Update on Symmetric Key Transport and Group Key Management

mcgrew@cisco.com

IETF 78

Recap

- Multicast requires symmetric key transport
- Should MSEC protocols use Key Wrap?
  - RFC 3394 *Advanced Encryption Standard (AES) Key Wrap Algorithm*
  - RFC 5649 *Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm*
- Key Wrap does not match GDOI data model
  - No good combinations

Update

- Decision: Key Wrap is not needed/suitable
- GDOI 'Key Wrap' allowed by NIST FIPS-140
  - Thanks to Tim and his NIST colleagues!
  - SP 800-131 Draft 2, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths*
  - *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*
- New NIST key wrap guidance is expected
  - Other algorithms may be allowed
  - Will forward information to MSEC as available

Going Forward

- MSEC should coordinate with NIST
  - No urgent issues, but alignment desirable
- Areas of interest
  - Key Transport (Protocols)
  - Key Wrap Algorithms