

Contents

Introduction	1
Who Should Read This Book	1
What You Should Know to Use This Book	1
Sample Code	1
Chapter 13: Working With Memory	3
Memory APIs	3
The VirtualAlloc* Functions	4
Decommitting / Releasing Memory	7
Reserving and Committing Memory	8
The <i>Micro Excel</i> Application	10
Working Sets	17
The <i>Working Sets</i> Application	19
Heaps	23
Private Heaps	24
Heap Types	28
Heap Debugging Features	30
The C/C++ Runtime	32
The Local/Global APIs	34
Other Heap Functions	34
Other Virtual Functions	37
Memory Protection	37
Locking Memory	37
Memory Block Information	38
Memory Hint Functions	39
Writing and Reading to/from Other Processes	40
Large Pages	41
Address Windowing Extensions	44
NUMA	46
The VirtualAlloc2 Function	49
Summary	51
Chapter 14: Memory Mapped Files	53
Introduction	53
Mapping Files	53
The <i>filehist</i> Application	56

Sharing Memory	60
Sharing Memory with File Backing	64
The <i>Micro Excel 2</i> Application	66
Other Memory Mapping Functions	69
Data Coherence	73
Summary	73
Chapter 15: Dynamic Link Libraries	75
Introduction	75
Building a DLL	76
Implicit and Explicit Linking	81
Implicit Linking	82
Explicit Linking	86
Calling Conventions	89
DLL Search and Redirection	90
The <code>DllMain</code> Function	91
DLL Injection	93
Injection with Remote Thread	94
Windows Hooks	96
DLL Injecting and Hooking with <code>SetWindowsHookEx</code>	98
API Hooking	104
IAT Hooking	104
“Detours” Style Hooking	112
DLL Base Address	115
Delay-Load DLLs	118
The <code>LoadLibraryEx</code> Function	120
Miscellaneous Functions	121
Summary	122
Chapter 16: Security	123
Introduction	123
WinLogon	124
LogonUI	125
LSASS	125
LsaIso	126
Security Reference Monitor	126
Event Logger	126
SIDs	127
Tokens	133
The Secondary Logon Service	143
Impersonation	146
Impersonation in Client/Server	149
Privileges	150
Super Privileges	155
Access Masks	158
Security Descriptors	160

The Default Security Descriptor	169
Building Security Descriptors	170
User Access Control	173
Elevation	175
Running As Admin Required	177
UAC Virtualization	178
Integrity Levels	179
UIPI	181
Specialized Security Mechanisms	182
Control Flow Guard	182
Process Mitigations	190
Summary	194
Chapter 17: The Registry	195
The Hives	196
HKEY_LOCAL_MACHINE	196
HKEY_USERS	197
HKEY_CURRENT_USER (HKCU)	198
HKEY_CLASSES_ROOT (HKCR)	198
HKEY_CURRENT_CONFIG (HKCC)	199
HKEY_PERFORMANCE_DATA	199
32-bit Specific Hives	199
Working with Keys and Values	200
Reading Values	202
Writing Values	204
Deleting Keys and Values	206
Creating Registry Links	207
Enumerating Keys and Values	210
Registry Notifications	217
Transactional Registry	221
Registry and Impersonation	222
Remote Registry	222
Miscellaneous Registry Functions	223
Summary	227
Chapter 18: Pipes and Mailslots	229
Mailslots	230
Mailslot Clients	233
Multi-Mailslot Communication	234
Anonymous Pipes	234
The Command Redirect Application	236
Named Pipes	238
Pipe Client	241
The Pipe Calculator Application	242
Other Pipe Functions	248
Summary	249

Chapter 19: Services	251
Services Overview	251
Service Process Architecture	256
A Simple Service	256
Installing the Service	266
A Service Client	269
Controlling Services	271
Installing a Service	272
Starting a Service	277
Stopping a Service	278
Uninstalling the Service	280
Service Status and Enumeration	282
The <i>enumsvc</i> Application	284
Service Configuration	288
Service Description	292
Failure Actions	292
Pre-Shutdown Information	295
Delayed Auto-Start	296
Trigger Information	296
Preferred NUMA Node	300
Launch as PPL	301
Debugging Services	301
Interactive Services	302
Service Security	303
Service SID	305
Service Security Descriptor	306
Per-User Services	308
Miscellaneous Functions	310
Summary	310
Chapter 20: Debugging and Diagnostics	311
Debugger Output	311
The <i>DebugPrint</i> Application	313
Performance Counters	315
Working with Counters	323
The <i>QSlice</i> Application	326
Process Snapshots	331
Querying a Snapshot	334
The <i>snapproc</i> Application	337
Event Tracing for Windows	341
Creating ETW Sessions	358
Processing Traces	376
Real-Time Event Processing	390
The Kernel Provider	393
More ETW	397
Trace Logging	401

Publishing Events with Trace Logging	402
Debuggers	413
A Simple Debugger	416
More Debugging APIs	422
Writing a Real Debugger	424
Summary	424
Chapter 21: The Component Object Model	425
What is COM?	426
Interfaces and Implementations	430
The IUnknown Interface	433
HRESULTs	435
COM Rules (pun intended)	437
COM Clients	438
Step 1: Initialize COM	439
Step 2: Create the BITS Manager	439
Step 3: Create a BITS Job	441
Step 4: Add a Download	443
Step 5: Initiate the Transfer	443
Step 6: Wait for Transfer to Complete	444
Step 7: Display Results	444
Step 8: Clean Up	445
COM Smart Pointers	445
Querying for Interfaces	448
CoCreateInstance Under the Hood	449
CoGetClassObject	450
Implementing COM Interfaces	455
COM Servers	466
Implementing the COM Class	467
Implementing the Class Object (Factory)	469
ImplementingDllGetClassObject	472
Implementing Self Registration	473
Registering the Server	477
Debugging Registration	478
Testing the Server	479
Testing with non C/C++ Client	481
Proxies and Stubs	484
IDL and Type Libraries	487
Threads and Apartments	492
The Free Threaded Mrshalar (FTM)	496
Odds and Ends	498
Summary	498
Chapter 22: The Windows Runtime	499
Introduction	499
Working with WinRT	501

402 Publishing Events with Trace Logging
 403 Debuggers
 404 A Simple Debugger
 405 More Debugging APIs
 406 Writing a Real Debugger
 407 Summary

408 Chapter 21: The Component Object Model
 409 What is COM?
 410 Interfaces and Implementations
 411 COM Rules (not intended)
 412 HRESULTs

CONTENTS

413 The IInspectable interface 506
 414 Language Projections 508
 415 C++/WinRT 511
 416 Asynchronous Operations 515
 417 Other Projections 523
 418 Summary 523

419 Chapter 23: Structured Exception Handling 525
 420 Termination Handlers 525
 421 Replacing Termination Handlers with RAII 527
 422 Exception Handling 528
 423 Simple Exception Handling 529
 424 Using EXCEPTION_CONTINUE_EXECUTION 532
 425 Exception Information 535
 426 Unhandled Exceptions 538
 427 Just in Time Debugging 539
 428 Windows Error Reporting (WER) 541
 429 Vectored Exception Handling 542
 430 Software Exceptions 543
 431 High-Level Exceptions 544
 432 Visual Studio Exception Settings 544
 433 Summary 546
 434 Book Summary 547

435 Proxies and Stubs
 436 IDL and Type Libraries
 437 Threads and Apartments
 438 The Free Threaded Model (FTM)
 439 Odds and Ends
 440 Summary

441 Chapter 25: The Windows Runtime
 442 Introduction
 443 Working with WinRT
 444