Marc Vauclair

From: James Blaisdell [JBlaisdell@mocana.com]
Sent: Wednesday, July 06, 2011 23:27
To: Marc Vauclair; OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG
Subject: RE: UCA Embedded Systems Security - Random Number Generation Sub Group Meetings - AIS Documents

Hello,

On the last RNG call, I took up the task of digging up information for requirements for a proper NDRNG seed when using a DRNG. NIST SP 800-90 is a great source.

FIPS 140 should be considered a requirement for DRNG. Why? You actually need to understand your implementation to be able to fill out the questionnaire forms for FIPS 140, which is a very good thing. In the past (before CY2011), FIPS 140 was simply CMVP (runtime error detection) testing and CAVP (i.e. KAT and PWT). Not sure of cutoff date, but I would recommend no older FIPS 140 be accepted. Not all FIPS 140 cryptographic modules are equal, and many very old implementations still exist and under FIPS 140 are still valid.

If anyone from NIST is on the list, you're doing a great job, and please add more questionnaires. While I am usually the poor soul stuck with completing FIPS 140 questionnaires, I have to admit they are extremely useful for proving validity of implementation. I've never seen CAVP test failure, other than bug in CAVP test for AES-CCM with one byte integrity check (please fix that bug! =)).

If there are any plans to offer OpenSG certified devices, it would be a useful thing for implementations to answer the following questions to ensure a strong RNG seed is used --- these questions are derived from common FIPS 140 questionnaires for NDRNG seeds [I paraphrased the original questions (I don't know the original author) and added some of my own based on FIPS process / dialogue];

1) What are the source(s) of NDRNG (e.g. clock drift, thermal noise, interrupts, non-bias diode, etc)?
2) If multiple sources, how are the source(s) combined?
3) Describe any whitewashing of the NDRNG seed (e.g. run through symmetric or hash algorithm, etc).
4) Describe NDRNG seed (e.g. how often is it replenished, size, how is it used, do you block DRNG when generating seed, etc).
5) Describe how DRNG uses the NDRNG.
6) What is your entropy assessment results for min-entropy of the NDRNG seed generation algorithm? See NIST SP 800-90 Section C.3. Note: I'd like to see people generating at least 4x more entropy then they believe is necessary just to be safe. And they should state why they meet this requirement.
7) Is there any configuration where the source of entropy would not be present? For example, not applicable to embedded devices, keyboard latency was used as input, and no keyboard was attached --- should collect more entropy from other sources to meet the requirement.

I am likely going to miss tomorrow's call due to conflict. I am in PST, and happy to do earlier morning calls. Please let me know if there are any questions. It's a lot to digest, and may be easier to do so during an upcoming RNG call.

Regards,

James