

SP 800-90B Non-Proprietary Public Use Document

Ruckus Ironware 10.0.10 Entropy Source

Entropy Source Version: 1.0
Document Version: 1.1
Document Date: 2024-06-03

Prepared by:

Ruckus Wireless LLC

Salarpuria Supreme, #137,

Marathahalli, Bangalore -560037

Template Revision History

Version	Date	Change
V1.0	February 22, 2023	Initial release
V1.1	June 3, 2024	Updated the Min-Entropy Rate

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 5

Configuration Settings 5

Physical Security Mechanisms 6

Conceptual Interfaces 6

Min-Entropy Rate 6

Health Tests 6

Maintenance 7

Required Testing 7

Vendor Permissions and Relationship 7

Description

Ruckus FastIron™ IronWare 10.0.10 Entropy Source v1.0 is the entropy source used on each Ruckus FastIron ICX™ 7150, 7550, 7650, 7850 and 8200 Series Router with firmware IronWare OS 10.0.10 to seed the approved DRBG. The noise source of entropy is periodic sampling of the high-precision CPU clock within the ARM CPU. There is no conditioning component applied on the output of the clock source. Health testing is implemented on the output of the noise source. Health tests are discussed in detail in the below "Health Tests" section.

This public use document is applicable to below production devices of Ruckus.

Router Series	Firmware Version	Processor	Models
ICX7150 Series	IronWare OS 10.0.10	ARM Cortex A9	ICX7150-C12P, ICX7150-24/24P, ICX7150-48/48P/48PF, ICX7150-48ZP
ICX7550 Series	IronWare OS 10.0.10	ARM Cortex-A72	ICX7550-24/48/24P/48P, ICX7550-24ZP/48ZP, ICX7550-24F, ICX7550-48F main board
ICX7650, ICX7850 Series	IronWare OS 10.0.10	ARM Cortex-A57	ICX7650-48C, ICX7650-48F, ICX7650-48P, ICX7650-48ZP, ICX7850-32Q, ICX7850-48F, ICX7850-48FS
ICX8200 Series	IronWare OS 10.0.10	ARM Cortex A55	ICX8200-24/24P/48/48P/48PF/48PF2/C08PF/24ZP/48ZP2/C08ZP/24F/48F/24FX

Table 1. Evaluated Routers' Specifications

Security Boundary

The boundary for this non-physical, software-based entropy source is the executable binary file. It is compiled from the C code that implements it. Figure 1 depicts the overall design of the entropy source and its core operations.

FastIron™ products have a management CPU which runs the software that performs cryptographic operations. The entire unit is the physical cryptographic security boundary (figure 1). The entropy source for all FastIron™ products is the sampling mechanism of reading system time counter of the clock value. There is no interface on the system which can affect this system clock's behavior. An adversary outside the physical cryptographic boundary doesn't have read/write access to this system clock value.

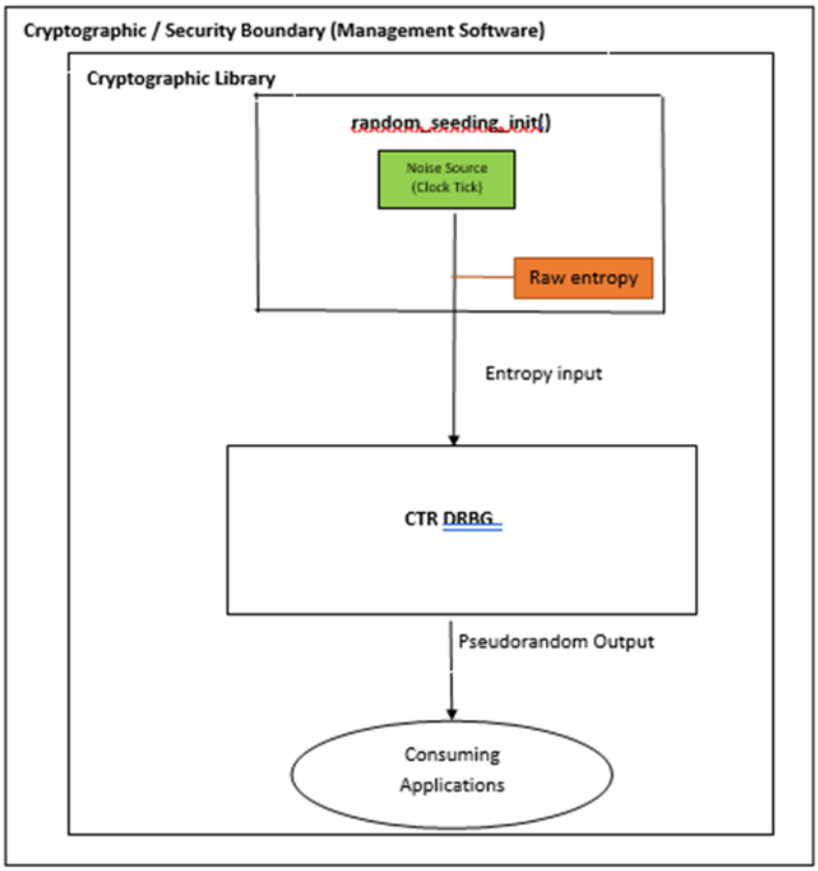


Figure 1: SP 800-90A CTR_DRBG and Entropy Source Model in ICX OS

Operating Conditions

The noise source is not physical in nature, and therefore, its operating conditions are determined by the environment in which the ICX7150/7550/7650/7850/8200 Routers operate properly, as depicted in table 2 below.

Temperature	Voltage
-5° C to 70° C	100-240 V

Table 2. Operating conditions

Configuration Settings

The noise source is a clock source, and no specific configurations are required.

Physical Security Mechanisms

The entropy source/noise source is non-physical. As a result, the physical security mechanisms are applicable solely to the physical boundary of the models listed in table 1 where the entropy source is present. The physical security mechanisms will be available in the respective device series security policy documents.

Conceptual Interfaces

The entropy data can be collected using the below CLI in the test devices.

fips entropy raw: Collects raw entropy upto 1 MB from entropy source for analysis purposes. This will call an API called random_seeding_init which gives 8-bit sample data per call. As a result, each data sample will be in the range of 0 to 255. This sample data is concatenated to generate the 1 MB entropy data file by calling random_seeding_init multiple times.

GetNoise: It is equivalent of GetNoise interface with 1 MB number of samples requested (as there is no conditioning component) mentioned in SP800-90B which is used to collect noise samples.

GetEntropy: It is not explicitly implemented in this case. Instead, the above API is called multiple times and the resultant data is accumulated in a buffer. This buffer is used by DRBG to get entropy input. Buffer size is big enough that the overall effective entropy is more than that is required for the DRBG instantiation. Similar implementation is done for DRBG reseeding.

HealthTest: The entropy source doesn't have a dedicated health test interface, but health tests run continuously on the entropy source output. On-demand and thus start-up health tests can be run by reloading the device. See "Health Tests" section for more details.

Min-Entropy Rate

The entropy source of ICX7150/7550/7650/7850/8200 Routers with IronWare OS 10.0.10 provides a minimum entropy of 4 bits per entropy sample with the sample size: 8 bits.

Health Tests

The entropy source's health tests operate continuously, during start-up, and on-demand on the entropy source output. These are directly applied on noise source output and there is no conditioning component in between. The health tests include both the Repetition Count Test (RCT) and the Adaptive Proportion Test (APT). If either of these two tests fails, the DRBG gets disabled, and the module automatically reboots. No developer defined health tests are implemented as there are no known noise source failure modes.

The following continuous health tests conforming to the SP800-90B section 4.4.1 & 4.4.2 are implemented on the output of entropy source:

- Repetition Count Test.
  H = 4 bits of entropy per 8-bit sample
  false-positive probability $\alpha = 2^{-28}$
  Cutoff value C = 8

- Adaptive Proportion test conforming to SP 800-90B section 4.4.2
  Window size W = 512
  H = 4 bits of entropy per 8-bit sample
  false-positive probability $\alpha = 2^{-28}$
  Cutoff value C = 69

The start-up tests which occur at initialization run the above continuous health tests over the first 1024 samples. On-demand health tests are also implemented in the module. These on-demand tests can be run by simply restarting/reloading module which will in turn run the start-up tests. If there is any failure in these continuous health tests (RCT and APT) within the first 1024 samples, the DRBG gets disabled, and the device will be reloaded. These continuous, start-up and on-demand tests are run in the normal operating conditions mentioned in table 2.

Maintenance

Maintenance is not needed as this is a software-based entropy source.

Required Testing

There is no additional testing required by the target platform. The user or the module developer can verify that the entropy source is working as expected based on the health tests which run continuously. If the health tests fail, the device goes for a reload and an error message is generated to let the user/developer know that there is reduction in the min-entropy output by the entropy source compared to the expected entropy (H = 4). Start-up and on-demand health tests operate similarly.

Vendor Permissions and Relationship

If the ESV indicates “Reuse restricted to vendor”, someone other than the vendor can only use the certificate with written and signed permission from the vendor’s point of contact (as indicated on the ESV certificate). This optional section of the PUD can be used to include this signed permission with any associated details.

This section can also be used when two or more vendors are part of the same company (e.g., different divisions with slightly different names, or a company is a subsidiary of another company that has a validation) to clarify this relationship and include the supporting evidence.