Linux support for random number generator in i8xx chipsets

Introduction

The hw_random framework is software that makes use of a special hardware feature on your CPU or motherboard, a Random Number Generator (RNG). The software has two parts: a core providing the /dev/hwrng character device and its sysfs support, plus a hardware-specific driver that plugs into that core.

To make the most effective use of these mechanisms, you should download the support software as well. Download the latest version of the "rng-tools" package from the hw_random driver's official Web site:

http://sourceforge.net/projects/gkernel/

Those tools use /dev/hwrng to fill the kernel entropy pool, which is used internally and exported by the /dev/urandom and /dev/random special files.

Theory of operation

CHARACTER DEVICE. Using the standard open() and read() system calls, you can read random data from the hardware RNG device. This data is NOT CHECKED by any fitness tests, and could potentially be bogus (if the hardware is faulty or has been tampered with). Data is only output if the hardware "has-data" flag is set, but nevertheless a security-conscious person would run fitness tests on the data before assuming it is truly random.

The rng-tools package uses such tests in "rngd", and lets you run them by hand with a "rngtest" utility.

/dev/hwrng is char device major 10, minor 183.

CLASS DEVICE. There is a /sys/class/misc/hw_random node with two unique attributes, "rng_available" and "rng_current". The "rng_available" attribute lists the hardware-specific drivers available, while "rng_current" lists the one which is currently connected to /dev/hwrng. If your system has more than one RNG available, you may change the one used by writing a name from the list in "rng_available" into "rng_current".

Hardware driver for Intel/AMD/VIA Random Number Generators (RNG)

About the Intel RNG hardware, from the firmware hub datasheet

The Firmware Hub integrates a Random Number Generator (RNG) using thermal noise generated from inherently random quantum mechanical properties of silicon. When not generating new random bits the RNG circuitry will enter a low power state. Intel will provide a binary software driver to give third party software access to our RNG for use as a security feature. At this time, the RNG is only to be used with a system in an OS-present state.

Intel RNG Driver notes

FIXME: support poll(2)

> **Note**
>
> request_mem_region was removed, for three reasons:
>
> 1. Only one RNG is supported by this driver;
> 2. The location used by the RNG is a fixed location in MMIO-addressable memory;
> 3. users with properly working BIOS e820 handling will always have the region in which the RNG is located reserved, so request_mem_region calls always fail for proper setups. However, for people who use mem=XX, BIOS e820 information is **not** in /proc/iomem, and request_mem_region(RNG_ADDR) can succeed.

Driver details

Based on:

Intel 82802AB/82802AC Firmware Hub (FWH) Datasheet May 1999 Order Number: 290658-002 R

Intel 82802 Firmware Hub:
Random Number Generator Programmer's Reference Manual December 1999 Order Number: 298029-001 R
Intel 82802 Firmware HUB Random Number Generator Driver

Special thanks to Matt Sottek. I did the "guts", he did the "brains" and all the testing.