

CONTENTS IN DETAIL

ACKNOWLEDGMENTS	xix
------------------------	------------

INTRODUCTION	xxi
---------------------	------------

PART I INTRODUCTION TO IDA

1 INTRODUCTION TO DISASSEMBLY 3

Disassembly Theory	4
The What of Disassembly	5
The Why of Disassembly	6
Malware Analysis	6
Vulnerability Analysis	6
Software Interoperability	7
Compiler Validation	7
Debugging Displays	7
The How of Disassembly	7
A Basic Disassembly Algorithm	8
Linear Sweep Disassembly	9
Recursive Descent Disassembly	11
Summary	14

2 REVERSING AND DISASSEMBLY TOOLS 15

Classification Tools	16
file	16
PE Tools	18
PEiD	19
Summary Tools	20
nm	20
ldd	22
objdump	23
otool	24
dumpbin	25
c++filt	25
Deep Inspection Tools	27
strings	27
Disassemblers	28
Summary	29

3	IDA PRO BACKGROUND	31
	Hex-Rays' Stance on Piracy	32
	Obtaining IDA Pro.....	33
	IDA Versions.....	33
	IDA Licenses	33
	Purchasing IDA	34
	Upgrading IDA	34
	IDA Support Resources.....	35
	Your IDA Installation	36
	Windows Installation	36
	OS X and Linux Installation.....	37
	IDA and SELinux	38
	32-bit vs. 64-bit IDA	38
	The IDA Directory Layout.....	38
	Thoughts on IDA's User Interface.....	40
	Summary.....	40

PART II BASIC IDA USAGE

4	GETTING STARTED WITH IDA	43
	Launching IDA	44
	IDA File Loading	45
	Using the Binary File Loader	47
	IDA Database Files.....	48
	IDA Database Creation.....	50
	Closing IDA Databases	51
	Reopening a Database	52
	Introduction to the IDA Desktop	53
	Desktop Behavior During Initial Analysis	56
	IDA Desktop Tips and Tricks	57
	Reporting Bugs	58
	Summary.....	58

5	IDA DATA DISPLAYS	59
	The Principal IDA Displays.....	60
	The Disassembly Window	60
	The Functions Window	66
	The Output Window.....	66
	Secondary IDA Displays.....	66
	The Hex View Window.....	67
	The Exports Window	68
	The Imports Window	68

The Structures Window	69
The Enums Window.....	70
Tertiary IDA Displays	70
The Strings Window	70
The Names Window	72
The Segments Window	74
The Signatures Window.....	74
The Type Libraries Window.....	75
The Function Calls Window.....	76
The Problems Window.....	76
Summary.....	77

6 DISASSEMBLY NAVIGATION 79

Basic IDA Navigation	80
Double-Click Navigation	80
Jump to Address.....	82
Navigation History	82
Stack Frames	83
Calling Conventions	85
Local Variable Layout	89
Stack Frame Examples	89
IDA Stack Views.....	93
Searching the Database.....	98
Text Searches	99
Binary Searches	99
Summary.....	100

7 DISASSEMBLY MANIPULATION 101

Names and Naming.....	102
Parameters and Local Variables	102
Named Locations	103
Register Names.....	105
Commenting in IDA	106
Regular Comments	107
Repeatable Comments	107
Anterior and Posterior Lines	108
Function Comments	108
Basic Code Transformations	108
Code Display Options	109
Formatting Instruction Operands.....	112
Manipulating Functions	113
Converting Data to Code (and Vice Versa).....	119
Basic Data Transformations	120
Specifying Data Sizes.....	121
Working with Strings.....	122
Specifying Arrays.....	124
Summary.....	126

8	DATATYPES AND DATA STRUCTURES	127
Recognizing Data Structure Use	130	
Array Member Access	130	
Structure Member Access	135	
Creating IDA Structures.....	142	
Creating a New Structure (or Union)	142	
Editing Structure Members	144	
Stack Frames as Specialized Structures	146	
Using Structure Templates.....	146	
Importing New Structures	149	
Parsing C Structure Declarations	149	
Parsing C Header Files	150	
Using Standard Structures	151	
IDA TIL Files.....	154	
Loading New TIL Files.....	155	
Sharing TIL Files.....	155	
C++ Reversing Primer	156	
The this Pointer	156	
Virtual Functions and Vtables	157	
The Object Life Cycle.....	160	
Name Mangling	162	
Runtime Type Identification	163	
Inheritance Relationships	164	
C++ Reverse Engineering References.....	165	
Summary.....	166	
9	CROSS-REFERENCES AND GRAPHING	167
Cross-References	168	
Code Cross-References	169	
Data Cross-References	171	
Cross-Reference Lists.....	173	
Function Calls	175	
IDA Graphing.....	176	
IDA External (Third-Party) Graphing	176	
IDA's Integrated Graph View.....	185	
Summary.....	187	
10	THE MANY FACES OF IDA	189
Console Mode IDA.....	190	
Common Features of Console Mode	190	
Windows Console Specifics	191	
Linux Console Specifics.....	192	
OS X Console Specifics	194	
Using IDA's Batch Mode	196	
Summary.....	198	

PART III ADVANCED IDA USAGE

11		
CUSTOMIZING IDA		201
Configuration Files		201
The Main Configuration File: ida.cfg		202
The GUI Configuration File: idagui.cfg		203
The Console Configuration File: idatui.cfg		206
Additional IDA Configuration Options		207
IDA Colors		207
Customizing IDA Toolbars		208
Summary		210
12		
LIBRARY RECOGNITION USING FLIRT SIGNATURES		211
Fast Library Identification and Recognition Technology		212
Applying FLIRT Signatures		212
Creating FLIRT Signature Files		216
Signature-Creation Overview		217
Identifying and Acquiring Static Libraries		217
Creating Pattern Files		219
Creating Signature Files		221
Startup Signatures		224
Summary		225
13		
EXTENDING IDA'S KNOWLEDGE		227
Augmenting Function Information		228
IDS Files		230
Creating IDS Files		231
Augmenting Predefined Comments with loadint		233
Summary		235
14		
PATCHING BINARIES AND OTHER IDA LIMITATIONS		237
The Infamous Patch Program Menu		238
Changing Individual Database Bytes		238
Changing a Word in the Database		239
Using the Assemble Dialog		239
IDA Output Files and Patch Generation		241
IDA-Generated MAP Files		242
IDA-Generated ASM Files		242
IDA-Generated INC Files		243
IDA-Generated LST Files		243
IDA-Generated EXE Files		243

IDA-Generated DIF Files	244
IDA-Generated HTML Files.....	245
Summary.....	245

PART IV EXTENDING IDA'S CAPABILITIES

15	
IDA SCRIPTING	249
Basic Script Execution	250
The IDC Language.....	252
IDC Variables	252
IDC Expressions	253
IDC Statements	254
IDC Functions	254
IDC Objects	256
IDC Programs	257
Error Handling in IDC	258
Persistent Data Storage in IDC	259
Associating IDC Scripts with Hotkeys	261
Useful IDC Functions	261
Functions for Reading and Modifying Data.....	262
User Interaction Functions.....	263
String-Manipulation Functions	264
File Input/Output Functions.....	264
Manipulating Database Names	266
Functions Dealing with Functions	266
Code Cross-Reference Functions.....	267
Data Cross-Reference Functions.....	268
Database Manipulation Functions.....	268
Database Search Functions.....	269
Disassembly Line Components	270
IDC Scripting Examples.....	270
Enumerating Functions	270
Enumerating Instructions.....	271
Enumerating Cross-References.....	272
Enumerating Exported Functions.....	275
Finding and Labeling Function Arguments	275
Emulating Assembly Language Behavior	278
IDAPython	280
Using IDAPython	281
IDAPython Scripting Examples	282
Enumerating Functions	282
Enumerating Instructions.....	282
Enumerating Cross-References.....	283
Enumerating Exported Functions.....	283
Summary.....	284

16	THE IDA SOFTWARE DEVELOPMENT KIT	285
SDK Introduction		286
SDK Installation.....		287
SDK Layout.....		287
Configuring a Build Environment.....		289
The IDA Application Programming Interface		289
Header Files Overview		290
Netnodes		294
Useful SDK Datatypes		302
Commonly Used SDK Functions.....		304
Iteration Techniques Using the IDA API.....		310
Summary.....		314
17	THE IDA PLUG-IN ARCHITECTURE	315
Writing a Plug-in		316
The Plug-in Life Cycle.....		318
Plug-in Initialization		320
Event Notification.....		321
Plug-in Execution		322
Building Your Plug-ins		324
Installing Plug-ins		329
Configuring Plug-ins		330
Extending IDC		331
Plug-in User Interface Options.....		333
Using the SDK's Chooser Dialogs.....		334
Creating Customized Forms with the SDK.....		337
Windows-Only User Interface-Generation Techniques		341
User Interface Generation with Qt.....		342
Scripted Plug-ins.....		344
Summary.....		346
18	BINARY FILES AND IDA LOADER MODULES	347
Unknown File Analysis.....		348
Manually Loading a Windows PE File.....		349
IDA Loader Modules.....		358
Writing an IDA Loader Using the SDK		358
The Singleton Loader		361
Building an IDA Loader Module		366
A pcap Loader for IDA.....		366
Alternative Loader Strategies		372
Writing a Scripted Loader		373
Summary.....		375

19

IDA PROCESSOR MODULES

377

Python Byte Code.....	378
The Python Interpreter.....	379
Writing a Processor Module Using the SDK.....	380
The processor_t Struct.....	380
Basic Initialization of the LPH Structure.....	381
The Analyzer.....	385
The Emulator.....	390
The Outputter.....	394
Processor Notifications.....	399
Other processor_t Members.....	401
Building Processor Modules.....	403
Customizing Existing Processors.....	407
Processor Module Architecture.....	409
Scripting a Processor Module.....	411
Summary.....	412

PART V

REAL-WORLD APPLICATIONS

20

COMPILER PERSONALITIES

415

Jump Tables and Switch Statements.....	416
RTTI Implementations.....	420
Locating main.....	421
Debug vs. Release Binaries.....	428
Alternative Calling Conventions.....	430
Summary.....	432

21

OBFUSCATED CODE ANALYSIS

433

Anti-Static Analysis Techniques.....	434
Disassembly Desynchronization.....	434
Dynamically Computed Target Addresses.....	437
Imported Function Obfuscation.....	444
Targeted Attacks on Analysis Tools.....	448
Anti-Dynamic Analysis Techniques.....	449
Detecting Virtualization.....	449
Detecting Instrumentation.....	451
Detecting Debuggers.....	452
Preventing Debugging.....	453
Static De-obfuscation of Binaries Using IDA.....	454
Script-Oriented De-obfuscation.....	455
Emulation-Oriented De-obfuscation.....	460
Virtual Machine-Based Obfuscation.....	472
Summary.....	474

22		
VULNERABILITY ANALYSIS		475
Discovering New Vulnerabilities with IDA.....		476
After-the-Fact Vulnerability Discovery with IDA		483
IDA and the Exploit-Development Process		488
Stack Frame Breakdown		488
Locating Instruction Sequences		492
Finding Useful Virtual Addresses		494
Analyzing Shellcode.....		495
Summary.....		498

23		
REAL-WORLD IDA PLUG-INS		499
Hex-Rays.....		500
IDAPython		503
collabREate		503
ida-x86emu.....		506
Class Informer.....		506
MyNav		508
IdaPdf.....		509
Summary.....		510

PART VI

THE IDA DEBUGGER

24		
THE IDA DEBUGGER		513
Launching the Debugger		514
Basic Debugger Displays.....		518
Process Control		521
Breakpoints		522
Tracing		526
Stack Traces		528
Watches		529
Automating Debugger Tasks		530
Scripting Debugger Actions		530
Automating Debugger Actions with IDA Plug-ins.....		536
Summary.....		538

25		
DISASSEMBLER/DEBUGGER INTEGRATION		539
Background.....		540
IDA Databases and the IDA Debugger		541
Debugging Obfuscated Code		543
Launching the Process		545
Simple Decryption and Decompression Loops		546

Import Table Reconstruction	550
Hiding the Debugger	555
IdaStealth.....	560
Dealing with Exceptions	561
Summary.....	568

26

ADDITIONAL DEBUGGER FEATURES 569

Remote Debugging with IDA.....	569
Using a Hex-Rays Debugging Server	570
Attaching to a Remote Process	573
Exception Handling During Remote Debugging.....	574
Using Scripts and Plug-ins During Remote Debugging	574
Debugging with Bochs	574
Bochs IDB Mode	575
Bochs PE Mode.....	576
Bochs Disk Image Mode.....	577
Appcall.....	578
Summary.....	579

A

USING IDA FREEWARE 5.0 581

Restrictions on IDA Freeware	582
Using IDA Freeware	583

B

IDC/SDK CROSS-REFERENCE 585

INDEX 609