Part 3 Mechanisms

June 22, 2005

Elaine Barker
NIST

changes

d Definitions):

tions changed to match Part

be discussed:

Appl
Entropy
Full entropy
Instantiation of an RBG
Random Bit Generator
Security Strength
Seed
Statistically Unique
Supporting Functions

(Contd.)

- Instantiations):
  - about multiple
- Boundaries):
  - Distributed boundaries
    - Generate function not required with Instantiate or Reseed functions (not precluded, though)
    - Uninstantiate function in all sub-boundaries

(contd.)

- ration and Handling
  - moved here
  - *ity_strength*/2
- Section 8.6 (Prediction and Backtracking Resistance):
  - Description of backtracking method simplified

s (Contd.)

Discussion):

hat Get_entropy and
tions could be defined

- Section (instantiating a DRBG):
  - If generate function is present, generate bits to check successive internal states (steps 12 & 13)
  - Added a note that if the nonce is a random value, can be acquired with the entropy input

s (Contd.)

...):

...checks that 2 consecutive states

..., uninstantiate all instantiations

(SFP

- Section 9.4 (Generate...):
  - Same changes as 9.3
  - Expanded text re prediction resistance
  - Expanded text re mods. when reseed not available

...s (Contd.)

...m of Self Testing):
...test a function and configuration

...sting the Instantiate

Function
- Test before creating an operational instantiation using given parameters
- Perform known-answer tests
- Test error handling
- On-demand testing recommended

(Contd.)

- ng the Generate
- and periodically
- ut until the function is tested
- "Periodic" depends on the environment
- Perform known-answer tests on input parameters
- Test error handling
- On-demand testing recommended

s (Contd.)

ne Reseed Function):

Strength of the state to be

nswer tests

- Te[illegible]andling
- If prediction resistance available, test when the generate function is tested
- If prediction resistance not available, test before reseeding
- On-demand testing is recommended

s (Contd.)

- ng the Uninstantiate
- ther functions are tested
- test error handling

s (Contd.)

- Algorithm
- 57 for security strengths;
- to ANSI document
- Added tests to the reseed and genrate algs. To compare successive states.

To Do List

- [illegible] maintaining security
- [illegible] Considerations):
  - [illegible] following?
    - C.1 (Security of Hash Functions)
    - C.2 (Algorithm and Key Size Selection)
- Annex D (Functional Requirements): Remove or retain?

ist (Contd.)

- ction): Summarize
  ion-retained DRBGs
- ples): Revise for retained
  DRBGs

Which DRBGs to retain?

- [illegible]HA-x)
- [illegible] AES)
- [illegible]EA, AES)
- Dual_EC_DRBG (4 Prime Field Curves: P-224, P-256, P- 384, P-521)

- Remove:
  - Hash_DRBG
  - Dual_EC_DRBG (Non-prime field curves)
  - MS_DRBG