Subject: comments on SP
Date: Wednesday, April 12, 2006 3:43:06 PM Eastern Daylight Time
From: John Kelsey
To: Barker, Elaine B.

--John Kelsey, NIST

Elaine,

Here are my comments on the current version of the SP:

General Comments:

a. We need to work out better terminology for both entropy input and DRBGs vs. DRBG mechanisms, algorithms, functions, etc. I have no idea how to do this yet.

b. We need to put the security levels supported by the DRBG algorithms as of this writing in the text about the DRBGs, or the reader won't know what he's supposed to use.

Specific Comments:

Section 7, first para: "An RBG that uses a DRBG includes...." should be "An RBG that uses a DRBG mechanism includes...." Later in the same sentence, "...depending on the DRBG,..." should be "...depending on the implementation of the DRBG mechanism,..."

7.1, last para, next to last sentence: "In all cases, the DRBG expects...." should be "In all cases, the DRBG mechanism expects...."

7.2, first para: How can the implementation check this data, when there are no requirements on it?

7.3, first para: Kill the last sentence; it only muddies the waters.

8.4, first para, second sentence: "...and on the amount of entropy provided...." should be "...and on the amount of entropy available...."

8.5, general question: Do we need to phrase this in normative language, given that it's all a convenience for explaining the DRBG algorithms/mechanisms/DRBGs/whatever?

8.5, 5th para: (End of page 16)

Isn't this thing about bringing entropy input from outside the boundary counter to what you were doing before? I think this is a DRBG/DRBG Mechanism/DRBG Algorithm issue.

8.6.5, item 3: What's an "appropriate" entropy source?

8.6.8, second para: The description in parentheses isn't informative to the reader. How about "(i.e., the number of outputs produced before a reseed)"?

8.6.8, last para: The overlap of talking about instantiation, the instantiate (vs. reseed) function, and a DRBG instantiation makes my head spin.

8.6.10: "...to create that seeds...." should be "...to create that seed...."

9, beginning:

I think this would be a great place to really spell out the distinction between DRBGs, DRBG algorithms, and DRBG mechanisms, or whatever better terminology we might come up with. I think three or four paragraphs would be enough.

9.1, paragraph after first numbered list, last sentence: I think the sentence should end "DRBG algorithm."

10.1, table: We really need to tell people what security level they can expect from the DRBGs. Refering them to another document that they'll have to decode (does Hash_DRBG with SHA256 have 128 or 256 bits of security, and how could an average reader decide that?) is pretty hard on them.

10.1.1.2, picture: There's something odd with the counter part of the picture. This is repeated other places. I think you tried to shade the box, but it's kind-of an odd effect. If this is what you intended, then disregard this comment.

10.2.1, table 3: Smae comment as above for 10.1.

10.3.1, comment box: I think the right term here is working state. What am I missing?

10.3.1, table 4, same comment as above for 10.1

10.4.3, title (among other places): We can't call this a block cipher hash, or readers will think we're proposing it for the hash-based DRBGs, or for general-purpose hashing. Let's call it the "block cipher accumulator" instead.

11, general comment: This ignores all the stat testing for the entropy source. I recognize we don't really have much of that, but I expect real world systems will end up doing a lot more work there than on the known-answer tests.

11.1, 7th bullet point: Whether the CTR_DRBG implementation uses a derivation function is all inside the DRBG mechanism. Is it still something that needs to be documented?

C.2, 5th para (2nd from top on page 86): In this paragraph, we seem to use "conditioning" to mean both any processing of the digitized noise source values that makes them more uniform, and to producing full entropy outputs.

C.3, last para: "uncorrelated" should be "independent"

D.1, item c: Can we use the term "approved entropy source?"

D.1, item d: This is the most baffling paragraph I've ever read, and yet I think I understand it. We have got to come up with better terms for this stuff.

D.1, item d: "entropy resource" should be "entropy source"

D.3: I agree with your comment, let's kill the whole of D.3.

G, item b, second para: "Since the security of the DRBG is...." should be "Since the security of the module is...."

G, item c: We should add an example here for symmetry with the other two items, like "For example, a module with both hash and block cipher support might choose the CTR_DRBG, if it needed the ability to parallelize the generation of random bits."

G.4, whole discussion: In the text, R and S should be lowercase,

because we're talking about scalar quantities. That's how they're written in the text description of the Dual EC DRBG.

G.4, 3rd para: "all three of the NIST-Approved...." Is this still accurate? I thought Certicom was trying to get us to include all of them in there. (I think at least part of this was to get some of the curves not covered by the NSA license into the standard.)

G.4, 4th para (second para on page 125): "...to generate truly high-security random numbers" should become "...to generate random numbers". We hope all our DRBGs are high security!