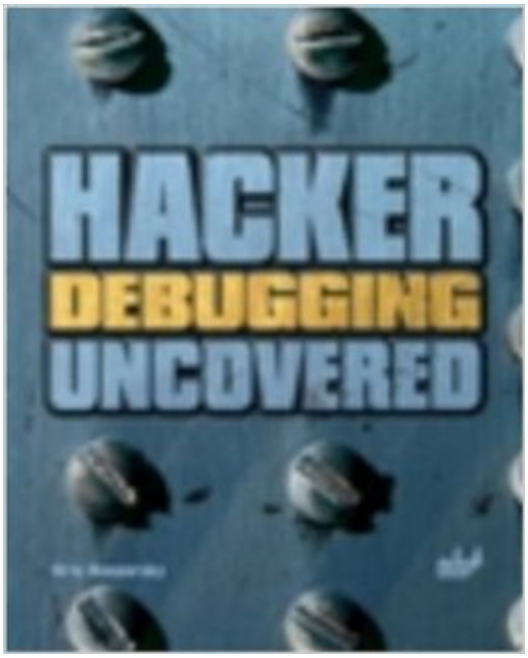
Hacker Debugging Uncovered (Uncovered Series)



Synopsis

Tips for the practical use of debuggers, such as NuMega SoftIce, Microsoft Visual Studio Debugger, and Microsoft Kernel Debugger, with minimum binding to a specific environment are disclosed in this debugger guide. How debuggers operate and how to overcome obstacles and repair debuggers is demonstrated. Programmers will learn how to look at what is inside a computer system, how to reconstruct the operating algorithm of a program distributed without source code, how to modify the program, and how to debug drivers. The use of debugging applications and drivers in Windows and Unix operating systems on Intel Pentium/DEC Alpha-based processors is also detailed.

Book Information

Series: Uncovered series

Paperback: 500 pages

Publisher: A-List Publishing (June 1, 2005)

Language: English

ISBN-10: 1931769400

ISBN-13: 978-1931769402

Product Dimensions: 9.1 x 7.4 x 1.3 inches

Shipping Weight: 2.3 pounds

Average Customer Review: 2.2 out of 5 starsÂ Â See all reviewsÂ (4 customer reviews)

Best Sellers Rank: #2,121,933 in Books (See Top 100 in Books) #95 inÂ Books > Computers & Technology > Programming > Languages & Tools > Debugging #1018 inÂ Books > Computers & Technology > Internet & Social Media > Hacking #4304 inÂ Books > Computers & Technology > Security & Encryption

Customer Reviews

First, a word about the publisher, A-List. This book was delayed time and time again. So much so that I had this book preordered for over a year. This sort of thing is just unacceptable, and would make me inclined to not purchase any books from this publisher in the future, and some of the rating I gave it is because of the publisher.This book has a much larger unix focus than the 'Hacker Disassembling Uncovered' which was largely windows based, however the author's relative unfamiliarity with unix tends to show.For example, on page 39 the author states:IDA Pro, the best disassembler of all times, is nw available under Linux! Users of FreeBSD and other operating systems will have to be content with the console Windows version started under the emulator or have to work on native MS-DOS, OS/2, and Windows.Unfortunately, the author does not mention

(or does not know?) that the OS2 and DOS4GW products were discontinued when the linux version was released. Additionally, FreeBSD (and OpenBSD and NetBSD) can easily run linux binaries by mapping the system calls. It's a very cheap way to run linux binaries, and it was acomplished for OpenBSD within a day or so of the 4.7 release. A much cleaner way is available now; others have managed to do the same for FreeBSD, and NetBSD is likely to be straihtforward as well.There's also some problems with the book that confuse me. For example, on page 432 the author states the following:The C programming language doesn't allow you to declare functionsreturning pointers to functions, because this declaration is recursivelylooped.I simply do not know where he pulled this from. The following small C example demonstrates how to do just this:#include int (*HelloWorld(void))(int,int);int helloworld(int a, int b){ printf("hello world: %d %d\n", a, b); return 0;}int main(void){ int (*foo)(int, int) = HelloWorld(); foo(1,2); return 0;}int (*HelloWorld(void))(int, int){ return helloworld;}And here is it being compiled:brian@lemon:~> gcc -ansi -std=c89 -Wall -o foo foo.cbrian@lemon:~>and here is it being run:brian@lemon:~> ./foohello world: 1 2brian@lemon:~>On to the actual content of the book, it's largely okay. However, if you are expecting new antidebugging ideas, or even ideas hackers are actually going to use, you are in for a rather unfortunate surprise.When I purchased this book, I sort of expected it would keep the duplication from Hacker Disassembling Uncovered to a minimum, but I found that the amount of the book dedicated to static analysis (ie: disassembling and the line) is significant. Far more significant than it should be; nearly the first half of the book is filled with static analysis stuff, working on straightforward crackmes (similar to the previous book in the series), and so forth. This strikes me as fluff in order to boost the price the publisher can charge.Once you get past these negative parts, you have an okay book about (mostly) antidebugging techniques, and some debugging techniques. There's also the requisite PE injection section (sorry, no elf version) along with some basic PE documentation (also no elf version of this).There's quite a bit here if you want a broad ovrview of binary analysis using both static and dynamic analysis. There's nothing new here at all, but if you'd like a bunch of things all in one place, this book may be useful, dispite its many flaws.

I did not completely read the book because I became so exasperated with the book and the author that I quit. The author's continuous praise for a certain software product and his severe criticism of other software used by the author makes one wonder about the relationship between the author and the commercial owner of the praised software. The author even alluded to the non-praised software as possibly being available in a pirated edition. Conversely, the author cautions the reader about copyright law when discussing the praised software. The author is very enamored with himself, and

it detracts from the book. The book is unnecessarily verbose and poorly edited. I was very disappointed, as I was looking for a *how-to-do-it book,* and this book is not suitable for that purpose. Of more concern is the cost of the book's recommended products, which are necessary in order to follow the author. The software products used by the author are commercial and range in cost from less than $100 to a lot more than $100. The reader will spend several hundred dollars on commercial software and other products (Microsoft DDK) if the reader gets the items discussed and recommended by the author. I don't dispute the quality of the products, just the cost of them in addition to the price of the book. There are some errors. For example, the author says Microsoft DDK is free, and yet it has cost about $100 for several years. It would be very expensive to buy the author's suggested products in order to follow the author while reading the book. A CD with source code is included, but without the software its value is diminished. I am sure others will have better experiences, but I cannot recommend the book.

This book was evidently written by a person who speaks English as a second language. It is full of overstatements, non sequiturs, and awkward phrasing that make it quite annoying to read. Here are some excerpts from Chapter 1:"The destiny, however, offered a surprise. This was the new operation system - Windows. Principally, new architecture has rendered all existing debuggers useless...NuMega again surprised the world with a new masterpiece. Its new debugger turned out to be beyond all possible praise...This was a triumph, which no one even dared to imitate.""...Gradually, antidebugging techniques went out of fashion. The victorious advances of Windows made it quit the stage."(!?)Where was the editor for this book? Does no one at ALIST speak English? I bought this book because I confused it with Hacker Disassembling (not Debugging) Uncovered, which is highly rated. I intend to return this book and replace it with the other one.Update: I bought the Disassembling book, and (silly me) it's written by the same author. I should mention that Kris Kaspersky is a well-recognized authority in this arena. He definitely knows his stuff, and the books contain lots of useful information if you can wade through the unfortunate prose. ALIST has done Mr. Kaspersky an injustice by not providing the editing that is needed to make these books what they could and should be.

As other have pointed out, this book offers some useful and advanced knowledge - but that's not enough to make it good. Erratic editing and frequent biased ego trips by the author make it somewhat difficult to read, and leave you wondering if there are better books on that topic. The answer is yes - sadly.

Hacker Debugging Uncovered (Uncovered series) Application Debugging: An MVS Abend Handbook for Cobol, Assembly, PL/I, and Fortran Programmers (Prentice-Hall Software Series) CICS/VS: A guide to application debugging (The QED IBM mainframe series) The Dead Sea Scrolls Uncovered: The First Complete Translation and Interpretation of 50 Key Documents Withheld for over 35 Years The Hacker Playbook 2: Practical Guide To Penetration Testing Secrets To Becoming A Genius Hacker: How To Hack Smartphones, Computers & Websites For Beginners (Hacking) (Volume 1) CEH Certified Ethical Hacker All-in-One Exam Guide, Second Edition CEH v9: Certified Ethical Hacker Version 9 Kit The Hacker Playbook: Practical Guide To Penetration Testing CEH v9: Certified Ethical Hacker Version 9 Study Guide CEH Certified Ethical Hacker: Exam Guide (All-in-One) CEH Certified Ethical Hacker Bundle, Third Edition (All-In-One) Growth Hacker Marketing: A Primer on the Future of PR, Marketing, and Advertising Rare Books Uncovered: True Stories of Fantastic Finds in Unlikely Places Alex & Me: How a Scientist and a Parrot Uncovered a Hidden World of Animal Intelligence--and Formed a Deep Bond in the Process Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker UNCOVERED: What REALLY Happens After The Storm, Flood, Earthquake or Fire E-Learning Uncovered: Articulate Storyline 2