

Re: Top Secret Crypto 3.70

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/0125.html>

From: headcrash (headcrash_at_platter.com)

Date: 01/02/05

Date: Sat, 01 Jan 2005 17:26:00 -0800

On Sat, 01 Jan 2005 19:45:47 GMT, Mack
<macckone@a_nospamjunk123_ol.com> wrote:

>On Fri, 31 Dec 2004 00:27:34 -0800, headcrash <headcrash@platter.com>

>wrote:

>

>First I have to say I agree with Tom St. Dennis on his assessment of
>the poor code quality. And I agree with headcrash in general. This
>is not a product that I would recommend.

>

>[snip]

>>><http://www.topsecretcrypto.com>

>>>mkp@topsecretcrypto.com

>>>

>>

>>I can help with that. It's easy when you have this kind of BS on your
>>site to describe the product in jingoistic, non-proven terms:

>>

>>This paragraph was taken verbatim from your website

>>

>>"Top Secret Crypto Gold's strength rests on three basic concepts:

>>(1) a true source of random bits which is provided by the program

>>(2) a very large key space for the pseudo random number generators

>>(3) a simple, but elegant, encryption formula. We call this The

>>Black-Hole Encryption System. Like a black hole in which nothing can

>>escape from, not even light, data encrypted using our system cannot be

>>decrypted and extracted without the correct key."

>>

>>

>>OK, let's start with number 1: Bullsh*t - there is not a true random

>>source of bits on a deterministic-by-nature PC. Anyone who claims

>>differently is a snake oil salesman

>

>This is not strictly true. The method used in the program is the

>collection of the TSC or QueryPerformanceCounter. This has

>been discussed somewhat in sci.crypt.random. The gist of it is

>the random bits are collected from the interrupts and activity

>(network, keyboard, mouse, hard drive activities) and put through a

>chaos generator (the operating system). Using the low bits of these
>counters is pretty effective based on chaos theory. Especially if
>they are hashed after an accurate entropy estimate is determined.
>So far no one has come up with a way to make a valid entropy
>estimate.

And entropy is what we are going for.

Without it, you're hosed.

And without valid methods to make sure we're getting it, we are on a
slippery dangerous slope.

But the problem I have is more with the "claims" being made.

>
>The way the program in question uses them is another matter entirely.
>The following code snippet is a perfect example.
>
> while(TRUE)
> {
> GetRandomBits(32,&dwTestNumber);
> if (dwTestNumber >= 100000001)
> {
> break;
> }
> }
>
>This shows a complete misunderstanding of what random means.
>This specifically eliminates some values. Of course these bits
>are further manipulated which prevents the output from looking
>bad but the method is entirely questionable.

And there is the rub. When someone, who is demonstrating lack of clue
in the first place, takes off and "claims" a "true random number
generator" with their product on these grounds, it raises a red flag.

He also claims the security of OTP. Guess where he's getting the pad?

To me, that is irresponsible.

And with the current tech situation, I would argue with you...
gently... that *anyone* who flatly claims they have a "true random
number generator" from a PC with nothing more than software is a snake
oil peddler.

With the actual environment we have here, there is no question in my
mind.

You are well-spoken, and I agree with most of what you've said. I
think maybe we just disagree on accountability to some extent.

>
>>
>>*Now on to number 2: Bullsh*t – very large keyspace for the pseudo
>>random number generators? What kind of double–speak is that? And
>>don't explain what keyspace means as everyone already knows it. A
>>well–crafted cipher only needs 128–bits of security. Meritless claims
>>of a zillion bits of keyspace are worthless, and the fodder of snake
>>oil peddlers.*
>
>*Agreed.*
>
>>
>>*Hey, we're already at number 3: Bullsh*t – I don't even know where to
>>begin in this one, it stinks so much. Black–Hole Encryption System?
>>WTF is that supposed to mean? How about your competitor's
>>Supermassive Black Hole Encryption System? As everyone (with a bit of
>>astro–physics) knows, supermassive black holes have the mass of over a
>>billion black holes. Suppermassive black holes eat regular black
>>holes. How puny your system looks now. Their system is over a
>>billion times better and stronger than yours. Whatever.*
>>
>>*And the decription of "simple but elegant". Simple – possibly.
>>Elegant – extremely highly unlikely. Everyone before you that has
>>spewed the kind gobbledegook that can be found on your website
>>describing your nimrod encryption product has turned out to have a
>>most inelegant product.*
>>
>
>*Looking at the source code leads me to the conclusion that the
>method may be simple but the source code is far from elegant.*
>
>>
>>*The obvious point here is that anyone who foregoes using an
>>established algorithm like AES or 3DES or Blowfish or Twofish that are
>>available FOR FREE in many reputable products like GNUPG in order to
>>pay actual money for an unproven and most likely insecure product like
>>yours is <explitive deleted> insane.*
>>
>
>*I agree completely with using standard ciphers.
>However the product is free for personal use.*

That may be true, but for an email product, possibly not so useful...

Most persons have jobs, are at work a good deal of the time, and with most of the "free for personal use" licenses I've seen, using the software at your place of work is a violation of the license.

Most persons probably encounter a need to send confidential email during times when they are *not* at home, and if they are using a product like GNUPG they do not need to worry if they are in violation.

If this product, and I use that term loosely, is free like that, then I recant my comments about spending any money on it. But that does little to change why I think using it is ill-advised.

(And before anyone decides to rail on about security at the office workplace, policies and procedures, etc. just a deep breath and suck it up and don't respond, because that is not what we are talking about. That is a different subject for a different thread)

>

>*I would recommend against this product unless you believe in security through obscurity. I was unable to decipher exactly what the program is supposed to do thanks to the lack of organization in the source code and odd mixing of assembly with C*

>

>*[valid ranting snipped]*

>

>>*So, in closing, I think that when he said:*

>>

>>*;) C 3.70 is a bit more than it seems...*

>>

>>

>>*He was being much nicer than I'm being, but the message was the same, which is your product is a bigger bag of snake oil than all get out.*

>>

>>

>>*Again, the better product to use would be GNUPG*

>>

>>*www.GNUPG.com*

>>

>>*Free*

>>

>>*Known-good algorithms designed by some of the best in the non-black crypto-world.*

>>

>>*Compatible with PGP*

>>

>>*Open, well-tested source*

>>

>>*The implementation of GNUPG has been recommended by many of the top crypto people. They've looked at its model closely and see that it is correctly designed and uses proper security techniques.*

>>

>>*And GNUPG doesn't use the snake oil terms "true one time pad" or "true source of random bits" or "Black Hole" anywhere in their website or documentation.*

>>

>>*I can explain it even further for you if this was not sufficient.*

>>

>

sci.crypt: Re: Top Secret Crypto 3.70

>Leslie 'Mack' McBride

>remove text between _ marks to respond via e-mail