Einleitung

Dieses Buch ist für Computerexperten (Entwickler, Sicherheitsforscher und Systemadministratoren) gedacht, die die Funktionsweise der Kernkomponenten von Microsoft Windows 10 und Windows Server 2016 kennenlernen möchten. Mit diesen Kenntnissen können Entwickler beim Schreiben von Anwendungen für die Windows-Plattform die Gründe für bestimmte Designentscheidungen besser verstehen. Sie helfen ihnen auch beim Debugging komplizierter Probleme. Auch Systemadministratoren profitieren von diesen Informationen, da das Wissen, wie das System in seinem Inneren »tickt«, sein Verhalten verständlicher macht und die Störungssuche erleichtert. Sicherheitsforscher erfahren hier, welche Fehlverhalten Softwareanwendungen und das Betriebssystem an den Tag legen können, wie sie missbraucht werden können und welche Schutzmaßnahmen und Sicherheitsfunktionen moderne Windows-Versionen dagegen bieten. Nach der Lektüre dieses Buches haben Sie ein besseres Verständnis darüber, wie Windows funktioniert und welche Gründe hinter seinem Verhalten stehen.

Die Geschichte dieses Buches

Dies ist die siebente Ausgabe eines Buches, das ursprünglich *Inside Windows NT* hieß (Microsoft Press, 1992) und noch vor der Erstveröffentlichung von Windows NT 3.1 von Helen Custer geschrieben wurde. Es war das erste Buch, das es je über Windows NT gab, und es bot wichtige Einsichten in die Architektur und das Design des Systems. *Inside Windows NT, Second Edition* (Microsoft Press, 1998) wurde von David Solomon geschrieben. Es deckte auch Windows NT 4.0 ab und ging weit tiefer in die technischen Details.

Inside Windows 2000, Third Edition (Microsoft Press, 2000) wurde von David Solomon und Mark Russinovich geschrieben. Hier kamen viele neue Themen wie Starten und Herunterfahren, interne Mechanismen von Diensten und der Registrierung, Dateisystemtreiber und Netzwerkanbindung hinzu. Auch die Änderungen am Kernel in Windows 2000 wurden erläutert, darunter das Windows Driver Model (WDM), Plug & Play, Energieverwaltung, Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI), Verschlüsselung, Jobobjekte und Terminaldienste. *Windows Internals, Fourth Edition* (Microsoft Press, 2004) war die neue Ausgabe für Windows XP und Windows Server 2003 mit zusätzlichen Inhalten, um IT-Fachleuten zu helfen, ihre Kenntnisse über die internen Mechanismen von Windows praktisch anzuwenden, z. B. durch die Werkzeuge von Sysinternals und die Analyse von Absturzabbildern.

Mit *Windows Internals, Fifth Edition* (Microsoft Press, 2009) wurde das Buch auf Windows Vista und Windows Server 2008 aktualisiert. Da Mark Russinovich eine Vollzeitstelle bei Microsoft annahm (wo er jetzt als CTO für Azure arbeitet), kam der neue Co-Autor Alex Ionescu hinzu. Zu den neuen Inhalten gehörten der Abbildlader, Einrichtungen für das Debugging im Benutzermodus, ALPC (Advanced Local Procedure Call) und Hyper-V. Die nächste Ausgabe,

Windows Internals, Sixth Edition (Microsoft Press, 2012) war komplett aktualisiert, um viele Änderungen am Kernel in Windows 7 und Windows Server 2008 R2 abzudecken. Außerdem kamen viele neue praktische Experimente hinzu, um die Änderungen an den Werkzeugen deutlich zu machen.

Änderungen in dieser Auflage

Seit der letzten Aktualisierung dieses Buches hat Windows mehrere neue Releases durchlaufen und ist jetzt bei Windows 10 und Windows Server 2016 angekommen. Dabei ist Windows 10 jetzt praktisch der neue Name für Windows. Seit der Produktionsfreigabe hat es wiederum mehrere Releases gegeben. Bezeichnet werden sie jeweils mit einer vierstelligen Zahl, die sich aus dem Jahr und dem Monat der Veröffentlichung zusammensetzt, also z. B. *Windows 10 Version 1703* für die Version vom März 2017. Zum Zeitpunkt der Abfassung dieses Buches hat Windows also seit Windows 7 mindestens sechs Versionen durchlaufen.

Beginnend mit Windows 8 hat Microsoft mit einer Zusammenführung seiner Betriebssysteme begonnen, was für die Entwicklung und für das Windows-Konstruktionsteam von Vorteil ist. Windows 8 und Windows Phone 8 verwendeten bereits einen gemeinsamen Kernel, und mit Windows 8.1 und Windows Phone 8.1 kam auch eine Vereinheitlichung bei modernen Apps hinzu. Mit Windows 10 war die Zusammenführung abgeschlossen: Dieses Betriebssystem läuft auf Desktops, Laptops, Servern, der Xbox One, Smartphones (Windows Mobile 10), der HoloLens und verschiedenen IoT-Geräten (Internet of Things).

Angesichts dieser großen Vereinheitlichung war die Zeit reif für eine neue Ausgabe dieses Buches, um die Änderungen von fast einem halben Jahrzehnt aufzuarbeiten, die zu einer stabileren Kernelarchitektur geführt haben. Daher deckt dieses Buch verschiedene Aspekte des Betriebssystems von Windows 8 bis Windows 10 Version 1703 ab. Des Weiteren heißen wir Pavel Yosifovich als neuen Co-Autor willkommen.

Praktische Experimente

Auch ohne Zugriff auf den Windows-Quellcode können Sie mithilfe des Kerneldebuggers, der Sysinternals-Tools und der eigens für dieses Buch entwickelten Werkzeuge viel über die internen Mechanismen von Windows herausfinden. Immer wenn ein Aspekt des internen Verhaltens von Windows mit einem der Tools sichtbar gemacht oder veranschaulicht werden kann, erfahren Sie in den mit »Experiment« betitelten Abschnitten, wie Sie dieses Tool selbst ausprobieren können. Diese Abschnitte sind über das ganze Buch verteilt, und wir raten Ihnen dazu, diese Experimente bei der Lektüre auszuführen. Es ist viel eindrucksvoller, die sichtbaren Auswirkungen der internen Mechanismen von Windows zu beobachten, als nur darüber zu lesen.

Nicht behandelte Themen

Windows ist ein umfangreiches und vielschichtiges Betriebssystem. In diesem Buch können wir nicht sämtliche internen Mechanismen von Windows abdecken, sondern konzentrieren uns auf

die grundlegenden Systemkomponenten. Beispielsweise werden COM+, die verteilte objektorientierte Programmierinfrastruktur von Windows, und Microsoft .NET Framework, die Grundlage für Anwendungen mit verwaltetem Code, in diesem Buch nicht behandelt. Da es ein Buch über die »Interna« von Windows ist und kein Leitfaden für die Benutzung, die Programmierung oder die Systemadministration, erfahren Sie hier auch nicht, wie Sie Windows verwenden, programmieren oder konfigurieren.

Warnung

Dieses Buch beschreibt nicht dokumentierte Aspekte der internen Architektur und Funktionsweise von Windows (wie interne Kernelstrukturen und -funktionen), die sich zwischen den einzelnen Releases ändern können.

Das soll nicht heißen, dass sie sich zwangsläufig ändern, sondern nur, dass Sie sich nicht auf ihre Unveränderbarkeit verlassen können. Software, die sich auf solche nicht dokumentierten Schnittstellen oder auf Insiderkenntnisse über das Betriebssystem verlässt, kann in zukünftigen Releases von Windows unter Umständen nicht mehr funktionieren. Software, die im Kernelmodus läuft (z. B. Gerätetreiber) und diese nicht dokumentierten Schnittstellen nutzt, kann bei der Ausführung in einer neueren Windows-Version sogar einen Systemabsturz und damit möglicherweise einen Datenverlust für den Benutzer hervorrufen.

Kurz: Bei der Entwicklung von Software für Endbenutzersysteme und allgemein für jegliche Zwecke außer Forschung und Dokumentation sollten Sie niemals auf die in diesem Buch erwähnten internen Windows-Einrichtungen, Registrierungsschlüssel, Verhaltensweisen, APIs oder sonstigen nicht dokumentierten Elemente zurückgreifen. Suchen Sie immer erst auf MSDN (Microsoft Software Developer Network) nach einer offiziellen Dokumentation.

Zielgruppe

In diesem Buch wird vorausgesetzt, dass die Leser mit Windows auf dem Niveau von »Power-Usern« vertraut sind und Grundkenntnisse über Betriebssystem- und Hardwareelemente wie CPU-Register, Arbeitsspeicher, Prozesse und Threads mitbringen. In einigen Abschnitten sind auch Grundkenntnisse über Funktionen, Zeiger und ähnliche Konstrukte der Programmiersprache C von Nutzen.

Der Aufbau dieses Buches

Ebenso wie die sechste Ausgabe ist auch diese in zwei Bände aufgeteilt, von denen Sie den ersten in Händen halten.

- Kapitel 1, »Begriffe und Werkzeuge«, gibt eine allgemeine Einführung in die Grundbegriffe von Windows und in die wichtigsten Werkzeuge, die wir in diesem Buch einsetzen werden. Es ist sehr wichtig, dieses Kapitel als erstes zu lesen, da es die Hintergrundinformationen für das Verständnis des Restes gibt.

Kapitel 2, »Systemarchitektur«, zeigt die Architektur und die Hauptkomponenten auf, aus denen Windows besteht, und erläutert sie. Mehrere dieser Komponenten werden in den folgenden Kapiteln noch ausführlicher beschrieben.

- Kapitel 3, »Prozesse und Jobs«, erklärt, wie Prozesse in Windows implementiert sind, und zeigt die verschiedenen Vorgehensweisen zu ihrer Bearbeitung auf. Des Weiteren werden Jobs beschrieben, die eine Möglichkeit bieten, um eine Gruppe von Prozessen zu steuern und die Containerunterstützung von Windows zu aktivieren.
- Kapitel 4, »Threads«, beschreibt ausführlich, wie Threads verwaltet, geplant und auf sonstige Weise in Windows bearbeitet werden.
- Kapitel 5, »Speicherverwaltung«, zeigt, wie der Speicher-Manager physischen und virtuellen Arbeitsspeicher verwendet, und erklärt die verschiedenen Möglichkeiten, mit denen Prozesse und Treiber den Arbeitsspeicher bearbeiten und nutzen können.

  Kapitel 6, »Das E/A-System«, beschreibt, wie das E/A-System von Windows funktioniert und wie es mit den Gerätetreibern zusammenwirkt, um die Mechanismen für E/A-Peripheriegeräte bereitzustellen.
- Kapitel 7, »Sicherheit«, beschreibt ausführlich die verschiedenen Sicherheitsmechanismen von Windows einschließlich systemeigener Schutzmaßnahmen gegen Exploits.

Schreibweisen

In diesem Buch gelten die folgenden Schreibweisen:

- **Fettschrift** wird für Text verwendet, den Sie in einer Schnittstelle eingeben müssen.
- *Kursivschrift* kennzeichnet neue Begriffe sowie die Bezeichnungen von GUI-Elementen, Dateinamen und Webadressen.
- Codeelemente stehen in `nichtproportionaler Schrift`.
- Bei Tastaturkürzeln steht ein Pluszeichen zwischen den Bezeichnungen der einzelnen Tasten. Beispielsweise bedeutet Strg + Alt + Entf, dass Sie gleichzeitig die Tasten Strg, Alt und Entf drücken müssen.

Begleitmaterial

Damit Sie aus diesem Buch noch größeren Nutzen ziehen können, haben wir Begleitmaterial zusammengestellt, das Sie von der folgenden Seite herunterladen können:

https://dpunkt.de/windowsinternals1

Den Quellcode der Tools, die wir eigens für dieses Buch geschrieben haben, finden Sie auf *https://github.com/zodiacon/windowsinternals*.