Clarification to the Entropy Documentation and Assessment Annex

The generation of random bits is vital for key generation and the security strength of our cryptosystems. During analysis of different products, discoveries of weak random values are common, making the remaining security measures irrelevant. There has been significant research into generating pseudorandom bits using a Deterministic Random Bit Generator (DRBG) and an unknown seed value, but ensuring that unknown seed is truly 'unknown' is not as well documented. As a result, entropy implementations traditionally have not been tested to ensure that bits with suitable entropy are input into various DRBG implementations.

Given that there is now an effort by NIST to describe entropy sources and to provide tests that can be used to validate the quality of an entropy source, it is appropriate for the Protection Profiles and CC evaluations to move in that direction as well. Since this is still a new concept for both evaluators and for the vendors, a staggered approach is being used by NIAP to bring all parties to a common understanding so that the common entropy testing is less arduous at the outset. The first step is a documentation exercise, commonly referred to as the "Annex D" requirement or the Entropy Assessment Report (EAR).

The goal of this requirement is to get vendors, evaluators, and validators thinking about the entropy and Random Bit Generation (RBG) implementation. In the short timeframe that this has been a requirement, the resulting reports have varied widely despite the fairly detailed guidance given in the assurance activity. The understanding of entropy between vendors varies - some vendors trust third-party sources they do not fully comprehend. Others have an in-depth understanding and are easily able to provide rationale regarding the security of their products. A small subset has identified problems with their implementations when putting together this information, and has instituted updates to fix the issues. While it may seem like little progress, all of these (acknowledgement of current lack of understanding, practice in rationale/justification submission or data testing, and mitigation of problems) are a significant step forward in ensuring quality entropy.

The US Scheme has developed a fairly standard method for evaluating the entropy documentation provided by the vendors and has identified three major types of entropy sources. Below, for information, are some examples of how the US Scheme reviews the EAR for each of these entropy source types. The information provided within this document is meant to provide general guidance on entropy reporting and should not be considered a "check-list" for successful EAR documentation. Questions on this topic should be directed to the project validator or NIAP.

Software Sources

A number of vendors have submitted entropy documentation for software sources. For such vendors we examine the documentation to verify that the entropy is described completely, from the raw noise source to the input to the DRBG. We verify that the vendor has correctly described what the raw entropy is (i.e., before any conditioning functions such as hashes, mixing functions, or shift registers) and has described how this raw entropy is collected for statistical tests used to justify the entropy claim. If the vendor has not correctly identified or described collecting raw entropy, updated documentation must be resubmitted and reviewed before the product is accepted into evaluation.

Self-Provided Hardware Source

A vendor could provide entropy documentation indicating that the product provides its own hardware source. We have, to date, seen one such report, and have found it appropriate to treat such sources in the same manner as we do software sources.

Third-Party Source

A few vendors have submitted entropy documentation for third-party sources. Unfortunately, due to the limited access to the design and raw entropy data of these third-party sources, the vendor is not able to test the raw entropy source and sometimes is not even able to fully describe the source. Any information that can be shared regarding the design should be included. At a minimum, the documentation must indicate an estimate of the amount of entropy obtained from a third-party source. We generally allow the vendor to “assume” an amount of entropy from the third-party source; however, this assumption must be clearly stated in the documentation provided, the expected amount of entropy must be specified, and a related entropy assumption needs to be made in the Security Target (ST). We still expect a full description of the processing of the output of the third-party source up to and including the seeding of the DRBG implemented in the TOE. Given the assumption, this description must indicate that the DRBG is seeded with the appropriate amount of entropy stated in the ST.

In the future, we intend to require that all third-party sources have been evaluated themselves. To that end, a “platform-based DRBG” source option is included as part of the FCS_RBG_EXT1.2 requirement in relevant Protection Profiles. Due to the limited number of evaluated platforms and to the lack of Protection Profiles for other types of third-party sources (e.g., Trusted Platform Modules), Entropy Assessment Reports for unevaluated third-party sources are still being accepted and treated in the manner described above.

Common Problematic Areas

Regardless of the type of entropy source claimed, there are common areas where EARs often fall short, requiring the documentation to be resubmitted for NIAP review prior to acceptance into evaluation. These are outlined below in order to offer some additional guidance.

Saved State

The capability to add the state of the RBG saved at power-off to use as input to the RBG, prevents an RBG that is slow to gather entropy, from producing the same output regularly and across reboots. This is an important feature for some RBGs so enough variation is introduced such that the initial RBG values are not predictable and exploitable. However, since there is no guarantee of the protections provided when the state is stored (and no requirement for any such protection), it must be assumed that the state is ‘known.’ Therefore, any saved state is not considered to contribute entropy to the seeding of the RBG in order to meet FCS_RBG_EXT.1.2.

Seeding

We expect the vendors to collect a large number of raw source bits, perform statistical tests, and from the statistical tests determine a rate of entropy (i.e. the minimum entropy (in bits) per bit or byte of source data). While no particular statistical tests are required, it is expected that some testing is necessary in order to determine the amount of entropy in each output. In order to verity that the DRBG is initialized with the entropy stated in the ST, we then verify that this rate is multiplied by the amount of source data used to seed the DRBG or that the rate of entropy expected based on the amount of source data is explicitly stated and compared to the statistical rate. If the amount of source data used to seed the DRBG is not clear or the calculated rate is not explicitly related to the seed, the vendor is required to resubmit documentation before the assurance activity for FCS_RBG_EXT.1.2 is considered acceptable.

Raw Samples

Unfortunately, it is sometimes the case that a vendor does not have access to the raw data for testing purposes, and the only data seen has already been processed by some conditioning function. This is especially true for products that use third-party sources; limited access is common. It is important to stress the fact that running statistical tests on conditioned data does not produce valid entropy results. Generally, we would not accept an estimate using conditioned data. At this time, if the raw source is unavailable, it must be stated along with a clear statement of the amount of entropy expected from the conditioned source. When testing eventually moves to the verification of the entropy estimate, lack of access to raw data will no longer be acceptable.

This information is provided for clarification and informational purposes and should not be considered comprehensive guidance, nor used as a checklist for entropy requirements in NIAP-approved Protection Profiles.