IEEE Security in Storage Workgroup (P1619.x) Status to T10

Matt Ball, SISWG Chair

May 6, 2008

P1619 “Disk encryption” and P1619.1 “Tape encryption”

- IEEE std 1619-2007 has been published and is now waiting for the IEEE store to make it available for purchase.
- IEEE std 1619.1-2007 will be published within the next couple weeks.
- IEEE-SA has agreed to submit the XTS-AES portion of IEEE 1619-2007 to NIST for consideration as an Approved Mode of Operation for FIPS 140-2. This process should start before the end of May, and will be open for 90-days

P1619.2 “Wide block encryption”

- Last face-to-face meeting held in San Jose on May 5th, 2008
- Both XCB and EME2 are in a P1619.2 draft. The group is now working through minor edits
- Next meeting on June 17th. Task group letter ballot will start shortly afterwards.
- Submit to IEEE Feb 2009
- Publication by middle of 2009

P1619.3 “Key Management Services”

- Latest draft P1619.3/D3 includes work from the Architecture and NameSpace subcommittees.
- Current focus is on Objects and Operations
- Next focus is the Messaging and Transport work
- Face-to-face in Anchorage canceled in favor of weekly teleconference meetings on Wednesdays at 10:00 Pacific Time

Key Management Summit
KMS 2008

- IEEE is sponsoring a Key Management Summit.
- There is a call for presentations and sponsors that ends May 30th, 2008
- Sponsorship is $1000 for 1 free pass, a vendor speaking slot, and logo on front page
- The Summit will be on Sept 23-24, 2008 in Baltimore, MD
- See http://www.keymanagementsummit.com/2008 for more information.

Who should attend KMS 2008

- The Key Management Summit focuses more on the technical issues of key management, and is more suitable to those with a technical background. Prime candidates include:
  - Chief Technical Officers (CTO)
  - Chief Security Officers (CSO)
  - Technical Advisors
  - Security Consultants
  - Security Engineers
  - Standards Developers

KMS 2008 Tuesday (Proposed)

- **8:00 am - 9:00** **Breakfast and Registration**
- **9:00 am – 5:00 pm:**
- Welcome from the chair
- (Proposal) NIST key management standards
- (Proposal) NSA
- (Proposal) Key Management using IEEE P1619.3
- (Proposal) Key Management using OASIS EKMI's SKSML
- (Proposal) Key Management using IETF KEYPROV
- **5:00 pm - 7:00 pm** Dinner
- **7:00 pm - 10:00 pm** Social hour

KMS 2008 Wednesday (Proposed)

- 8:00 am - 8:30 am:
  - Breakfast and Registration
- 8:30 am - 12:00 pm:
  - Industry Use-Cases and Requirements
- 1:00 pm - 5:00 pm:
  - Vendor Key Management Solutions