

Re: Protecting Source code of a perl script

Source: <http://coding.derkeiler.com/Archive/Perl/comp.lang.perl.misc/2003-11/2442.html>

ctcgag_at_hotmail.com

Date: 11/24/03

Date: 24 Nov 2003 14:41:42 GMT

"Eric J. Roode" <REMOVEsdnCAPS@comcast.net> wrote:

> *Hash: SHA1*

>

> *ctcgag@hotmail.com wrote in news:20031120130645.330\$D@newsreader.com:*

>

>> *"Eric J. Roode" <REMOVEsdnCAPS@comcast.net> wrote:*

> *[...]*

>>> *What makes you think that hiding the source code will make your*

>>> *application more secure?*

>>

>> *Reality.*

>

> *Hah. It will make your application more secure if and only if there are*

> *no crackers who will try to reverse-engineer your algorithms,*

Actually, it will be more secure only if there are crackers. If there are no crackers, security isn't an issue in the first place.

> **and* there*

> *are no bugs or holes that can be found by white-hats.*

If you change "can" to "will", I might agree with you there.

>>> *Typically, a dedicated cracker will figure out*

>>> *what the program is doing and find a way around it anyhow,*

>>

>> *True, and a dedicated lock-picker can pick my lock. But I'd prefer*

>> *not to make the parts transparent, as that would lower the bar for how*

>> *dedicated he would have to be.*

>

> *That analogy is not quite on. The parts need not be transparent, but the*

> *design of the lock should be published. Would you trust a lock from a*

> *manufacturer who refused to tell you how it worked, but simply said,*

> *"Trust me. It's super-duper secure. Nobody can pick this lock!" ?*

Well, if *I* was that manufacturer, sure, I would trust myself. And isn't that what's going on here?

> >> *while your*
> >> *program may not be reviewed for bugs or security holes by your peers.*
> >
> > *It seems like a rather unlikely event that some kind-hearted person is*
> > *going to stumble upon your code uninvited, find the holes, and point*
> > *them out to you. Premeditated code review is a great thing, but in*
> > *the absense of it, it's hard to see how making the code available to*
> > *untrustworthy parties is a good thing.*
>
> *It may seem unlikely, but nearly every month some white-hat finds and*
> *reports (or patches) a security hole in sendmail, bind, or any of a*
> *hundred other unix networking and administration tools.*

But the poster isn't writing any of a hundred unix networking or administration tools. It doesn't sound like he wants to upload his code to CPAN. He doesn't command the attention and respect of a bunch of white-hats. So if he makes it easy for someone to find the holes, chances are that that someone will be doing so in order to exploit the holes, not to report them. If he doesn't even trust his administrator, who is he going to trust to be wearing the white hat?

> *Often, these are*
> *professionals who have encountered a problem at work, but often they are*
> *also hobbyists who are endeavoring to understand the program.*
>
> *There is no possibility of such peer-review with, say, Microsoft*
> *networking and administration tools. Many bugs are reported, and many*
> *patches come out. These must perforce come by way of internal code*
> *review at Microsoft, or painstaking reverse-engineering by people in the*
> *field.*

Right. And that reverse-engineering by people in the field is just as painstaking for the black-hats as it is for the white-hats. You can't have it both ways.

> *I suspect there are far more latent security holes in MS-Windows OS*
> *software than in unix OS software, simply because in the unix world, it*
> *is all laid bare for everyone to see.*

But he isn't writing unix OS software. I doubt he has a bunch of groupies to review the code he is writing.

>
> *Take for example the PGP program with which I signed this message.*
> *Nobody will argue that it's not secure -- and its source code is open for*
> *anyone to see.*

And does that make it secure from an untrusted administrator? How do you know that what I, evil person in charge of your computer, installed on the machine is actually identical to the source that is open for anyone to see?

comp.lang.perl.misc: Re: Protecting Source code of a perl script

Xho

--

----- <http://NewsReader.Com/> -----
Usenet Newsgroup Service New Rate! \$9.95/Month 50GB