

Re: [PATCH] API for true Random Number Generators to add entropy (2.6.11)

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-03/9183.html>

From: Andrew James Wade (ajwade_at_CPE0020e06a7211-CM0011ae8cd564.cpe.net.cable.rogers.com)
Date: 03/30/05

To: linux-kernel@vger.kernel.org
Date: Tue, 29 Mar 2005 18:36:55 -0500

On March 29, 2005 05:50 am, Evgeniy Polyakov wrote:

- > *I think the most people use hardware accelerated devices to*
- > *speed up theirs calculations – embedded world is the best example –*
- > *applications that are written to use /dev/random*
- > *will work just too slow, so hardware vendors*
- > *place HW assistant chips to unload that very cpu-intensive work*
- > *from main CPU.*
- > *Without ability speed this up in kernel, we completely [ok, almost]*
- > *lose all RNG advantages.*

The reason for hardware random number generators is that computers are pretty deterministic machines and random number sources tend to be few, far between, very low bitrate, and of uncertain randomness. So much so that without a user (a decent entropy source), a computer might take minutes to collect a few hundred bits of entropy.[1] The advantage of a hardware RNG is that it is random in the first place, high bitrates are just icing on the cake.

[1] Vague recollection from a hardware RNG article.

The thing is few applications need truly random data, and even fewer need much. (Maybe casinos). Even cryptographic applications don't need much; they can be served by a carefully crafted pseudo-random number generator, so long as that generator is seeded with enough entropy. (512 bits of entropy is plenty). And while a cryptographically strong pseudo-random number generator is pretty cpu-intensive, I would be quite surprised to learn that a hardware RNG is faster.

–
To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>