

Re: New entropy source proposal.

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-03/0040.html>

From: David Schultz (*das_at_FreeBSD.ORG*)

Date: 03/08/05

Date: Tue, 8 Mar 2005 10:24:30 -0500

To: Richard Coleman <rcoleman@criticalmagic.com>

On Tue, Mar 08, 2005, Richard Coleman wrote:

> *Ian G wrote:*

> > *You might want to check out:*

> >

> > <http://www.av8n.com/turbid/paper/turbid.htm>

> >

> > *There is some controversy over the new FreeBSD /dev/random system,*

> > *is there any analysis of the system? I wasn't able to find anything*

> > *from a brief search.*

> >

> > *iang*

>

> *The FreeBSD /dev/random was originally based on the Yarrow paper that is*

> *given as a reference in the paper above. But I think the current*

> *implementation is more similar to to the version of Yarrow that is*

> *discussed in Bruce Schneier's "Practical Cryptography". I'm not sure if*

> *that is a coincidence or not.*

>

> *The paper mentioned above only briefly mentions Yarrow, and doesn't*

> *mention the FreeBSD implementation, so it's hard to compare the two.*

>

> *At first glance, both systems appear strong.*

There's also:

http://www.usenix.org/publications/library/proceedings/bsdcon02/full_papers/murray/murray_html/

The only objection with it that I'm aware of is that the random device does not ordinarily block, which may make it vulnerable to side channel or cryptanalytic attacks.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"