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

Matt Ball, SISWG Chair

July 30, 2008

P1619 "Disk encryption" and P1619.1 "Tape encryption"

- IEEE Std 1619-2007 (XTS) and IEEE Std 1619.1-2007 (Tape encryption) are now available for purchase at the IEEE store

- IEEE has released an excerpt of IEEE 1619-2007 to describe the XTS-AES encryption mode. During this time, NIST is requesting public comments while considering XTS as an Approved Mode of Operation under FIPS 140-2. The public comment period began June 5, 2008, and will be open for 90 days

  - (See http://csrc.nist.gov/groups/ST/documents/Request-for-Public-Comment-on_XTS.pdf)

◆IEEE

P1619.2 "Wide block encryption"

- Last face-to-face meeting held in San Jose on July 29, 2008
- P1619.2 will shortly start working group ballot
- Submit to IEEE Feb 2009
- Publication by middle of 2009

◆IEEE

P1619.3 "Key Management Services"

- Walt Hubis of LSI Logic appointed as new task group chair.

- Latest draft P1619.3/D4 includes work from the Objects and Operations Subcommittee.

- The group is cleaning up some of the Operations

- The group has a matrix comparing different transport options (e.g., XML variants vs. Binary variants), but there is no clear option preferred by the working group.

SISWG Plenary

- The Security in Storage Working Group has started holding plenary sessions again.

- The last plenary was July 30th, 2008 in San Jose.

- Membership is now only counted at the working group level, not the task group level (e.g., P1619.2, .3).

- New Operating Procedures have been proposed and will be voted on shortly

- Next meeting will be on Sept 26th in Baltimore

◆IEEE

IEEE Key Management Summit (KMS 2008)

- KMS 2008 will be on Sept 23-24, 2008 in Baltimore, MD and is co-located with the Mass Storage Systems and Technologies symposium (MSST) and the Security in Storage Workshop (SISW).

- See http://www.keymanagementsummit.com/2008 for more information.

◆IEEE

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

◈IEEE

Miscellaneous Info

- SISWG Letter ballot about to start for modifying the Operating Procedures
- URL for siswg: http://www.siswg.net
- Upcoming SISWG F2F meeting in Baltimore, MD: Sept 26, 2008, 9:00 – noon PT.

◆IEEE