Lessons Learned from the 90B Pre-Reviews

Allen Roginsky

April 28, 2021

Main Technical Issues Discovered
1st page

- A confusion between the SP 800-90B notions of a ‘noise source’ and an ‘entropy source’.

- The conversion of an analog signal’s characteristics and measurements into those of a digitized one.

- The testers’ implicit assumption of the independence of the generated entropy bits. They used the independence property without demonstrating that it held.

Main Technical Issues Discovered 2nd page

- An entropy source includes an unbiasing mechanism which is presented as part of a noise source. A lab views an output of an unbiasing function as raw data. Both the statistical tests and the health tests are performed on these data. Instead, an unbiasing function shall be positioned as a conditioning component.

- Labs' handling of the developer-defined health tests (should the vendor introduce them). The 90B standard requires the vendor/tester to prove certain properties of these tests. We often received only some handwaving arguments.

Main Technical Issues Discovered 3rd page

- A heuristic analysis of the amount of entropy produced by the source is not performed properly, and as the result, the selected value of $H_{submitter}$ has not been justified.

- The very high entropy estimates which make the reviewer suspect that there is a hidden step somewhere in the design that is not mentioned in the lab’s Entropy Test Report. (Could be an unbiasing.)

Main Technical Issues Discovered
4th page

- Passing entropy strings that are less than full-entropy to a Counter DRBG without the derivation function. Sometimes this problem is accompanied by another one: several different DRBGs have been CAVP-tested and the lab does not know which one(s) are responsible for generating keys, seeds, etc.

- An excessive reliance on the results of statistical tests.

- Math errors.

Other Issues

- Data collection methods are not identified

- It is not clear where the health tests are performed

- Sample size inconsistency

- An excessive reliance on published books and articles. The assumptions made there are often different, and, in some cases, we were able to point to a specific mismatch.

Summary

- It has been a great learning experience for all parties (I hope), including the CMVP
- Identified some common issues
- The SP 800-90B developers joined the review process and contributed their views and knowledge
- It is difficult to judge an Entropy Test report on the first submission. Usually, the reviewer can only scratch the surface with the notational and the basic design questions.