Request for Public Comment on XTS

The P1619 Task Group of the Security in Storage Working Group (SISWG) of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) has submitted the XTS-AES algorithm (XTS, for short) to NIST as an encryption mode of operation of the Advanced Encryption Standard (AES) block cipher. Although XTS does not provide authentication in order to avoid expansion of the data, it is designed to provide some protection against malicious manipulation of the encrypted data. Subject to the 90-day period of public comment that is described below, NIST proposes to approve XTS for government use under the auspices of FIPS Pub. 140-2.

XTS is specified in IEEE Std 1619-2007. IEEE has agreed to make a relevant extract from this standard available for free during the period of public comment. NIST proposes to approve the specification by reference to IEEE Std 1619-2007, while reserving the right to specify additional requirements/restrictions on XTS for government use. After the period of public comment, the standard would be available for purchase from IEEE for $85 to IEEE members and affiliates, and $105 to non-members.

The chair of the SISWG informed NIST that he is unaware of any patent claims on XTS, but that NeoScale Systems, subsequently acquired by nCipher, submitted a Letter of Assurance of Essential Patents to the IEEE, without elaborating on what aspect of IEEE 1619 was patented.

The period of public comment for this proposal is from June 5, 2008 to September 3, 2008. The extract of IEEE Std 1619-2007 is available for free during this period at http://grouper.ieee.org/groups/1619tmp/1619-2007-NIST-Submission.pdf. Comments may be submitted to EncryptionModes@nist.gov. NIST particularly invites comments on the following topics:

- The XTS algorithm itself;
- The depth of support in the storage industry for which it was designed;
- The appeal of XTS for wider applications;
- The proposal for the approved specification to be available only by purchase from IEEE;
- Concerns of intellectual property rights.