

Re: strengthening /dev/urandom

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-08/1344.html>

From: Paul Rubin (//phr.cx_at_NOSPAM.invalid)

Date: 08/20/04

Date: 19 Aug 2004 15:42:12 -0700

Tom St Denis <tomstdenis@iahu.ca> writes:

> *As I understand the code /dev/random isn't an RNG. True RNG support is
> provided by other /dev/<name> virtual files. /dev/random is just a PRNG
> which *happens to* block when it *guesses* it lacks the entropy required.*

Is that right? I thought /dev/random was a pseudo-device that gathered measurements taken from various places around the kernel, as well as (optionally) some from user inputs, and ran those measurements through a PRNG. Maybe the PRNG is cryptographically clever, and Fortuna as a PRNG is maybe even more clever. But the interesting part is the non-PRNG part, i.e. the part that takes physical measurements and tries to estimate the amount of entropy in them.

You guys are saying the entropy estimates are bad and we shouldn't believe them. I'm ok with that notion. Then you say it's impossible to come up with better estimates, so you refuse to do so. That's fine too, if you replace the estimates with the most conservative possible estimate, namely zero, and conclude that /dev/random should simply not be trusted for security purposes. But it seems to me that you're saying two conflicting things:

- 1) there is no way to put a believable number on the amount of entropy inside /dev/random at any moment;
- 2) despite that, it's still ok to use /dev/random in security apps.

That just doesn't make sense to me.

Question for JLC, who seems to say that entropy estimation is inherently impossible no matter what hardware you use: imagine you have an experimental setup containing one atom of some radioactive isotope with a 23.5 second half-life. The experiment simply monitors that atom for 23.5 seconds and outputs a 1 if the atom decays during that interval, and a 0 otherwise. Do you claim that this device is not a TRNG? Do you claim that you can't, with great confidence, estimate the output entropy as being very close to 1 bit?

I'm asking this to check whether I have some severe misconception about JLC's claims.