-Based Enterprise Management (Microsoft-Implementierung des webbasierten Unternehmensmanagements)
WDK	Windows Driver Kit (Software-Toolsammlung von Microsoft, die eine Entwicklung von Gerätetreibern für die Windows-Plattform ermöglicht. Die Sammlung umfasst Dokumentationen, Beispiele, Build-Umgebungen und Tools für Treiberentwickler)
WDM	Windows Driver Model (Framework für Gerätetreiber, das mit Windows 98 und Windows 2000 eingeführt wurde, um VxD zu ersetzen, welches in älteren Windows-Versionen wie Windows 95 und Windows 3.1 sowie dem Windows NT Driver Model verwendet wurde)
WHEA	Windows Hardware Error Architecture (Mechanismus zur Behandlung von Hardwarefehlern des Betriebssystems, der mit Windows Vista SP1 und Windows Server 2008 als Nachfolger der Machine Check Architecture in früheren Windows-Versionen eingeführt wurde)
WMI	Windows Management Instrumentation (Microsoft-Implementierung für die Infrastruktur von Verwaltungsdaten und -vorgängen unter Windows-basierten Betriebssystemen)
WQL	WMI Query Language (SQL-ähnliche Skriptsprache zur Ansteuerung von WMI)
XMP	Extreme Memory Profile (Von Intel eingeführte Zertifizierungen beginnend mit DDR3-Speichermodulen für eine bessere Ausnutzung der Speichergeschwindigkeit und damit stabileren Betrieb)