Executive Summary: IDA Pro – at the cornerstone of IT security

What is IDA Pro?

The official line is: *IDA Pro combines an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment.* Quite a mouthful, isn't it? We are aware that the above speaks only to geeks. The "raison d'être" of this small document is to clarify the nature and the purpose of IDA to the non-technical user.

IDA Pro is a disassembler

As a disassembler, IDA Pro explores binary programs, for which source code isn't always available, to create maps of their execution. The real interest of a disassembler is that it shows the instructions that are actually executed by the processor in a symbolic representation called *assembly language*. If the friendly screen saver you have just installed is spying on your e-banking session or logging your e-mails, a disassembler can reveal it. However, assembly language is hard to make sense of. That's why advanced techniques have been implemented into IDA Pro to make that code more readable, in some cases, quite close to the original source code that produced the binary program. The map of the program's code then can be postprocessed for further investigation. Some people have used it as the root of a genomic classification of viruses. (digital genome mapping – advanced malware analysis)

IDA Pro is a debugger

But, in real life, things aren't always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms and trojans are often armored and obfuscated. More powerful tools are required. The debugger in IDA Pro complements the static analysis capabilities of the disassembler: by allowing an analyst to single step through the code being investigated, the debugger often bypasses the obfuscation and helps obtain data that the more powerful static disassembler will be able to process in depth. IDA Pro can be used as a local and as a remote debugger on various platforms, including the ubiquitous 80x86 (typically Windows/Linux) and the ARM platform (typically Windows CE PDAs) and other platforms. Remote debuggers are very useful when one wants to safely dissect potentially harmful programs.

Some IDA debuggers can run the application in a virtual environment: this makes malware analysis even safer.

IDA Pro is interactive

Because no computer can currently beat the human brain when it comes to exploring the unknown, IDA Pro is fully interactive. In sharp contrast with its predecessors, IDA always allows the human analyst to override its decisions or to provide hints. Interactivity culminates in a built-in programming language and an open plugin architecture.

IDA Pro is programmable

IDA Pro contains a complete development environment that consists of a very powerful macro-like language that can be used to automate simple to medium complexity tasks. For more advanced tasks, our open plugin architecture puts no limits on what external developers can do to enhance IDA Pro's functionality. One could, for example, extend IDA Pro with a MP3 player and make malware sing. However, we suspect our governmental customers are involved in more serious projects.

How is IDA Pro useful?

Hostile Code analysis

Given the speed and the complexity of today's hostile code, a powerful analysis solution is required. IDA Pro has become such a standard in the field of malware analysis that information about new viruses is often exchanged under the form of “IDA Databases”. The 2001 “CODE RED” incident is typical of what usually happens in the background. When eEye isolated a new worm whose payload targeted the White House's web site, IDA Pro was used to analyse and understand it: it helped the talented eEye analysts deliver a prompt and accurate warning of the impending attack. 24 hours a day, seven days a week, somewhere in the world, thanks to IDA Pro, anti-virus analysts investigate new virus samples and provide timely solutions.

Vulnerability research

IDA Pro is the ideal tool to investigate why software breaks. While the topic of vulnerability disclosure remains, more than ever, controversial, one cannot ignore the fact that software is unfortunately often vulnerable to outside attacks. It is, without any doubt, a bad idea to let vulnerabilities lurk in essential pieces of software: if they aren't fixed, they could very well be exploited by what we usually call “the bad guys”. The Wisconsin Safety Analyzer is a very interesting project investigating software vulnerability and tamper resistance where IDA Pro plays an important role.

COTS validation

A lot of software is now developed outside the country where it is used. Since programs are incredibly hard to verify, since complete source code audit and rebuilds aren't always practical, tools, such as IDA provide a convenient means to check if a program really does what it claims to do.

Privacy protection

Software is invading our lives at every level. In some cases, such as in what is known as the “Sony Rootkit” story, IDA Pro helps protect your essential rights.

Other uses

IDA Pro has generated quite a lot of interest in academic circles. A partial list of papers where IDA Pro plays a role is visible here.

Recognition

In 2001, IDA Pro was a finalist in the 18th PC Magazine Awards for Technical Excellence. It was a runner-up to Microsoft .NET architecture.

Who are IDA Pro users?

Virtually all anti-virus companies, most vulnerability research companies, many of the large software development companies and, above everything else, three letter agencies and military organizations.