Selection of Future Cipher Standards

`draft-mcgrew-standby-cipher-00`

McGrew, Sheffer, Grieco

IRTF CFRG @ IETF 87 Berlin
July 29, 2013

Problems

- Current standards rely on the security of a single cipher (AES)
  - 3DES insufficient for high data rates
  - An exploitable flaw is unlikely, but would be catastrophic
- Many alternative cipher proposals
  - Camellia, SEED, ARIA, SMS4, Salsa20, RC4, …
- Standards should not proliferate ciphers
  - Costs: policy, interoperability, implementation, validation, ...

Standby Cipher

- For use in case of the possibility that future advances in cryptanalysis might uncover security issues with the current global standard cipher
- Implementation of the standby cipher should not be required, but could be RECOMMENDED for implementation by security protocol standards

(AES) Evalutation Criteria

- Security
- Computational efficiency
- Memory requirements
- Hardware and software suitability
- Simplicity
- Flexibility
- Licensing requirements; it should be available worldwide on a royalty-free basis.

Other Criteria

- It should have a design that is as independent of that of the AES as is possible, so that advances in cryptanalysis that lower the effective security of one design have as little effect as possible on the other one
- It should also perform well on existing hardware that is optimized for AES implementation

Proposed Action

- CFRG should
  - document the need for a standby cipher (if that is the consensus)
  - Document the evaluation criteria
  - Provide input to the cryptographic community
- Open Question:
  - How would a standby block cipher fit into the overall picture of modes, authenticated encryption, and ciphersuites?