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

Matt Ball

Quantum, Corp.

March 13, 2007

Work group overview

- The IEEE SISWG is working on standards that relate to cryptographic protection of stored data.
- Official Homepage: http://www.siswg.org
- Working Homepage: http://ieee-p1619.wetpaint.com/
- E-mail archive: http://grouper.ieee.org/groups/1619/email/
- Membership is open to anyone who attends two meetings a year (no membership fee).

SISWG subgroups

- P1619: Narrow-block encryption with fixed size (including XML key backup format)
- P1619.1: Authenticated encryption with length expansion for storage media
- P1619.2: Wide-Block encryption
- P1619.3: (newly approved) Key management infrastructure for cryptographic protection of stored data

P1619 Status

- P1619 recently finished reviewing workgroup letter-ballot comments.
- Latest Draft is P1619/D13
- Group is starting to form sponsor ballot pool.
- Based on workgroup vote from January, P1619 will submit a new PAR to match the title, scope, and purpose.

P1619.1 Status

- This standard specifies authenticated encryption using AES-GCM, AES-CCM, CBC-HMAC, and XTS-HMAC modes.
- Latest draft: D17
- Working group recently completed a workgroup ballot and is now going through letter-ballot comments
- Goal to submit final draft to IEEE before August 17th, 2007 RevCom deadline for September.

P1619.2 Status

- The group voted to start work on three wide-block encryption modes:
  - XCB (David McGrew)
  - EME* (Hal Finney)
  - TET (Shai Halevi)
- Charlie Martin appointed as technical editor
- Many of these modes have patent claims.
- Goal is to finish by February 2008.

P1619.3 Status

- IEEE has recently approved the Project Authorization Form (PAR) for P1619.3.
- This work group will handle key management infrastructure for cryptographic protection of stored data
- Final solution will likely require coordination with SSC-3 (or 4) to standardize entry of encrypted keys (stay tuned…)