DRBG Issues

Tuesday, July 20, 2004

Elaine Barker and John Kelsey

Operational and Validation Testing

- Is the approach in Section 9.9 reasonable for known answer testing?
- How many strings should be requested during testing and of what length?
- How should error handling be tested?
- When errors are found during testing, what kind of recovery advice or restrictions should be provided?
- How should errors found during normal operation be handles?
- Other issues?

DRBG Design and Handling

- DRBG boundaries
- DRBG boundaries in relation to cryptomodule boundaries
- Internal state handling
- Seed handling
- Is a security parameter of 2^{64} appropriate?
- Collision resistance?

DRBG Design and Handling (contd.)

- DRBG processes:
  - Instantiation
  - Generation
  - Reseeding
  - Uninstantiation
- Assurance

DRBG Design and Handling (contd.)

- Hash-based DRBGs
  - How many DRBGs of each type
  - Hash_DRBG
  - HMAC_DRBG
  - KHF_DRBG

DRBG Design and Handling (contd.)

- Block Cipher-based DRBGs
  - CTR_DRBG
  - OFB_DRBG

DRBG Design and Handling (contd.)

- Number theory-based DRBGs
  - Dual_EC_DRBG
  - MS_DRBG
    - Should sample moduli be provided in the Standard (e.g., for testing)?
    - Should the factorization information be provided with the test vectors?