

Contents at a Glance

	Preface.....	ix
	Acknowledgments.....	xiii
Part 1	Essentials	
Chapter 1	Windows NT: An Inside Look	3
Chapter 2	Writing Windows NT Device Drivers	17
Chapter 3	Win32 Implementations: A Comparative Look ...	23
Chapter 4	Memory Management	33
Chapter 5	Reverse Engineering Techniques	85
Part 11	Undocumented Windows NT	
Chapter 6	Hooking Windows NT System Services	109
Chapter 7	Adding New System Services to the Windows NT Kernel	123
Chapter 8	Local Procedure Call	143
Chapter 9	Hooking Software Interrupts	189
Chapter 10	Adding New Software Interrupts	201
Chapter 11	Portable Executable File Format	223
Part 111	Appendixes	
Appendix A	Details of System Calls with Parameters	253
Appendix Å	What's on the CD-ROM	327
	Index.....	329
	End-User License Agreement	336
	CD-ROM Installation Instructions	340

Contents

	Preface.....	ix
	Acknowledgments.....	xiii
Part 1	Essentials	
Chapter 1	Windows NT: An Inside Look	3
	Evaluating Windows NT	3
	Portability	3
	Extensibility	4
	Compatibility	4
	Maintainability	4
	Plus Points over Windows 95/98	5
	Security	5
	•- Multiprocessing	5
	International Language Support	6
	'ë Multiprogramming	6
	' " Delving into the Windows NT Architecture	7
	The Subsystems	7
	The Core	9
Chapter 2	Writing Windows NT Device Drivers	17
	Prerequisites to Writing NT Device Drivers	17
	Driver Build Procedure	18
	Structure of a Device Driver	19
Chapter 3	Win32 Implementations: A Comparative Look ...	23
	Win32 API Implementation on Windows 95	24
	Win32 API Implementation on Windows NT	24
	• Win32 Implementation Differences	26
	Address Space	26
	-.' Process Startup	27
	Toolhelp Functions	28
	Multitasking	28
	Thinking	29
	Device Drivers	29
	Security	30
	Newly Added API Calls	30

Chapter 4	Memory Management	33
	Memory Models in Microsoft Operating Systems	33
	Windows NT Memory Management Overview	34
	Memory Management Interface - Programmer's View	34
	Below the Operating System	35
	The Inside Look	38
	Flat Address Space	38
	Process Isolation	38
	Code Page Sharing in DLLs	39
	Virtual Memory Management	49
	Virtual Address Descriptors	51
	Impact on Hooking	62
	Copy-on-Write	62
	Switching Context	79
	Differences between Windows NT and Windows 95/98	82
Chapter 5	Reverse Engineering Techniques	85
	How to Prepare for Reverse Engineering	86
	How to Reverse Engineer	87
	Understanding Code Generation Patterns	90
	How Windows NT Provides Debugging Information	91
	ExpEchoPoolCalls	91
	ObpShowAllocAndFree	92
	LpcpTraceMessages	92
	MmDebug	92
	ObDebugFlags	94
	NtGlobalFlag	94
	SepDumpSD	96
	TokenGlobalFlag	96
	CmLogLevel and CmLogSelect	97
	How to Decipher the Parameters Passed to an	
	Undocumented Function	97
	Examining the Error Handling Code	98
	Use in the Function	98
	Checking the Validation Code	99
	Typical Assembly Language Patterns and	
	Their Meanings	99
	The Practical Application of Reverse Engineering	101
Part 11	Undocumented Windows 1MT	
Chapter 6	Hooking Windows NT System Services	109
	System Services: The Long View	109
	System Services under DOS	109

	System Services under Windows 3.x and Windows 95/98	110
	System Services under Windows NT	110
	Need for Hooking System Services	III
	Trapping Events at Occurrence	III
	Modifying System Behavior to Suit User Needs	III
	Studying the Behavior of the System	112
	Debugging	112
	Getting Performance Data for Specific Tasks and Generating Statistics	112
	Types of Hooks	112
	Kernel-Level Hooking	112
	User-Level Hooking	113
	Implementations of Hooks	113
	DOS	113
	Windows 3.x	113
	Windows 95 and 98	114
	Windows NT	114
	Windows \AE System Services	114
	Hooking NT System Services	116
	Implementation of a System Service in Windows NT	116
	Hooking NT System Services	117
Chapter 7	Adding New System Services to the Windows NT Kernel	123
	Detailed Implementation of a System Service in	
	Windows NT	124
	Windows NT System Service Implementation	126
	JCiEndUnexpectedRange (NT 3.51)	127
	_KiErrormode (in Windows NT 4.0 and KiBBTEndUnexpectedRange in Windows 2000)	127
	Adding New System Services	128
	Example of Adding a New System Service	129
	Device Drivers as a Means of Extending the Kernel versus Adding New System Services	141
	KeAddSystemServiceTable	141
	NT 3.51 Design versus NT 4.0 and Windows 2000 Design: Microsoft's Options	141
Chapter 8	Local Procedure Call	143
	The Origin of the Subsystems	143
	Integral Subsystems	144
	Environment Subsystems	144
	Local Procedure Call	145
	Short Message Communication	146
	Shared Section Communication	147

I

	Port-Related Functions	148
	NtCreatePort	148
	NtConnectPort	149
	NtReplyWaitReceivePort	150
	NtAcceptConnectPort	152
	NtCompleteConnectPort	153
	NtRequestWaitReplyPort	153
	NtListenPort	154
	NtRequestPort	154
	NtReplyPort	155
	NtRegisterThreadTerminatePort	155
	NtSetDefaultHardErrorPort	155
	NtImpersonateClientOfPort	156
	LPC Sample Programs	156
	Short Message LPC Sample	157
	Shared Section LPC Sample	166
	Quick LPC	175
	Advantages of Quick LPC	175
	Quick LPC and Win32 Subsystem	176
	Steps in Quick LPC Communication	177
	Quick LPC Sample	178
	Enhancements to the Sample Program	184
Chapter 9	Hooking Software Interrupts	189
	What Are Interrupts?	189
	Interrupt Processing in Real Mode	189
	Interrupt Processing in Protected Mode	190
	Interrupt Processing in V86 Mode	190
	How Operating Systems Use Software Interrupts	190
	Why Software Interrupts Need to Be Hooked	191
	How to Hook Software Interrupts	192
Chapter 10	Adding New Software Interrupts	201
	What Happens When a 32-Bit Application Executes an INT nn Instruction?	201
	Adding New Software Interrupts to the Windows NT Kernel	202
	Using Callgates to Execute Privileged Code	207
	How to Use the Callgate Technique	209
	Paging Issues	220
Chapter 11	Portable Executable File Format	223
	Overview of a PE File	224
	Structure of a PE File	224
	Relative Virtual Address	225

	ImageRvaToVaQ	226
	ImageNtHeader()	227
	MapAndLoad()	227
	UnMapAndLoad()	228
	Details of the PE Format	229
	ReBaseImage()	232
	ImageDirectoryEntryToDataO	235
	Indices in the Data Directory	236
	Export Directory	236
	Import Directory	238
	BindImage()	240
	BindImageEx()	241
	Resource Directory	242
	Relocation Table	243
	Debug Directory	244
	Thread Local Storage	245
	Section Table	246
	Loading Procedure	248
Part 111	Appendixes	
Appendix A	Details of System Calls with Parameters	253
Appendix Â	What's on the CD-ROM	327
	 I n d e x	 329
	 End-User License Agreement	 336
	 CD-ROM Installation Instructions	 340