CPE Hardware Random Number Generator (TRNG)

Broadcom Corporation
5300 California Avenue
Irvine, California, USA 92677
Phone: 949-926-5000
Fax: 949-926-5203
www.broadcom.com

Revision History

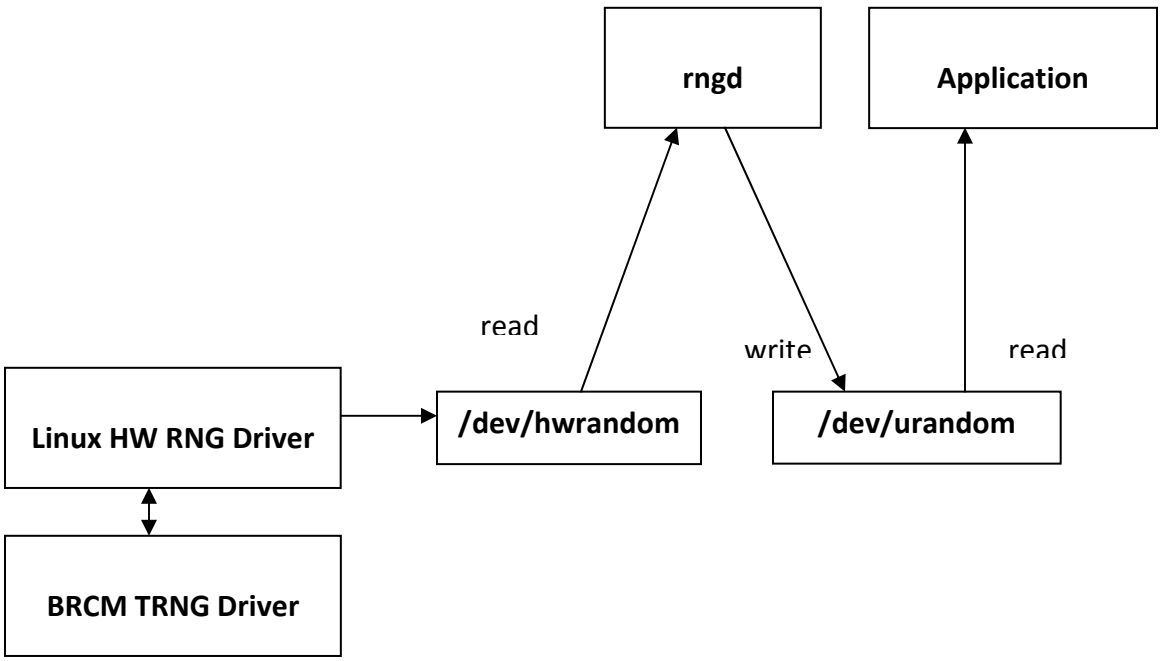
Revision	Date	Change Description
1.0	06/26/09	Initial release

Table of Contents

Introduction

Most of the software random number generators generate Pseudo random numbers which can follow a pattern or might be predictable. This will create a security risk for CPE equipment which is vulnerable to attacks. Broadcom's new generation CPE Chips like BCM6368, 6816 and 6362 provide a Security processing Unit (SPU) hardware block that can generate a True Hardware Random Number (TRNG) that does not follow a pattern or easily predictable. This document will provide information on how to enable and use the TRNG feature.

CPE TRNG Architecture



Architecture of CPE TRNG feature

Standard Linux hardware random number generator architecture is used to access TRNG registers from CPE SPU block. A new character driver, BRCM TRNG driver accesses the hardware TRNG registers and interfaces to standard Linux HW_RANDOM driver. A user space daemon, "rngd" accesses hardware driver and reads the random numbers and fills that information as seed to software random number device "urandom"'s entropy.

If this feature is enabled and any application accessing the "/dev/urandom" will get a better randomness than the Pseudo randomness generated by software random number generator.

How to TRNG Feature

1. In make menuconfig, select "TRNG driver" and "RNGD"
2. Build the newly saved profile
3. access /dev/urandom for True Random Numbers.