Public Comments on the August, 2009 Draft of Special Publication 800-38E

This document contains the public comments that NIST received on the August, 2009 draft of Special Publication 800-38E: *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality in Block-Oriented Storage Devices.* The 30-day comment period ended on September 17, 2009.

Matt Ball

Dear NIST,

As chair of the IEEE P1619 Security in Storage Working Group, I thank you for accepting XTS-AES as defined in IEEE Std 1619-2009 as an approved mode of operation. This IEEE standard is the product of years of work by many skilled cryptographers, and, while not ideal in all cases, provides an excellent mode for unauthenticated narrow-block encryption. The addition of Cipher Text Stealing, in particular, will help with several implementations that up until now were forced to use unwanted padding in a FIPS-certified solution.

I've reviewed draft SP 800-38E, and the normative content looks correct.

Thanks again!

Sincerely,

Matt Ball

Alexandr Mazuruc

Dear members of NIST team,

As a vendor of the disk encryption software we are pleased to see the IEEE Std 1619-2007 standard being accepted by NIST/CSEC. Our product is currently certified for FIPS 140-2 Level 1 and 2 and we plan to include this mode in our certified cryptographic module. This initiative will allow us to maintain FIPS certification in future without any problem.

Being aware about coming SP we made a comment to the Protection Profile for Full Disk Encryption which NIAP/CCEVS are currently developing stating that it would be beneficial to have XTS as an approved encryption mode in the profile.

Regards,

Alexandr Mazuruc,
Senior Software Developer
WinMagic Data Security,

The Department of Energy
Office of the ACIO for Cyber Security

#1
Type: G
Reference: Page 4, section 2, 2nd paragraph, 1st sentence
Comment (Include rationale for comment): Attempt at a more accurate statement of FISMA requirement. The standards and guidelines may be applied to NSSs but they are not required to be applied. As stated, no one is allowed to apply them to NSSs.
Suggested change: NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets for non-national security systems~~, but such standards and guidelines shall not apply to national security systems~~.
#2
Type: G
Reference: Page 4, section 3, 1st paragraph, 3rd sentence
Comment (Include rationale for comment): Approving technical standards through the use of a "guideline" does not seem adequate. Approval of another organizations standard should be done through the publication of a FIPS related to the original FIPS. As stated, the "approval" is no more than a guideline ("Recommendation") and the conformance section is not required to be implemented for compliance with FIPS 197 or any other standard.
#3
Type: G
Reference: Page 5, section 4, 2nd paragraph, 2nd sentence
Comment (Include rationale for comment): It should be noted that this publication also does not require the limitation of 2^{20} blocks since it is a guideline. This would need to be published in a FIPS approved by the Secretary of Commerce to be a requirement.
#4
Type: G
Reference: Page 6, section 5, 4th paragraph, 1st sentence
Comment (Include rationale for comment): The alternative ordering may not be permitted through a guideline if it is non-compliant with the FIPS.
#5
Type: E
Reference: Section 2, 2nd paragraph
Comment (Include rationale for comment): This approach does not forbid the use of these standards and guidelines from being used by National Security Systems. As written they were forbidden from being used by NSS
Suggested change: NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, ~~but~~ and such standards and guidelines shall ~~not~~ apply to non-national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III

Russ Housley

I would prefer a write up that does not require an implementor to purchase the IEEE document.