Quantum

IEEE 1619/1619.1 Status Report to T10

Matt Ball

July 11, 2006

General

- The Security in Storage workgroup has setup an active web page, or ‘Wiki’, as a homepage. See http://ieee-p1619.wetpaint.com/.
- Original SIS homepage is at http://www.siswg.org.
- Email archive is at http://grouper.ieee.org/groups/1619/email/
- Meetings are open to the public

IEEE P1619 (LRW)

- The P1619 standard proposes to standardize the AES-LRW encryption mode and an XML-based key backup format
- Latest Draft: P1619-D5 (see http://grouper.ieee.org/groups/1619/email/pdf00033.pdf)
- Last meeting was June 20th
- The working group is attempting to resolve several comments (see minutes from Wiki)
- The next P1619 meeting will be July 20th, from 8-10 AM, PDT (hosted by Sun).

IEEE 1619 Recent Changes

- IEEE editors have provided comments
- SISWG is mostly making editorial changes in preparation for letter ballot.
- Proposal to add a subtitle “Length Preserving Encryption Mode” – Possibly requires new PAR
- Questions surrounding use of AES-LRW in a FIPS 140-2 solution.

IEEE P1619.1 (GCM/CCM)

- P1619.1 standardizes the GCM and CCM authenticated encryption modes for use in storage devices
- Latest draft: P1619.1-D8 (see http://grouper.ieee.org/groups/1619/email/bin00047.bin and rename to P1619_1-D8.pdf)
- Last meeting on May 23rd, 2006
- Next meeting on July 19th, 2006 from 9 am to noon, PDT.

IEEE 1619.1 Recent Changes

- Proposal to change the title to “Draft Standard for Encrypted Storage with Authentication and Length Expansion” – change requires new PAR (Project Authorization Request)
- Requirement for always using a 96-bit random number when creating the IV (initialization vector)
- Requirement to define an IVDF (IV derivation function)
- Updated test vectors for GCM and CCM