X9.82, Part 3
DRBG Mechanisms

June 22, 2005

Elaine Barker
NIST

Latest Changes

Section 4 (Terms and Definitions):

- Several definitions changed to match Part 1
- Definitions to be discussed:
  - Approved
  - Entropy
  - Full entropy
  - Instantiation of an RBG
  - Random Bit Generator
  - Security Strength
  - Seed
  - Statistically Unique
  - Supporting Functions

Changes (Contd.)

- Section 8.2.2 (DRBG Instantiations): Removed text about multiple instantiations
- Section 8.3 (DRBG Boundaries): Distributed boundaries
  - Generate function not required with Instantiate or Reseed functions (not precluded, though)
  - Uninstantiate function in all sub-boundaries

Changes (contd.)

- Section 8.4.2 (Generation and Handling of Seeds):
  - Nonce section moved here
  - 64 → *security_strength*/2
- Section 8.6 (Prediction and Backtracking Resistance):
  - Description of backtracking method simplified

Changes (Contd.)

- Section 9.1 (General Discussion):
  - Inserted a note that Get_entropy and Block_Encrypt functions could be defined differently
- Section 9.2 (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

Changes (Contd.)

- Section 9.3 (Reseeding…):
  - Each DRBG alg. checks that 2 consecutive states are different
  - If 2 states equal, uninstantiate all instantiations (step 6)
- Section 9.4 (Generate…):
  - Same changes as 9.3
  - Expanded text re prediction resistance
  - Expanded text re mods. when reseed not available

Changes (Contd.)

- Section 9.7.1 (Discussion of Self Testing):
  - Simplified – just test a function and configuration before using it
- Section 9.7.2 (Testing the Instantiate Function)
  - Test before creating an operational instantiation using given parameters
  - Perform known-answer tests
  - Test error handling
  - On-demand testing recommended

Changes (Contd.)

Section 9.7.3 (Testing the Generate Function):

- Test at power-up and periodically
- No bits output until the function is tested
- "Periodic" depends on the environment
- Perform known-answer tests on input parameters
- Test error handling
- On-demand testing recommended

Changes (Contd.)

Section 9.7.4 (Testing the Reseed Function):

- Test the *security_strength* of the state to be reseeded
- Perform know-answer tests
- Test error-handling
- If prediction resistance available, test when the generate function is tested
- If prediction resistance not available, test before reseeding
- On-demand testing is recommended

Changes (Contd.)

Section 9.7.5 (Testing the Uninstantiate Function):

- Test whenever other functions are tested
- If possible, test error handling

Changes (Contd.)

Section 10 (DRBG Algorithm Specifications):

- Points to SP 800-57 for security strengths; need pointer to ANSI document
- Added tests to the reseed and genrate algs. To compare successive states.

To Do List

- ANSI document containing security strengths
- Annex C (Security Considerations): Remove the following?
  - C.1 (Security of Hash Functions)
  - C.2 (Algorithm and Key Size Selection)
- Annex D (Functional Requirements): Remove or retain?

To Do List (Contd.)

- Annex E (DRBG Selection): Summarize and remove non-retained DRBGs
- Annex F (Examples): Revise for retained DRBGs

The Biggie: Which DRBGs to retain?

- Recommendation:
  - HMAC_DRBG (SHA-x)
  - CTR_DRBG (TDEA, AES)
  - OFB_DRBG (TDEA, 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