

Re: trying to predict next rand value

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1323.html>

From: Skybuck Flying (*nospam_at_hotmail.com*)

Date: 10/29/04

Date: Fri, 29 Oct 2004 01:24:07 +0200

Well I figured it out myself now lol...

This C line is nicely obfuscated... ;)

I was wondering what was returned... holdrand after or before calculating...

```
return(((holdrand = holdrand * 214013L + 2531011L) >> 16) & 0x7fff);
```

I should read this as:

```
(holdrand = holdrand * 214013L + 2531011L);
```

```
return ((holdrand >> 16) & 0x7fff);
```

Bingo ! ;)

(So it does actually two things in one line

1. Update the holdrand variable
2. Calculate some random value and return it ;)

Bye,
Skybuck.

"Mok-Kong Shen" <mok-kong.shen@t-online.de> wrote in message
news:clru70\$hqe\$05\$1@news.t-online.com...

>

>

> *Skybuck Flying wrote:*

>

>> "Mok-Kong Shen" <mok-kong.shen@t-online.de> wrote in message

>> news:clrsp3\$egh\$01\$1@news.t-online.com...

>>

>>>

>>> *Skybuck Flying wrote:*

>>>

>>>

sci.crypt: Re: trying to predict next rand value

```
> >>> Well the question is what does this code do ?
> >>>
> >>> int __cdecl rand (void)
> >>> {
> >>> #ifdef _MT
> >>> _ptiddata ptd = _getptd();
> >>> return( ((ptd->_holdrand = ptd->_holdrand * 214013L + 2531011L) >>
> >
> > 16) &
> >
> >>> 0x7fff);
> >>> #else /* _MT */
> >>> return(((holdrand = holdrand * 214013L + 2531011L) >> 16) & 0x7fff);
> >>> #endif /* _MT */
> >>> }
> >>>
> >>> I am not a C programmer but to me it looks like the next time rand() is
> >>> called... the new value will be based on the old value of rand() ?
> >>>
> >>> But maybe I am reading it wrong :)
> >>>
> >> Perhaps it's best that you look at a textbook like Knuth,
> >> 'The Art of Computer Programming', vol. 2, to see how the PRNGs
> >> commonly function.
> >
> >
> > Neh perhaps it s better if I ask this question in the C lang newsgroup
;)
>
> I believe that you are quite surely right.
>
> M. K. Shen
>
```