

# New entropy source proposal.

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-03/0025.html>

---

**From:** Pawel Jakub Dawidek ([pjd\\_at\\_FreeBSD.org](mailto:pjd_at_FreeBSD.org))

**Date:** 03/07/05

Date: Mon, 7 Mar 2005 14:03:30 +0100

To: [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)

Hi.

I've been playing a bit with "use sound card as an entropy source" idea.  
This simple program does what I wanted:

<http://people.freebsd.org/~pjd/misc/sndrand.tbz>

The program is very simple, it should be run with two arguments:

```
% sndtest /dev/dspW 1048576 > rand.data
```

This command will generate 1MB of random data.

With my sound card:

```
pcm0: <Intel ICH3 (82801CA)> port 0xe100-0xe13f,0xe000-0xe0ff irq 11 at device 31.5 on pci0  
pcm0: [GIANT-LOCKED]  
pcm0: <Cirrus Logic CS4299 AC97 Codec>
```

It produce very good entropy. I tried those tests to prove its quality:

- FIPS 140–2 tests
- 'ent' tests: <http://www.fourmilab.ch/random/>
- Famous 'diehard' tests

The full output from diehard tests is here:

[http://people.freebsd.org/~pjd/misc/sndrand\\_diehard.txt](http://people.freebsd.org/~pjd/misc/sndrand_diehard.txt)

The idea of using sound card as entropy source was taken from RFC 1750.

If people like the idea and someone more skilled than me in this subject can review this stuff, we can start to put it into kernel "random infrastructure". It could also be implemented as userland daemon which writes collected entropy to /dev/random maybe...

--

Pawel Jakub Dawidek

<http://www.wheel.pl>

## FreeBSD–Security: New entropy source proposal.

pjd@FreeBSD.org  
FreeBSD committer

<http://www.FreeBSD.org>  
Am I Evil? Yes, I Am!

---

- application/pgp–signature attachment: [stored](#)