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

May 8, 2007

IEEE

SISWG 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 for a particular standard (no membership fee).
- New Officers:
  - Matt Ball, Quantum – Chair
  - Eric Hibbard, Hitachi Data Systems – Vice Chair
  - Fabio Maino, Cisco - Secretary

IEEE

SISWG Task Groups and Subcommittees

- 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: Key management infrastructure for cryptographic protection of stored data
- Operating Procedures Subcommittee

P1619 Status

- P1619 specifies the XTS-AES encryption algorithm with an XML-based key backup format
- P1619 recently finished reviewing workgroup letter-ballot comments.
- Latest Draft is P1619/D14
- Group is starting to form sponsor ballot pool.
- New PAR has been submitted and should be approved shortly

P1619.1 Status

- This standard specifies authenticated encryption using GCM, CCM, CBC-HMAC, and XTS-HMAC modes.
- Latest draft: P1619.1/D19
- First working group ballot finished and we will soon start a second one.
- Goal to submit final draft to IEEE before August 17th, 2007 RevCom deadline for September.
- Removed Key-Transform, interchange format (Annex D), and authenticate-only mode

P1619.2 Status

- The group voted to start work on three wide-block encryption modes:
  - XCB
  - EME*
  - TET
- Currently integrating XCB into P1619.2/D1.
- Goal is to finish by February 2008.

P1619.3 Status

- This work group will handle key management infrastructure for cryptographic protection of stored data
- The group will use the straw man proposal from Decru for the first draft
- Bob Lockhart of NeoScale appointed as technical editor
- The group is also producing a use-case white paper