

Book Review: The IDA Pro Book 2nd Ed

Review by Ryan Linn, CISSP, MCSE, GPEN

It seems like yesterday that I was reviewing Chris Eagle's book, but in reality it's been 3 years. So when I had an opportunity to review *The IDA Pro Book: The Unofficial Guide To The Worlds Most Popular Disassembler, 2nd Edition*, I looked forward to seeing what had changed. And thus a change in the normal extensive EH-Net book review is in order and brevity is the word of the day.

A few things haven't changed since my last review. I am still not a reverse engineer, although I occasionally use the tools clumsily for Capture The Flag (CTF) exercises. I'm not a professional programmer, although I can program and do so frequently. Although this isn't material that I suspect I will master in the near future, this is material in which I have an interest. If you have basic programming skills, an interest in learning, and are willing to sit down and spend time with this material, you will definitely benefit from this book.

After the break, look for a link to a free download of Chapter 24: "The IDA Debugger."

Discuss in Forums {mos_smf_discuss:Book Reviews}

[Click Here to Download Chapter 24: "The IDA Debugger"](#)

Much of the material hasn't changed significantly since the first edition (see review here), however most of the screenshots have been updated to use the Qt version of IDA Pro introduced in the 6.0 major series. As IDA Pro's core functionality hasn't changed drastically since the last version, much of the material from the first edition is still relevant, although Mr. Eagle does a good job of updating critical areas to point out new functionality.

Not surprisingly, the major differences in the book center around new functionality introduced in the 6.0 series of IDA Pro. The biggest changes center around the plugin architecture for IDA Pro. Chris Eagle does an expert job (as he is an expert) demonstrating how to extend IDA Pro to do additional tasks that fall outside of the core functionality of the IDA Pro framework. Whether it is in the newly added Qt API or scripted plugins, Mr. Eagle lays out the new ways to interact with IDA Pro to perform real-world tasks.

The "Real World IDA Plugins" section has seen a number of updates as well as including the IdaPdf plugin. IdaPdf is a plugin that Chris Eagle has written that will aid in analyzing PDF files. With the prevalence of PDF exploits in the wild, this real world plugin is definitely useful. Also covered are the MyNav plugin which extends features in IDA to allow more visual navigation through binaries, and the Class Informer plugin that assists in recovering function names. All of these real world plugins perform tasks that will speed up analysis especially of malware and obfuscated binaries.

A new debugger is also introduced in the "Additional Debugger Features" chapter: the Bochs Debugger. The three main modes are covered along with when to use them. An additional section is also added to this chapter, the Appcall feature. Appcall allows a user to call API functions in the current process through IDAPython or IDC, the languages used to extend IDA.

Overall, the additions made to the book have made an excellent resource even better. If you don't know where to get started, the introduction lays out how the book is organized and where you should start. This is definitely a resource that you will want to read with a computer close by. Just as you wouldn't learn how to cook by just reading cookbooks and not applying them in real-world circumstances, this is a book that you will want to keep with you as you work through the IDA Pro program itself.

While definitely not light reading, this book is clear and concise, and it is going to be one of the resources I turn to every time I am faced with a binary and want to know what it does. Whether you are a reverse engineer, a corporate security admin, a pen tester, or a security enthusiast, this book brings light to a complicated program and works to make it accessible for all. The updates to this book just make it better with up-to-date, real-world examples and Mr. Eagle's experience augmenting the material. I'm glad to have read the book a second time, and I'm excited that it comes so close to an upcoming CTF exercise, where I will have a chance to try these skills out in the wild.

Ryan Linn, CISSP, MCSE, GPEN - Ryan is currently an Information Security Engineer at SAS Institute. Employed in the computer industry since 1997, he has held positions ranging from web developer to Unix Systems Programmer at a large university to his current position in Information Security. Ryan has been responsible for working with large scale deployments of various flavors of *nix, high availability web and database clusters, as well as for application programming in high availability environments. In the past few years, Ryan has incorporated Windows security into his

responsibilities, and is now part of the team responsible for information security globally in one of the largest privately held software companies in the world.