IEEE Security in Storage Workgroup (P1619) Status to T10

Matt Ball

Quantum, Corp.

November, 7, 2006

Work group overview

- Officers
  - Chair: Jim Hughes (Sun Microsystems)
  - Vice-chair: Serge Plotkin (Stanford)
  - Secretary: Fabio Maino (Cisco)
  - Sponsor Chair: Jack Cole (U.S. Army)
- Homepage: http://ieee-p1619.wetpaint.com/
- E-mail archive: http://grouper.ieee.org/groups/1619/email/

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 (newly approved)

P1619 Status

- Workgroup has dropped the AES-LRW mode and replaced it with AES-XEX
  - AES-LRW mode has a vulnerability when key 2 is encrypted on the medium.
- Latest Draft is D8:

  http://grouper.ieee.org/groups/1619/email/pdf00038.pdf
- Group is starting to form letter ballot pool
- Next meeting: Monday, November 20th, and face-to-face Dec 6th in conjunction with T11.

P1619.1 Status

- This standard specifies authenticated encryption using AES-GCM and AES-CCM modes.
- Latest draft: D12

  http://grouper.ieee.org/groups/1619/email/bin00079.bin
- We are starting to form a letter-ballot pool
- Goal is to submit draft for letter ballot before the end of the year

P1619.2 Status

- IEEE recently approved PAR (project authorization form)
- The group is evaluating candidates for wide-block encryption:
  - XCB (David McGrew)
  - EME* (Shai Halevi)
  - PEP (Chakraborty, Sarkar)
  - HCTR (Wang, Feng)
- Many of these modes are covered by patents
- Group agreed to not include message integrity for this draft
- Next meeting: Dec 12th from 9-12 pacific time