

Re: Why does reading from /dev/urandom deplete entropy so much?

## Re: Why does reading from /dev/urandom deplete entropy so much?

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Kernel/2007-12/msg02630.html>

---

- *From:* Jon Masters <[jonathan@xxxxxxxxxxxxxxxx](mailto:jonathan@xxxxxxxxxxxxxxxx)>
  - *Date:* Sat, 08 Dec 2007 12:54:13 -0500
- 

On Sat, 2007-12-08 at 12:49 -0500, Theodore Tso wrote:

On Sat, Dec 08, 2007 at 11:33:57AM -0600, Mike McGrath wrote:

Huh? What's the concern? All you are submitting is a list of hardware devices in your system. That's hardly anything sensitive....

We actually had a very vocal minority about all of that which ended up putting us in the unfortunate position of generating a random UUID instead of using a hardware UUID from hal :-/

Tinfoil hat responses indeed! Ok, if those folks are really that crazy, my suggestion then would be to do a "ifconfig -a > /dev/random" before generating the UUID, and/or waiting until you just about to send the first profile, and/or if you don't yet have a UUID, generating it at that very moment. The first will mix in the MAC address into the random pool, which will help guarantee uniqueness, and waiting until just before you send the result will mean it is much more likely that the random pool will have collected some entropy from user I/O, thus making the random UUID not only unique, but also unpredictable.

I do like that idea, and it could be combined with the DMI data for the system containing things like asset tracking numbers, etc. Could use HAL to generate a UUID based on hardware IDs and feed that in as entropy ;-)

Jon.

--

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to [majordomo@xxxxxxxxxxxxxxxx](mailto:majordomo@xxxxxxxxxxxxxxxx)  
More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Re: Why does reading from /dev/urandom deplete entropy so much?

Re: Why does reading from /dev/urandom deplete entropy so much?

Please read the FAQ at <http://www.tux.org/lkml/>