libgcrypt CPU Time Jitter RNG Entropy Source version 3.4.0

SP 800-90B Non-Proprietary Public Use Document

Document Version 1.1

Document Date: 2023-03-27

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1 Description

The libgcrypt CPU Time Jitter RNG version 3.4.0 is a non-physical entropy source. The noise generation of this entropy source is based on the tiny variations in the execution time of the same piece of code. The execution time of this piece of code is made unpredictable by the complexity of the different hardware components that comprise modern CPUs and the different internal states that the operating system can have at a certain point in time. In addition, the timing of these variations depends upon the timer that is used. In this case, the only timer that can be used is the high-resolution timer provided by the CPU of the operational environment.

The entropy source was tested on the operational environments listed in Table 1. The noise source was tested under the assumption that its output is non-IID.

Table 1: Operational environment and version.

Manufacturer	Model	Operational Environment and Version	Processor
Supermicro	Super Server X11DDW-L	SUSE Linux Enterprise Server 15 SP4	Intel(R) Xeon(R) Silver 4215R
GIGABYTE	R181-Z90-00	SUSE Linux Enterprise Server 15 SP4	AMD EPYC(TM) 7371
GIGABYTE	G242-P32-QZ	SUSE Linux Enterprise Server 15 SP4	ARM Ampere(R) Altra(R) Q80-30
IBM	z15 Model T01	SUSE Linux Enterprise Server 15 SP4	IBM z15
IBM	IBM 9080-HEX	SUSE Linux Enterprise Server 15 SP4	IBM Power10

2 Security Boundary

The boundary for this non-physical, software-based entropy source is the libgcrypt shared library in which it resides. It is compiled from the C code that implements it.

The noise source is implemented by collecting and accumulating time variances of variable memory accesses and variances in the execution time of a defined set of instructions, which includes an implementation of SHA3-256. The time variances, in the form of time deltas, are accumulated and mapped down to 256-bits by the SHA3-256 vetted conditioning function which outputs 256 bits of full entropy.

Figure 1 depicts the overall design of the entropy source and its core operations.

If the Repetition Count Test (RCT) or the Adaptive Proportional Test (APT) health tests fail, the noise data is discarded, the entropy source halts without outputting any data, and a failure code is returned to the caller.

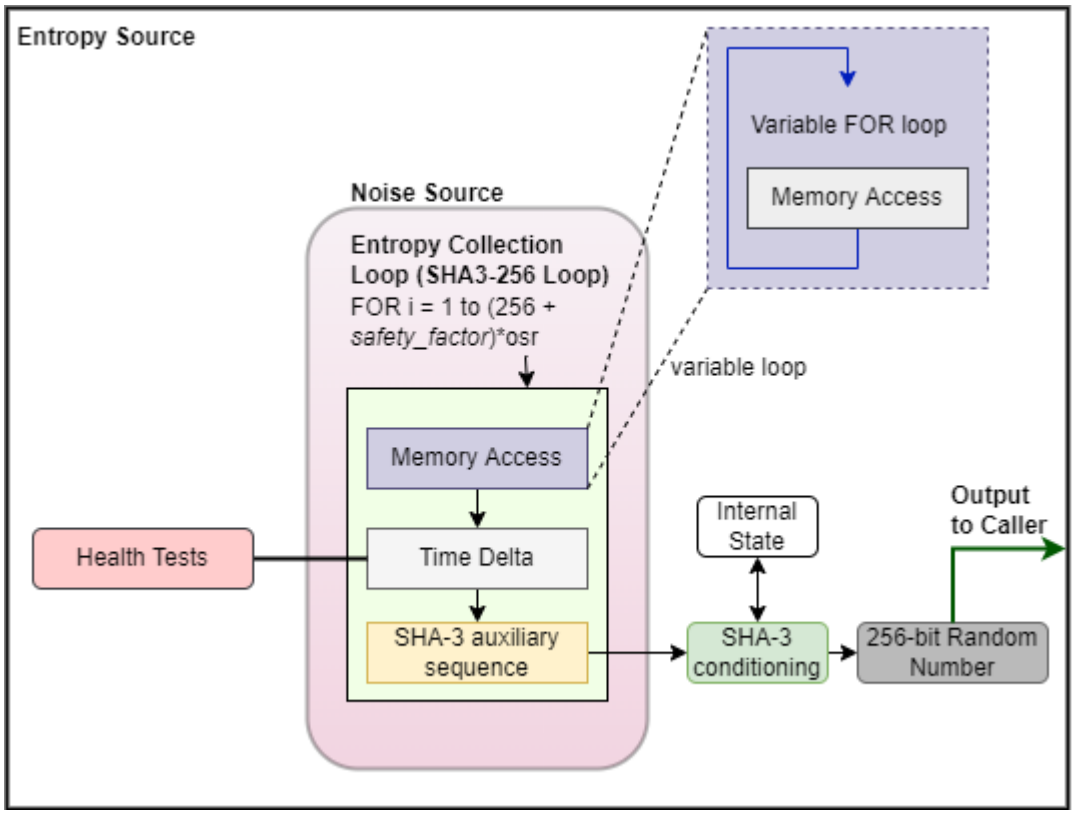

Figure 1: CPU Jitter 3.4.0 Design

3 Operating Conditions

The noise source is non-physical, and thus the operating conditions are inherited from the operational environment in which the entropy source is installed, as shown in Table 2 below.

Table 2: Operating Conditions for each Operational Environment

Manufacturer / Model	Temperature	Voltage	Humidity	Clock Speed	Cache Sizes
Supermicro Super Server X11DDW-L	10C° – 35C°	+12 V	8% - 90%	3.2 GHz	L1: 8x32 KB L2: 8x1 MB L3: 11 MB
GIGABYTE R181-Z90-00	10C° – 35C°	100-240 V	20% - 95%	3.1 GHz	L1: 16x64 KB or 16x32 KB L2: 16x512 KB L3:64 MB
GIGABYTE G242-P32-QZ	10C° – 35C°	100-240 V	8% - 80%	3.3 GHz	L1: 80x64 KB L2: 80x1 MB L3: 80x32 MB

Manufacturer / Model	Temperature	Voltage	Humidity	Clock Speed	Cache Sizes
IBM Z15 Model T01 mainframe	5C - 40C	200-240 V	8% - 85%	5.2 GHz	L1: 128 KB L2: 4 MB L3: 256 MB
IBM IBM 9080-HEX	4C – 40C	4.6k VA	8% – 85%	3.5 GHz	L1: 48+32 KB L2: 2 MB L3: 120 MB

4 Configuration Settings

Configuration of the entropy source can only be done when building the entropy source as part of the libgcrypt cryptographic module.

The only configurable setting is to ensure that the timer selection is to use the external high-resolution CPU timer. Therefore, this ESV certificate is only valid when the external high-resolution CPU timer is used.

The timer settings are defined in the file jitterentropy.h:

```
#define JENT_CONF_ENABLE_INTERNAL_TIMER /* enables internal non-CPU timer. This setting shall be disabled */

#define JENT_FORCE_INTERNAL_TIMER (1<<3) /* forces the use of the internal timer. This setting shall be disabled */

#define JENT_DISABLE_INTERNAL_TIMER (1<<4) /* disable the potential use of the internal timer. This setting shall be enabled */
```

There are other settings in jitterentropy.h that can be changed but this would invalidate the ESV certificate. The following are some examples:

```
#define ENTROPY_SAFETY_FACTOR 64

#define JENT_MEMORY_BITS 17

#define JENT_MEMORY_SIZE (UINT32_C(1)<<JENT_MEMORY_BITS)

#define JENT_MEMORY_BLOCKS 512

#define JENT_MEMORY_BLOCKSIZE 128

#define JENT_MEMORY_ACCESSLOOPS 128
```

5 Physical Security Mechanisms

The noise source is non-physical. The physical security mechanisms only apply to the hardware component of the operational environment in which the entropy source is installed, and thus the entropy source inherits those mechanisms.

6 Conceptual Interfaces

The entropy source provides the following interfaces:

- jent_entropy_init(): Initializes the entropy source context.

- jent_read_entropy(): Obtains conditioned entropy for the caller. This is the main function of the entropy source, the one that shall be used to request entropy data. The entropy gathering logic creates 256 bits per invocation. This interface corresponds to the GetEntropy() conceptual interface from SP800-90B.
- jent_hash_time(): Obtains raw noise data for testing purposes. This interface corresponds to the GetNoise() conceptual interface from SP800-90B.
- jent_entropy_collector_free(): zeroizes and frees the given entropy collector instance.

7 Min-Entropy Rate

$H_{submitter}$ = 1/3 bit per 64 bits of time delta. The original noise sample size has a length of 64 bits. The 64-bit time deltas are concatenated to gather sufficient entropy for the SHA3-256 vetted conditioning function.

The entropy source provides an output of 256 bits. This output provides 256 bits of entropy.

8 Health Tests

The entropy source implements the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1.
  - $H = 1$ bit of entropy per 64-bit sample.
  - alpha value of $\alpha = 2^{-30}$.
  - Cutoff value $C = 31$.
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
  - $W = 512$
  - $H = 1$ bit of entropy per 64-bit sample
  - alpha value of $\alpha = 2^{-30}$.
  - Cutoff value $C = 325$.
- Stuck (Non-Permanent) Test: The stuck test computes the first, second and third discrete derivatives of the time value that will be processed by SHA3-256. If any of these derivatives are zero, then the received time delta is considered stuck. In this case the input state to SHA3-256 is not updated, and the entropy value is not counted. The stuck test then triggers the RCT for further processing. The second derivative is in fact the RCT itself.
- Lag Predictor Test: The goal of this test is to detect a failure mode in which the outputs may become mostly deterministic. In essence, this test constructs a scoreboard and tracks the number of times that a subpredictor was correct. The subpredictor that scored the most correct predictions is used to predict the next value of a series. The lag predictor test is configured in this entropy source with the following parameters:
  - $\alpha = 2^{-22}$
  - Window size: $window\_size = 131072$
  - Lag history size: $lag\_history\_size = 8$
  - Global cutoff = $InverseBinomialCDF = CRITBINOM(n = window_{size} - lag_{history_{size}}; p = 2^{-\frac{1}{osr}}; 1 - \alpha)$

- Local cutoff = 111

The continuous-health tests are applied to each new sample obtained from the noise source. Whenever a failure is detected during the health testing specifically for the RCT and APT, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to acknowledge the failure. The entropy source then halts and will refuse new requests for entropy. Upon return of the failure code, the caller shall attempt to reset or reboot the entropy source or return an error to its own operator. The stuck test is considered non-permanent, as positive stuck tests will be registered but will not immediately halt the entropy source.

Startup tests conduct the same set and parameters of the continuous health tests on 1024 samples of noise data. The data is discarded after the startup tests have completed successfully.

On-demand health tests of the noise source may be performed by rebooting the operational environment, which results in the immediate execution of the start-up tests. Typically, this entropy source designed for user space cannot be reloaded without restarting the executable. Similarly, the data used for the on-demand health tests are discarded after successful completion.

The following error codes are defined for jent_read_entropy():

- -1 entropy_collector is NULL
- -2 RCT failed
- -3 APT test failed
- -4 The timer cannot be initialized
- -5 LAG failure

9 Maintenance

There are no maintenance requirements as this is a software-based noise source.

10 Required Testing

To test the entropy source, raw data samples must be collected using a test harness that is capable of accessing the jent_hash_time() noise interface from the entropy source. The test harness and accessory tools must be supplied by the vendor.

Raw noise data samples consisting of at least 1,000,000 bits must be collected from the operational environment at its normal operating conditions and processed by the SP 800-90B entropy tool that is provided by NIST. The expected min-entropy rate must approach the one in Section 7.

Restart data must be collected at normal operating conditions through the jent_hash_time() interface following the restart procedure specified in SP 800-90B (i.e., 1,000 samples from 1,000 restarts each) and processed by the NIST SP 800-90B entropy tool. The minimum of the row-wise and column-wise entropy rate must be more than half that of the raw noise entropy rate.

In order to access the conditioned output of the SHA3-256 vetted conditioning function a test harness must be able to access jent_read_entropy().