VIA C3 Nehemiah Hardware Random Number Generator Linux Driver & Test Utility Usage Guide

Version 0.7, March 26, 2003

1. Summary

The VIA C3 Nehemiah processor includes a high-performance hardware-based random number generator (RNG) on the processor die. The kernel starts to have a driver supporting the RNG from version 2.5.65. This document describes how to update the kernel and then make use of the RNG. We also offer a test utility with source code for users' immediate evaluation. The information and the utility in this document are provided "AS IS," without guarantee of any kind.

2. File description

The package contains 6 files as described below.

`linux-2.5.65.tar.bz2`	31,889,910	03-17-03	06:29	kernel source
`sample/relnote`	330	03-26-03	09:08	utility release note
`sample/bin/rngtest`	13,883	03-26-03	09:14	utility binary
`sample/bin/help`	783	03-26-03	09:17	help file
`sample/src/rngtest.c`	5,512	03-26-03	09:14	utility source code
`Readme.doc`				this file

Users are advised to directly download the kernel source package ver 2.5.65 or later from http://www.kernel.org.

3. Update kernel

The following procedures should work on most Linux distributions, though we tested them only on SuSE Linux 8.1.

(1) Install the kernel source

Run the following command to decompress the kernel source code.

```
# tar xjf linux-2.5.65.tar.bz2
```

(2) Configure the kernel

Change the current directory to "**`linux-2.5.65`**" and run the following command to configure the kernel.

```
# make menuconfig (xconfig or config)
```

There are some situations that may need your special attention.

(a) Enable “**`VIA C3-2 (Nehemiah)`**” under “**`Processor type and features`**”. And if your platform is not a dual-processor system or above, disable “**`Symmetric multi-processing support`**”.

(b) Enable “**`Intel/AMD/VIA HW Random Number Generator support`**” under “**`Character device`**”, by selecting the built-in mode.

In case seeing the following message, this is because the system built-in module tool cannot load the newly added module.

```
#modprobe hw_random
modprobe : QM_MODULES: Function not implemented
modprobe : Can’ t locate module hw_random
```

Then, download and install “**`module-init-tools-x.y.z.tar.gz`**” (**`x.y.z`** the version) at http://www.kernel.org/pub/linux/kernel/people/rusty/modules/.

(3) Rebuild the kernel

Run the following command to rebuild the kernel.

```
# make dep clean bzImage modules modules_install
```

Next, copy the newly built kernel to **`/boot/`**.

```
#cp arch/i386/boot/bzImage /boot/vmlinuz-test
```

If using the **`GRUB`** boot loader, add the following two lines to the **`/boot/grub/menu.lst`** file. Note you may need to modify the “**`hda1`**” according to your actual system settings.

```
Title linux-test
kernel /boot/vmlinuz-test ro root=/dev/hda1
```

On the other hand, if using the **`LILO`** boot loader, add the following four lines to the **`/etc/lilo.conf`** file. Note you may need to modify the “**`hda1`**” according to your actual system settings.

```
image=/boot/vmlinuz-test
Label=linux-test
read-only
root=/dev/hda1
```

Run “**`lilo`**” and let the newly added boot configuration take into effect. On the screen you should be able to see a message like below.

```
Added linux *
Added linux-test
```

Finally, reboot the system and test the new kernel.

4. Verify success of driver installation

Reboot the system and choose the newly added “**`linux-test`**” label to boot. If **`/dev/hwrandom`** does not exist, run the following command to create one.

```
#mknod –m 644 /dev/hwrandom c 10 183
```

Next, run the following command to confirm whether the RNG driver has been loaded into kernel. If not, verify if you have re-build the kernel correctly or if you have the right CPU model.

```
#dmesg | grep “hw_random”
hw_random hardware driver 0.9.0 loaded
```

We also offer a test utility for users’ immediate evaluation. For example, run the following command to generate 10240 bytes of data with 32 hexadecimals per line. Refer to the help file of the utility for more usage information.

```
#./rngtest –b 10240 –n 32
```

5. Test configuration

The following configuration was used for test.

Mainboard	EPIA-M M10000 (CLE266+VT8235)
CPU	VIA C3 Nehemiah CPU 1 GHz (133x7.5)
System Memory	128MB DDRAM
HDD	Maxtor MX6L040J2 40GB
OS (kernel)	SuSE Linux 8.1 (2.4.19-4GB)