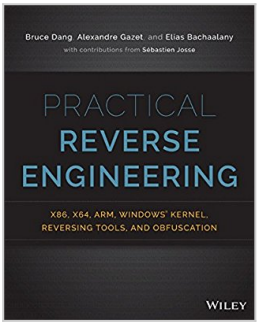

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

By Bruce Dang, Alexandre Gazet, Elias Bachaalany

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany

Analyzing how hacks are done, so as to stop them in the future

Reverse engineering is the process of analyzing hardware or software and understanding it, without having access to the source code or design documents. Hackers are able to reverse engineer systems and exploit what they find with scary results. Now the good guys can use the same tools to thwart these threats. *Practical Reverse Engineering* goes under the hood of reverse engineering for security analysts, security engineers, and system programmers, so they can learn how to use these same processes to stop hackers in their tracks.

The book covers x86, x64, and ARM (the first book to cover all three); Windows kernel-mode code rootkits and drivers; virtual machine protection techniques; and much more. Best of all, it offers a systematic approach to the material, with plenty of hands-on exercises and real-world examples.

- Offers a systematic approach to understanding reverse engineering, with hands-on exercises and real-world examples
- Covers x86, x64, and advanced RISC machine (ARM) architectures as well as deobfuscation and virtual machine protection techniques
- Provides special coverage of Windows kernel-mode code (rootkits/drivers), a topic not often covered elsewhere, and explains how to analyze drivers step by step
- Demystifies topics that have a steep learning curve
- Includes a bonus chapter on reverse engineering tools

Practical Reverse Engineering: Using x86, x64, ARM, Windows Kernel, and Reversing Tools provides crucial, up-to-date guidance for a broad range of IT professionals.

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

By Bruce Dang, Alexandre Gazet, Elias Bachaalany

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation
By Bruce Dang, Alexandre Gazet, Elias Bachaalany

Analyzing how hacks are done, so as to stop them in the future

Reverse engineering is the process of analyzing hardware or software and understanding it, without having access to the source code or design documents. Hackers are able to reverse engineer systems and exploit what they find with scary results. Now the good guys can use the same tools to thwart these threats. *Practical Reverse Engineering* goes under the hood of reverse engineering for security analysts, security engineers, and system programmers, so they can learn how to use these same processes to stop hackers in their tracks.

The book covers x86, x64, and ARM (the first book to cover all three); Windows kernel-mode code rootkits and drivers; virtual machine protection techniques; and much more. Best of all, it offers a systematic approach to the material, with plenty of hands-on exercises and real-world examples.

- Offers a systematic approach to understanding reverse engineering, with hands-on exercises and real-world examples
- Covers x86, x64, and advanced RISC machine (ARM) architectures as well as deobfuscation and virtual machine protection techniques
- Provides special coverage of Windows kernel-mode code (rootkits/drivers), a topic not often covered elsewhere, and explains how to analyze drivers step by step
- Demystifies topics that have a steep learning curve
- Includes a bonus chapter on reverse engineering tools

Practical Reverse Engineering: Using x86, x64, ARM, Windows Kernel, and Reversing Tools provides crucial, up-to-date guidance for a broad range of IT professionals.

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany Bibliography

- Sales Rank: #90943 in Books
- Brand: Brand: Wiley
- Published on: 2014-02-17
- Original language: English
- Number of items: 1
- Dimensions: 9.30" h x .72" w x 7.40" l, 1.47 pounds
- Binding: Paperback
- 384 pages

Editorial Review

From the Back Cover

LEARN THE SCIENCE AND CRAFT OF REVERSE ENGINEERING TO FIGHT HACKERS AND ROOTKITS

Criminals increasingly are using malicious software (exploits, viruses, rootkits, etc.) for fraud, denial-of-service, intrusions, and espionage operations. Reverse engineering is the only method to thoroughly dissect and understand such software. So it is no surprise that reverse engineering is one of the most important subjects in information security. Unfortunately, it is often perceived as a mysterious and complex black art. Although reverse engineering is a difficult subject, the authors believe there is a scientific approach to it. *Practical Reverse Engineering* aims to demystify the art and systematize the reverse-engineering process for students and professionals.

- Discover a unique, systematic approach to reverse engineering that incorporates hands-on analysis with real-world malware
- Find detailed coverage of the three most popular processor architectures: x86, x64, and ARM
- Use this concise, structured treatment of the Windows kernel and kernel-mode drivers, featuring walk-throughs and exercises with real-world rootkits
- Learn sophisticated code-obfuscation techniques, such as those used in virtual machine protections, and how to deobfuscate them using program-analysis techniques
- Discover advanced debugging techniques to automate and streamline the reverse-engineering process
- Apply newly learned concepts with complete walk-throughs and exercises using real-world malware

About the Author
Bruce Dang is a senior security development engineering lead at Microsoft focusing on Windows kernel and reverse engineering.

Alexandre Gazet is a senior security researcher at QuarksLab focusing on reverse engineering and software protection.

Elias Bachaalany is a software security engineer at Microsoft.

Users Review

From reader reviews:

Connie Deroche:

Why don't make it to become your habit? Right now, try to prepare your time to do the important behave, like looking for your favorite e-book and reading a guide. Beside you can solve your short lived problem; you can add your knowledge by the publication entitled Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. Try to the actual book Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation as your friend. It means that it can to become your friend when you truly feel alone and beside regarding course make you smarter than

previously. Yeah, it is very fortuned for yourself. The book makes you a lot more confidence because you can know almost everything by the book. So , let me make new experience and knowledge with this book.

Veronica McFadden:

The ability that you get from Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation is a more deep you looking the information that hide into the words the more you get thinking about reading it. It does not mean that this book is hard to understand but Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation giving you joy feeling of reading. The article writer conveys their point in certain way that can be understood by anyone who read the idea because the author of this guide is well-known enough. This book also makes your own personal vocabulary increase well. That makes it easy to understand then can go with you, both in printed or e-book style are available. We highly recommend you for having this kind of Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation instantly.

Deanna Christianson:

The guide untitled Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation is the reserve that recommended to you to learn. You can see the quality of the publication content that will be shown to anyone. The language that creator use to explained their ideas are easily to understand. The copy writer was did a lot of exploration when write the book, and so the information that they share for you is absolutely accurate. You also will get the e-book of Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation from the publisher to make you far more enjoy free time.

James Fulk:

Reading can called thoughts hangout, why? Because while you are reading a book specifically book entitled Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation your head will drift away trough every dimension, wandering in each and every aspect that maybe unknown for but surely will end up your mind friends. Imaging each word written in a publication then become one application form conclusion and explanation in which maybe you never get previous to. The Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation giving you one more experience more than blown away your thoughts but also giving you useful facts for your better life within this era. So now let us show you the relaxing pattern at this point is your body and mind will probably be pleased when you are finished studying it, like winning a game. Do you want to try this extraordinary investing spare time activity?

Bruce Dang, Alexandre Gazet, Elias Bachaalany #0US25JY73GD

Read Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany for online ebook

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany books to read online.

Online Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany ebook PDF download

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany Doc

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany Mobipocket

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany EPub

0US25JY73GD: Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation By Bruce Dang, Alexandre Gazet, Elias Bachaalany