What To Do About Entropy?

Lisa Rabe
Global Certifications Team
Cisco Systems, Inc.

Agenda

- Quick intro to cryptography
- What is entropy?
- Entropy terms
- ESV certification overview
- Types of noise sources
- Physical noise sources
- Non-physical noise sources
- What options are there?
- Need help?

What is Cryptography?

Cryptography is a way of obscuring information so that it can only be read by the intended recipient.

Encryption and decryption of data require two things: knowledge of the cryptographic algorithm and the key.

Modern Cryptography

Algorithms: Known to all

Key: Known only to the parties doing the encryption and decryption

IT'S ALL ABOUT THE KEY!

What is Entropy?

What is entropy (in terms of cryptography)?

Entropy is randomness.

How is entropy used in cryptography?

Entropy is used to produce random numbers, which are used to seed deterministic random bit generators (DRBGs) that generate keys to protect data.

Why should we care about entropy?

Cryptography is only as strong as its keys,

and the keys are only as strong

as the entropy used to create them

SP 800-90 Documents

Series of NIST special publications governing the generation of random bits

SP 800-90A – requirements for DRBGs
- Compliance already required by NIST and NIAP

SP 800-90B – requirements for entropy sources
- Basis of ESV certification

SP 800-90C – requirements for Random Bit Generators (RBGs)
- Still in draft form

Entropy and Security Certifications

- FIPS: NIST requires products seeking FIPS 140-3 validation to use entropy sources are compliant with SP 800-90B.
- Common Criteria: NIAP does not yet require products seeking CC certification to have entropy sources that are compliant with SP 800-90B, but has indicated that it will soon.

Entropy Terms

- Entropy – true, actual randomness
- Entropy data – data that contains bits of entropy mixed with bits of other (non-entropic) data

Entropy Terms

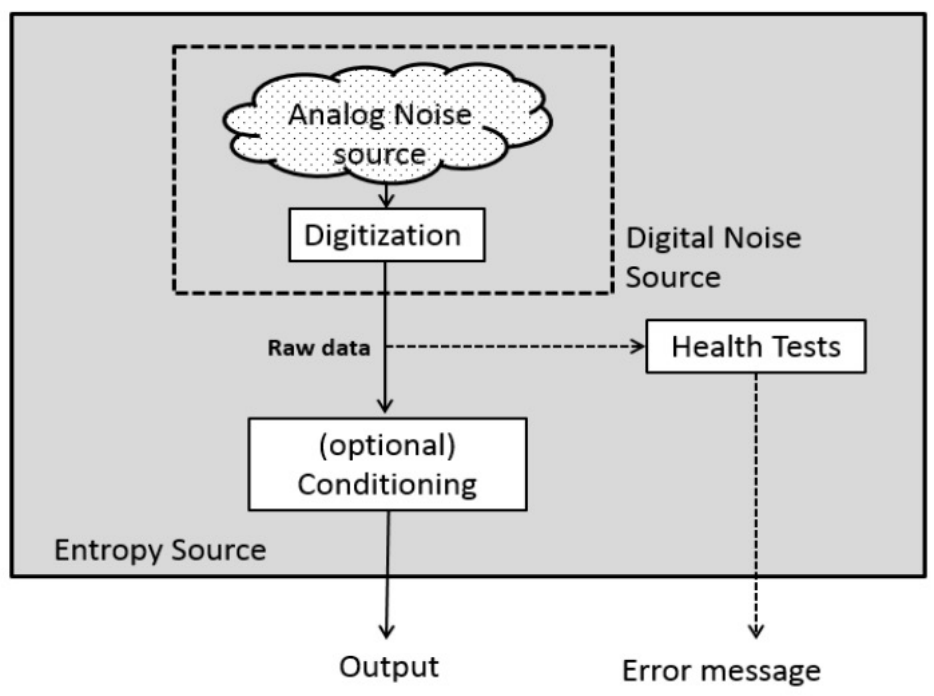
- Noise source – produces entropy data
- Entropy source – contains noise source, digitization, health tests, conditioning functions – produces data that can be used to seed DRBGs

Entropy Terms

- Digitization – process that converts raw data samples to bits
- Conditioning function - process that reduces bias and increases entropy rate of entropy data
- Health tests – tests that run continuously to monitor the health of the noise source

Parts of a 90B Entropy Source

90B Entropy Source Diagram:



ESV Overview

- Entropy Source Validation (ESV) certificate is a standalone entropy certification issued by NIST for entropy sources that are compliant with SP 800-90B
- A 90B-compliant entropy source contains a single primary noise source that can contribute all the entropy that is required
- ESV certs can be bound to the vendor or open for public use
- ESV certs can be reused
- ESV certification process requires two documents: Entropy Analysis Report (EAR) and Public Use Document (PUD)

What is required to get an ESV certificate?

- Very detailed heuristic description of all parts of the entropy source, which includes:
  - Raw noise source
  - Digitization process
  - Conditioning function(s)
  - Health tests
  - Theoretical estimate of the entropy the source should produce
- Statistical test results for:
  - Raw noise data (1,000,000 samples)
  - Restart data (1000 noise samples for each of 1000 restarts)
  - Conditioned data samples for non-vetted conditioning functions (1,000,000 samples)
- Shall statement matrix detailing where each of the almost 140 shall statements have been addressed (shall statements come from SP 800-90B and from the FIPS 140-3 IG)

Types of Noise Sources

- Physical noise sources (HW), which use dedicated HW to generate randomness
  - Ring oscillators
  - Noisy diodes
  - Metastable latches
- Non-physical noise sources, which use system data and/or human data to generate randomness
  - Interrupt timing
  - Disk seek timing
  - Mouse movements
  - Keyboard movements

Both are can be part of a 90B entropy source, and both must fully comply with all 90B requirements.

Physical Noise Sources

Products often rely on the RNGs on their CPUs to generate entropy. These are very commonly used physical noise sources.

Using CPU Entropy

Can I continue to use the Physical Entropy Source on my CPU?

Maybe

Using CPU Entropy

Two paths for using CPU Physical Entropy Source (such as Intel RdRand/RdSeed):

1. Use an ESV cert obtained by the CPU vendor

2. Obtain your own ESV cert on the CPU entropy source

Using CPU Entropy

In either case, the CPU manufacturer will have to provide extremely detailed information about the inner workings of their RNG, and the required raw and restart data for statistical testing.

This path requires the complete cooperation of the CPU manufacturer.

Using CPU Entropy

Best plan – talk to the CPU manufacturer

Alternatives to CPU Entropy

Non-physical entropy sources can receive ESV certification if they meet all 90B requirements.

Using a non-physical entropy source is a viable option, especially if a product doesn't have access to a physical entropy source or the physical entropy source can't be certified.

Non-Physical Entropy Sources

SP 800-90B allows additional noise sources to be mixed with the primary entropy source. The additional noise data must be combined in a specific way with the noise data from the primary source, and it is credited with zero entropy.

The use of additional entropy sources can increase the security of your product.

Non-Physical Entropy Sources

If I can’t use the entropy source on my CPU,
can I get my entropy from the unpatched Linux PRNG
(i.e., /dev/random and dev/urandom)?

No

Problems with Linux PRNG

- Linux PRNG doesn’t have a single primary noise source.
- Multiple noise sources are combined in a way that is not compliant with 90B.
- No Linux health tests are performed on the noise sources.
- Some of the noise sources are not independent, so some noise data is credited twice in the entropy assessment performed in the Linux kernel.
- The Linux PRNG uses multiple non-vetted conditioning functions, which would require large amounts of data to be gathered and run through the NIST statistical tests. This data is not easily accessible from user space.
- Linux PRNG is not compliant with SP 800-90C.
- In addition to the above, the Linux PRNG has so many variations that it’s very difficult to make any blanket statements about them except that none of the them comply with 90B!

Linux PRNGs That Are 90B-Compliant

There are a few versions of Linux that have been patched to make them compliant with 90B. Red Hat and SUSE both have Linux versions that have ESV certs.

Non-Physical Entropy Sources

These non-physical entropy sources were developed by Stephan Mueller. All were designed to be 90B-compliant:

- CPU Jitter Entropy – a small, portable program written in C that generates entropy in user space or in the kernel
- Linux RNG Patch (LRNG) – a kernel patch that makes the Linux PRNG compatible with 90B
- Entropy Source and DRNG Manager (ESDM) – a user-space version of the functionality in the LRNG

You can find more information on these entropy sources at www.chronox.de

CPU Jitter

- Open-source software, written in C, works on almost any processor/platform
- Based on the premise that any set of instructions will take slightly different amounts of time to execute when run multiple times

About 1/3 of the ESV certificates that have been issued so far are based on CPU Jitter

Entropy Delivery

In most cases, entropy should be delivered directly to the DRBG.

Funneling entropy (RDRAND, CPU Jitter, etc.) through an unpatched Linux PRNG is not acceptable.

Need help?

Anyone who wants to learn more about entropy and ESV certifications is welcome to join the CMUF Entropy Working Group

CMUF Entropy Working Group

- Entropy Working Group was started 5 years ago.
- Almost 200 members from labs, vendors, CMVP, BSI
- Members can hear presentations from industry leaders, ask questions of CMVP and 90B authors, provide feedback on documents
- To join, please email Lisa Rabe lirabe@cisco.com

Questions?