EMC²
where information lives®

# IKEv2-SCSI (06-449) Update

**David L. Black**

EMC² where information lives®

# IKEv2-SCSI (06-449) Plans and Status

- Plan
  - Revise IKEv2-SCSI draft for approval at this meeting
- Reality
  - The best laid schemes o' Mice an' Men ... gang aft FCoE !!
  - More info: Friday T11 FC-BB-5 meeting
- Status
  - Significant IKEv2-SCSI editing has been accomplished
  - Editors and reviewers found a few important issues
- This presentation: A few important issues
  - Decisions that must be made to finish IKEv2 SCSI
  - Hope: Settle these now, ask for document approval in September

EMC² where information lives®

# Combined Modes

- Mode = How to use an encryption cipher
  - E.g., CBC = Cipher Block Chaining (e.g., AES-CBC, 3DES-CBC)
- Combined mode: encryption + cryptographic integrity
  - One cryptographic mechanism does two jobs with one key
  - Example: GCM = Galois Counter Mode
  - Combined modes generating a lot of interest
- IKEv2-SCSI needs additional text for combined modes
  - Proposal: support both conventional (e.g., CBC) and combined (e.g., GCM) modes
  - Alternative: Only support combined modes (e.g., GCM)
    - Second combined mode: CCM = Counter with CBC-MAC

EMC² where information lives®

# Cryptographic Algorithm Negotiation

- IKEv2-SCSI negotiates cryptographic algorithms
  - Secure negotiation, signed and linked to Authentication
  - IKEv2-SCSI Authentication step requires encryption
- SA users (e.g., SSC-3) need crypto alg. negotiation
  - Would like to use IKEv2-SCSI's rather than invent their own
  - Works fine when all the same algorithms are used twice.
  - What if they're not? E.g., How can encryption be omitted?
- Possibility: Second round of negotiation
  - Key Exchange phase (first) negotiates IKEv2-SCSI algorithms
  - Authentication phase (second) negotiates SA usage algorithms
  - Complication: SA_AUTH_NONE: SA usage algorithms negotiated in Key Exchange phase (details to be worked out).
- Q: Should this be done?

EMC² where information lives

# Mandatory Algorithms (Tarpit warning)

- General: Common requirements for SBC and SSC devices
  - Avoid per-usage requirements.
- Cryptography I: Recommend no mandatory elliptic curve
  - Intellectual Property concerns: leave in specification as optional
- Cryptography II: Start with 128 bit AES
  - Encryption + Integrity: choose one:
    - **AES-CBC + [HMAC-SHA1_96 (96 bits)** or HMAC-SHA2_256_128 (128 bits)] or
    - AES-GCM + AUTH_COMBINED
  - PRF: IKEv2 based on **SHA1** (160 bits) or SHA2_256
  - D-H group: choose 1
    - **2048 bit mod-p** (~ 100 bits) or 3072 bit mod-p (~ 125 bits)
    - Q: Leave 4096 bit mod-p group in specification?
  - Prohibit SHA2_384 HMAC and PRF for simplicity
    - 192 bit AES already prohibited

EMC² where information lives®

# Mandatory Authentication Mechanisms (Bigger tarpit)

- Mandatory SA_AUTH_NONE - security disaster
  - But, inband device initialization is a concern
- Primary decision: RSA keys vs. shared secret keys
  - RSA Initialization: Public key via any means
    - E.g., label on device and sneaker-net are both secure.
  - Shared secret key (SKMIC) Initialization: Keep the key secret
    - If installed at factory, need secure key management infrastructure.
- 2.5 possibilities
  - RSA mandatory for app client and device server
    - Certificates optional, but may want to mandate certificate verification logic
  - SKMIC mandatory for app client and device server
    - Possible addition (+0.5): SA_AUTH_NONE with physical presence required
    - For device initialization (no design work done on this, yet)


EMC²
where information lives®