

Re: Reverse engineering != piracy (was Re: RosAsm disassembler output vs. IDA Pro)

Source: <http://coding.derkeiler.com/Archive/Assembler/alt.lang.asm/2004-01/1355.html>

From: Gerhard W. Gruber (*sparhawk_at_gmx.at*)

Date: 01/28/04

Date: Wed, 28 Jan 2004 21:56:32 +0100

On Wed, 28 Jan 2004 03:14:46 GMT wrote "Randall Hyde"

<randyhyde@earthlink.net> in alt.lang.asm with

<GOFrb.30418\$zj7.28784@newsread1.news.pas.earthlink.net>

*>I don't know how much time you've ever spent with a *good* disassembler
>reverse-engineering some code and bringing up to acceptable standards (God
>forbid you try this with a *bad* disassembler!), but it's a tremendous
>amount of work. If you've got the source code to the original routines *in just*

My main purpose of using ASM is for reverse engineering, though I usually don't do it that far to get a assembling sourcecode from it, but even if you just try to find something particular, extract a function or similar stuff is quite a lot of work. I did some reverse engineering on the Amiga back then, because the official documentation was so wrong on some points that it was unusable and the only way was to reverse engineer and document the library we needed. But this takes still quite a lot of time and of course in this case you have the advantage of having a documentation, which, even when wrong, gives you a rough idea what a particular code is supposed to do. :)

*>"Two-click" disassembly/reassembly is the "holy grail" of the disassembly
>crowd. Unfortunately, like the mythical grail, it's never going to be
>achieved.
>Even if it were perfect, it's still a ton of work to try and use the
>disassembler the way that Rene is suggesting. It's much easier to do the translation
>manually.*

As I said in my other post, even if the disassembling process is perfect, there is an inherent flaw which will prevent the creation of a usefull sourcecode, for almost all non-trivial and interesting pieces of code. Especially if the intention is to reuse that source then for your own purposes.

*>If Rene is *really* interested in doing something to make life easier for
>RosAsm users, he'd drop the disassembler project immediately and get to work on*

He would implement proper library support. :)

alt.lang.asm: Re: Reverse engineering != piracy (was Re: RosAsm disassembler output vs. IDA Pro)

>a MASM->RosAsm translator. Those who want a disassembler could then

It shouldn't be that hard to write a MASM translator with lexx & yacc if you are bent on it. Of course this violates the "Holy Assembly" approach. :)

--

Gerhard Gruber

Maintainer of

SoftICE for Linux - <http://pice.sourceforge.net/>

Fast application launcher - <http://sourceforge.net/projects/launchmenu>