IEEE Security in Storage Workgroup (P1619) Status to T10

Matt Ball

Quantum, Corp.

January 16, 2007

Work group overview

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

SISWG Officer Election

- The Security in Storage workgroup is currently holding an election for the positions of chair, vice chair, and secretary.
- Submit nominations to Jack Cole.
- Candidates must be members of IEEE-SA, be willing to run if nominated, and willing to serve if elected. There are no other requirements.

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 proposed) Key management infrastructure for cryptographic protection of stored data

P1619 Status

- P1619 recently finished a 30-day work group letter ballot with an affirmative vote to advance to sponsor ballot.
- Latest Draft is D11: http://grouper.ieee.org/groups/1619/email/pdf00046.pdf
- Group is starting to form sponsor ballot pool
- Stretch goal to submit final draft to IEEE before April 27th RevCom deadline for June.

P1619.1 Status

- This standard specifies authenticated encryption using AES-GCM and AES-CCM modes.
- Latest draft: D14 (see http://ieee-p1619.wetpaint.com/page/SISWG+Standards)
- Working group voted to start 30-day workgroup ballot with D15 (to be published).
- Stretch goal to submit final draft to IEEE before April 27th RevCom deadline for June.

P1619.2 Status

- The group voted to start work on three wide-block encryption modes:
  - XCB (David McGrew)
  - EME* (Shai Halevi)
  - TET (Shai Halevi)
- We need a technical editor
- Goal is to finish by February 2008, assuming we get an editor.

Key Management Subcommittee

- SISWG recently formed the Key Management subcommittee to create a project authorization form (PAR) for key management services as it relates to stored data (tentatively called P1619.3).
- This group has produced a PAR that will undergo review and will be submitted to IEEE before January 22, 2007.

P1619.3 PAR proposal

- Title:
  Draft Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data
- Scope:
  This standard specifies an architecture for the key management infrastructure for cryptographic protection of stored data, describing interfaces, methods and algorithms.
- Purpose:
  This standard defines methods for the storage, management, and distribution of cryptographic keys used for the protection of stored data. This standard augments existing key management methodologies to address issues specific to cryptographic protection of stored data. This includes stored data protected by compliant implementations of other standards in the IEEE 1619 family.