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

Matt Ball, SISWG Chair

Quantum, Corp.

July 10, 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 Task Groups

- 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

P1619 Status

- P1619 currently specifies the XTS-AES encryption mode and an XML-based key backup format.
- P1619 has entered Sponsor Ballot. Sponsor ballot ends on August 9, 2007
- Latest Draft is P1619/D17 (July 1, 2007)
- We are aiming to submit a final draft to IEEE before the August 17th deadline.

P1619.1 Status

- This standard specifies authenticated encryption using AES-GCM, AES-CCM, CBC-HMAC, and XTS-HMAC modes.
- We recently completed a second working group ballot.
- Latest draft: P1619.1/D21 (June 17)
- We will start a Sponsor Ballot Invitation within the next week or so
- Goal to submit final draft to IEEE before October 15th, 2007 RevCom deadline

P1619.2 Status

- The group voted to start work on three wide-block encryption modes:
  - XCB (David McGrew)
  - EME* (Hal Finney)
  - TET (Shai Halevi)
- Latest draft: P1619.2/D0 (Mar 6, 2007)
- No progress to report since May

P1619.3 Status

- P1619.3 is focusing on key management services.
- Latest draft: P1619.3/D1 (May 23, 2007)
- Current draft uses XML-SOAP for key management API.
- We are soliciting Use-Cases
- We are also creating a key identifier format.