UNDOCUMENTED WINDOWS NT

"A flaw in Microsoft's Windows NT operating system allows an ordinary network user . . . to impersonate a system administrator . . . Dabak, Phadke, and Borate discovered the flaw."

— CNET News, July 1998

Ready-to-run scripts and code on CD-ROM

Discover How Versions 3.51,4.0, and the 2000 Betas ReallyOperate

Harness Undocumented APIs to Enhance Performance

Understand and Address Microsoft Windows NT Security Issues

Prasad Dabak, Sandeep Phadke, and Milind Borate

Discoverers of the NT "privilege elevation **attack" security hole**

M&T BOOKS

Undocumented Windows NT®

Undocumented WindowsNT*

Prasad Dabak, Sandeep Phadke,
and Milind Borate

.<-,•:.f

M&T Books
An imprint of IDG Books Worldwide, Inc.

Foster City, CA ◂ Chicago, IL ◂ Indianapolis, IN ◂ New York, NY

Credits

ACQUISITIONS EDITOR
Greg Croy

DEVELOPMENT EDITOR
Barbra Guerra

TECHNICAL EDITOR
David Wall

COPY EDITORS
Nicole LeClerc
Victoria Lee
Mildred Sanchez

BOOK DESIGNER
Kurt Krames

ILLUSTRATOR
Andreas Schueller

PROJECT COORDINATORS
Ritchie Durdin
Linda Marousek

GRAPHICS Et PRODUCTION SPECIALISTS
Mario Amador
Jan Contestable
Jim Kussow
Jude Levinson
Ramses Ramirez

QUALITY CONTROL SPECIALIST
Chris Weisbart

PROOFREADING AND INDEXING
York Production Services

About the Authors

Prasad Dabak holds a master's degree in Computer Science from the University of Pune and has several years of experience working in DOS, Windows, and Unix. Prasad is presently working for Cybermedia Software Private Limited as Director of Engineering, NT Division. Prasad has had the lion's share of writing this book.

Milind Borate holds a bachelor's degree in Computer Science from Pune Institute of Computer Technology and a master's degree in Computer Science from in, Bombay. Milind specializes in file systems and has worked extensively with Solans and Windows NT in the last several years.

Sandeep Phadke holds a B. Tech. from IIT, Bombay and a master's degree from the University of Notre Dame. Sandeep presently is the CEO of Cybermedia Software Private Limited. Sandeep has previously worked for Advanced Computing Systems Company, and as the CEO of SEPL, Pune.

Prasad dedicates this book to his parents, Sharad Sadashiv Dabak and Sushila Sharad Dabak.

Sandeep dedicates this book to his late grandfather, Nana Phadke.

Milind dedicates this book to his parents, Aai and Bhau.

Preface

This book is an attempt to go beneath the surface of one of the most talked-about operating systems — Microsoft Windows NT. Since very little documentation is available on the actual implementation of Windows NT, developers are always searching for more. Windows NT rivals Unix variant operating systems for becoming the most popular operating system in the corporate world where performance, security, robustness, and fault tolerance are of essence.

The books available at the time of writing this book cover the architecture of Windows NT, the Win32 interface exposed by Microsoft to developers, and the usability aspects of Windows NT in great detail. However, none of the books (save a few, such as *Windows NT File System Internals - A Developer's Guide* by Rajeev Nagar, which focuses only on the file systems) has talked about the interfaces underlying the Win32 interface. Once these interfaces are known, they can be immensely valuable to programmers who need to invent ways to solve problems.

Microsoft has maintained the position that these interfaces need not be documented since they are subject to change at any time. It is our observation that a large number of the interfaces are so fundamental to the design of Windows NT operating system that they are unlikely to change. Indeed, they appear to have remained fundamentally intact through the current beta version of Windows 2000.

Another likely reason for not documenting these interfaces may be that all the functionality that is ever required by programmers is largely provided by the documented interfaces (the Win32 interface and a few NT OS Kernel interfaces). However, we feel programmers can benefit by knowing these presently undocumented interfaces. We can quote a large number of examples from Microsoft Windows NT Resource Kit-such as profile.exe (Profiler), tlistexe (Enumerate Threads), and so forth —that use these undocumented interfaces directly. Writing such utilities requires access to the undocumented interfaces - in the same straightforward manner that resource kit utilities are available.

The main goal of this book is to document all these interfaces for the benefit of the serious developer and provide an in-depth understanding of the operating system's architecture.

Who Should Read This Book

This book is intended for developers who want to go beyond the documented world into the depths of Windows NT. This book is also intended for those who want to get a better understanding of Windows NT architecture. The book provides in-depth, hands-on exposure to the various subsystems of Windows NT operating systems, thereby providing a new perspective on the Windows NT architecture. The book documents a very large part of the designs underlying the Win32 interface, including parameters and explanation of the calls. Often the Win32 API does not cover all that is required to write competitive applications in the market. This book, therefore, makes an ideal reference book for any individual or organization desiring to do Windows NT programming beyond the Win32 API. We have matched the underlying undocumented calls with the existing documented Win32 API call, wherever such a one-to-one mapping is possible.

What This Book Covers

Part I provides what we term the essentials as we begin examining the undocumented Windows NT. Topics include "Writing Windows NT Device Drivers" (Chapter 2) and "Reverse Engineering Techniques" (Chapter 5) that provide the reader with sufficient knowledge to experiment.

"Win32 Implementations: A Comparative Look" (Chapter 3) compares and contrasts the three popular Win32 implementations that are popular, and "Memory Management" (Chapter 4) provides a detailed insight into the Windows NT Memory Management architecture. A number of short programs used in this chapter help in better understanding the Memory Management architecture in Windows NT.

Part LI focuses on specific undocumented topics, including "Hooking Windows NT System Services" (Chapter 6) and "Adding New System Services to the Windows NT Kernel" (Chapter 7). These chapters delve into the addition of new system services to Windows NT that are not documented by Microsoft but can certainly be very handy for serious developers. Part LT also covers the "Local Procedure Call" (Chapter 8) mechanism used by the different Windows NT subsystems for communication within Windows NT.

The final chapters of Part II cover "Hooking Software Interrupts" (Chapter 9) and "Adding New Software Interrupts" (Chapter 10) to Windows NT-as well as callgates for Windows NT-and, last, the "Portable Executable File Format" (Chapter 11) used by Win32 executables.

This is followed by Appendix A, which documents most of the previously undocumented system services. The Win32 API heavily uses some of these services. Appendix B provides details about the CD-ROM that accompanies this book.

Conventions Used

Sprinkled throughout the book, you'll find icons indicating material that deserves some special attention.

TIP

Tips contain something that we've discovered to help you (and us) avoid or surmount a challenge.

NOTE

Notes contain a piece of noteworthy information that provides a brief aside from the text.

ON THE CD

On the CD-ROM icons point to code that you'll find on the CD that accompanies the book.

XREF

Cross-references point to another section of the book or other sources that relate to the material under discussion.

CAUTION

Every now and then we alert you to a pitfall or trouble spot — lessons we've gained by experience!

Acknowledgments

First, we acknowledge the encouragement that we received from Andrew Schulman who was instrumental in getting our initial contract for this book. For bringing us together with IDG Books Worldwide Inc., we acknowledge the efforts of Paul Farrell and Greg Croy in acquisitions. Barb Guerra, our development editor, and our IDG Books team of copy editors — Nicole LeClerc, Victoria Lee, and Mildred Sanchez — did a phenomenal job of editing this book on an expedited timetable to keep the book current. The technical editing of David Wall was invaluable, and we appreciate his insights and experience.

We acknowledge Mrs. Shilpa Nene (Patwardhan) for reviewing some of the chapters, and all others who were involved in this process one way or the other. We also acknowledge the late nights tolerated by our family members and thank them for their understanding. Finally, we acknowledge all of our friends who provided moral support for bringing this book to publication.