Testing SP 800-90B Entropy Sources

Tim Hall
CSD/ITL/NIST

Topics for discussion

- Transition Strategy
  - Current testing methodology
  - New methodology
  - Transition
- Recognition of other testing programs

More topics for discussion

- FIPS 140-2/3 Annexes
- Validation listings
- DRBG/NRBG issues (using entropy sources with DRBG mechanisms)

More topics for discussion

- Test tool available outside labs?
  - est
  - Other implementations
- Other topics – what challenges do you see as implementers and testers

Current testing - FIPS 140-2 IG 7.11

7.11 Definition of an NDRNG

Background

FIPS 140-2 defines a random number generator as follows: *Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed.* ***A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.***

AS.07.07: (Levels 1, 2, 3, and 4) Nondeterministic RNGs shall comply with all applicable RNG requirements of this standard.

AS.07.10: (Levels 1, 2, 3, and 4) Documentation shall specify each RNG (Approved and non-Approved) employed by a cryptographic module.

SP 800-90A addresses deterministic RBGs and nondeterministic RBG definitions**. Draft SP 800-90B addresses entropy testing.**

Current testing - FIPS 140-2 IG 7.11 (cont)

Question/Problem

What defines a nondeterministic RNG (NDRNG) and what are the requirements that apply to it?

Resolution

Any hardware, firmware or software construct that collects or samples bits from single or multiple sources within the modules defined boundary and converts this collection into a single random stream of bits **to be used as a seed input for an Approved RNG or as random input bits for other processes shall be defined as a NDRNG within the scope of FIPS 140-2.**

All the requirements of FIPS 140-2 Section 4.7.1; the self-test requirements specified in FIPS 140-2 Section 4.9; and the conditional Continuous Random Number Generator Test (CRNGT) addressed in IG 9.8 shall apply to an NDRNG implemented in a module. **The NDRNG shall be identified in the security policy and fully described in the test report. The description shall include all entropy sources and applicable smoothing function.**

Current testing - FIPS 140-2 IG 7.13

7.13 Cryptographic Key Strength Modified by an Entropy Estimate

…

Background

FIPS 140-2 Section 4.7 states that **"compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic RNG) shall require as least as many operations as determining the value of the generated key."** To comply with this requirement TE.07.13.02 states that "The tester shall determine the accuracy of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed."

New testing – SP 800-90B Validation Requirements

- Section 9 tests run on 1,000,000+ raw noise source samples
- Conditioning component:
  - CAVP validation of component if Approved (e.g., HMAC, bc_df)
  - Section 9 tests on 1,000,000 conditioned samples if non-Approved
- Validation of health tests
- Documentation for Validation Testing in Section 7

New testing – Some SP 800-90B Doc Requirements from Section 7

- The developer **shall** provide documentation that describes the operation of the entropy source to include how it works, how entropy is produced…

- Documentation **shall** provide a technical argument for why the noise source can support a defined entropy rate. This can be in broad terms of where the unpredictability comes from and a rough description of the behavior…

- Documentation shall describe the conditions under which the entropy source is claimed to operate correctly (e.g., temperature range, voltages, …

Transition Strategy Questions

- “Grandfathering” of entropy sources in already validated modules
  - Yes.
- How long will current FIPS 140-2 evaluation requirements/methodology be accepted after NIST SP 800-90B is published?
  - How long after testing is available?
- If entropy source testing is available but not required, how will distinction be made between tested and non-tested entropy sources?

Transition Strategy Questions

- How long until designs updated to enable collection of raw noise samples, implementation of health tests?
- Should the requirements of NIST SP 800-90B be phased in over time? e.g.,
  - documentation, validation of Approved conditioning components
  - statistical tests
  - continuous health tests implemented and tested

Transition Strategy

- Don’t want to exclude use of good entropy sources
- Do want to reward compliance with SP 800-90B and move designers towards meeting its requirements.
- Security levels for entropy sources based on level or rigor of testing?

Recognition of other programs

- Consider recognition of testing programs that do equivalent of SP 800-90B and additional testing?
- Want to acknowledge in-depth analysis and testing but presents issues:
  - How determine if meets 800-90B requirements?

FIPS 140-2/3 Annexes

- Plan to add NIST SP 800-90B/C to Annex C of FIPS 140-2
- Corresponding Annex of FIPS 140-3

Validation Lists

- NIST CSD will publish public NIST SP 800-90B Entropy Source validation lists on website.
- Separate list for entropy sources
- Format and details TBD.

DRBG/NRBG Issues

- Entropy sources will be validated and listed separately from
  - DRBG mechanisms in SP 800-90A
  - RBG constructions in NIST SP 800-90C.

- Entropy source (NIST SP 800-90B) validation and DRBG mechanism validation will be prerequisites for RBG validation.

Section 9 test tool available outside labs?

- Aid designers and researchers
- If est used as validation tool
  - Need to ask Australia DSD
- Internal NIST code
  - Not same as actual validation tool
  - Not supported
  - Easy to read and use

Questions and Discussion

contact:

tim.hall@nist.gov