NIST Special Publication 800-38E
DRAFT
August 2009

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices

Morris Dworkin

COMPUTER SECURITY

Abstract

This document approves the XTS-AES mode of the AES algorithm by reference to IEEE Std 1619-2007, subject to one additional requirement, as an option for protecting the confidentiality of data on block-oriented storage devices. The mode does not provide authentication of the data or its source.

KEY WORDS: block cipher; confidentiality; cryptography; information security.

TABLE OF CONTENTS

1 Purpose

This publication is the fifth Part in a series of Recommendations regarding modes of operation of symmetric key block ciphers.

2 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to 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.

This Recommendation has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Conformance testing for implementations of the mode of operation that is referenced in this Recommendation will be conducted within the framework of the Cryptographic Module Validation Program (CMVP), a joint effort of NIST and the Communications Security Establishment Canada. An implementation must adhere to the requirements in the specification and in this Recommendation in order to be validated under the CMVP. The requirements in both documents are indicated by the word "shall."

3 Introduction

The XTS-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES) [1] algorithm. The Security in Storage Working Group (SISWG) of the P1619 Task Group of the Institute of Electrical and Electronics Engineers, Inc (IEEE), developed and specified XTS-AES in IEEE Std. 1619-2007 [2]. This Recommendation approves the XTS-AES mode as specified in that standard, subject to one additional requirement on the lengths of the data units, discussed in Section 4 below.

The XTS-AES mode was designed for the cryptographic protection of data on block-oriented storage devices. Note that other approved cryptographic algorithms continue to be approved for such devices. The XTS-AES mode was not designed for other purposes, such as the encryption of data in transit.

The XTS-AES mode is an instantiation of Rogaway's XEX (XOR Encrypt XOR) tweakable block cipher [3], supplemented with a method called "ciphertext stealing" to extend the domain of possible input data strings. In particular, XEX can only encrypt sequences of *complete* blocks, i.e., any data string that is an integer multiple of 128 bits; XTS-AES can encrypt *any* string alignment of 128 or more bits. (The acronym XTS stands for the **X**EX **T**weakable Block Cipher with Ciphertext **S**tealing).

The specification of the ciphertext stealing method in [2] includes an ordering convention for the final two elements of the encrypted data string: one complete block and one partial block. A different convention, in which the order of these two elements is swapped, may be desirable in some cases. There is flexibility in the physical location of these elements, as long as interoperability is not compromised, as discussed in Section 5.

The XTS-AES mode provides confidentiality for the protected data. Authentication is not provided, because the P1619 Task Group designed XTS-AES to provide encryption without data expansion, so alternative cryptographic methods that incorporate an authentication tag are precluded. The rationale for this design choice and the ramifications for the incorporation of XTS-AES into an information system are discussed in Annex D of [2]. Prospective implementers of XTS-AES should consider this information carefully to ensure that XTS-AES is an appropriate solution for a given threat model.

4 Conformance

An instance of an XTS-AES implementation is defined by the following three elements, as specified in [2]:

1) a secret key,
2) a single, fixed length for the data units that the key protects,
3) an implementation the XTS-AES-Enc procedure or the XTS-AES-Dec procedure, or both, for the key and the length of the data units

The length of the data unit for any instance of an implementation of XTS-AES shall not exceed 2^{20} blocks. Note that Section 5.1 of [2] recommends this limit but does not require it.

An implementation of the XTS-AES encryption mode may claim conformance with this Recommendation if every supported instance satisfies this requirement, in addition to all of the applicable requirements in [2].

Consistent with the 2^{20} block limit, an implementation of XTS-AES may further restrict the length of the data units for any key, as long as at least one instance can be supported. For example, an implementation may support only data units that are sequences of *complete* blocks. In this case, the ciphertext stealing components in the implementations of the XTS-AES-Enc and the XTS-AES-Dec procedures would be unnecessary, and these procedures essentially would be reduced to the XTS-AES-blockEnc and the XTS-AES-blockDec procedures, as specified in [2].

Similarly, an implementation may support either the 256-bit key size (for XTS-AES-128) or the 512-bit key size (for XTS-AES-256), or both.

Restrictions on the supported lengths of the key or the data units may affect interoperability with other implementations.

5 Ordering Convention for the Ciphertext Stealing Case

If the length of the data units for an instance of XTS-AES is not an integral multiple of the block size, then the specification in [2] denotes the unencrypted form of a data unit, i.e., the plaintext, as a sequence of complete blocks, P_0, P_1, …$P_{m\text{-}1}$, followed by a single, non-empty partial block P_m, where m is a positive integer determined by the length of the data unit.

In this case, the encrypted form of the data unit, i.e., the ciphertext, has the same structure: a sequence of complete blocks, denoted C_0, C_1, …$C_{m\text{-}1}$, followed by a single, non-empty partial block C_m, whose length is the same as the length of P_m.

For some implementations, an alternative ordering convention, in which the positions of $C_{m\text{-}1}$ and C_m are swapped, may be desirable for the physical storage of the bits, because that ordering corresponds more closely with the generation of the ciphertext. In particular, C_m is the truncation of a block that is derived from $P_{m\text{-}1}$, and $C_{m\text{-}1}$ is derived from P_m, concatenated with the discarded bits from the truncation.

This alternative ordering is permitted if it does not affect interoperability with other implementations. Section 5.1 of [2] indicates that an implementation of XTS-AES should include a mapping between the pairs of indices that define the elements of a data unit and the physical location of those elements in the storage device, but that the mapping itself is outside the scope of the standard.

Thus, the last block and the partial block may be stored in any convenient location in the storage device, as long as any external interface to the data retrieves them in a manner that is consistent with the ordering specified in [2]. In other words, if necessary, a mechanism for swapping the last block and the partial block could be built into the interface.

Appendix A: Bibliography

[1] Federal Information Processing Standards (FIPS) Publication 197, *Announcing the Advanced Encryption Standard (AES)*, U.S. DoC/NIST, Nov. 26, 2001.

[2] IEEE Std 1619-2007, *The XTS-AES Tweakable Block Cipher*, Institute of Electrical and Electronics Engineers, Inc., Apr. 18, 2008.

[3] P. Rogaway, *Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC*, Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Computer Science, vol. 3329, pp. 16-31, Springer-Verlag, 2004.