NIST Special Publication 800-38E
January, 2010

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

Morris Dworkin

C O M P U T E R S E C U R I T Y

NIST Special Publication 800-38E

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

Morris Dworkin

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

January 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Reports on Information Security Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 800-38E
Natl. Inst. Stand. Technol. Spec. Publ. 800-38E, 9 pages (January 2010)
CODEN: NSPUE2

Acknowledgements

The author wishes to thank Matt Ball, the Chair of the Security in Storage Working Group of the IEEE P1619 Task Group, as well as the author's colleagues who reviewed drafts of this publication and contributed to its development, especially Elaine Barker, Lily Chen, John Kelsey, Tim Polk, Bill Burr, and Sharon Keller. The author also gratefully acknowledges the comments from the public and private sectors to improve the quality of this publication.

Abstract

This publication 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 storage devices. The mode does not provide authentication of the data or its source.

KEY WORDS: block cipher; ciphertext stealing; computer security; confidentiality; cryptography; encryption; information security mode of operation; tweakable block cipher.

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 publication 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 federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Clause 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Clauses. Supplemental information is provided in A-130, Appendix III.

Nothing in this publication should be taken to contradict the 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. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

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, which is discussed in Section 4 below.

The XTS-AES mode was designed for the cryptographic protection of data on storage devices that use of fixed length "data units," as defined in Ref. [2]. 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; whereas for XTS-AES, the data string may also consist of one or more complete blocks followed by a single, non-empty partial

block. (The acronym XTS stands for the **X**EX **T**weakable Block Cipher with Ciphertext **S**tealing).

The specification of the ciphertext stealing method in Ref.[2] includes an ordering convention for the final complete block and partial block of the encrypted data string. A different convention, in which the order is swapped, may be desirable in some cases. The specification in Ref.[2] provides 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. In the absence of authentication or access control, XTS-AES provides more protection than the other approved confidentiality-only modes against unauthorized manipulation of the encrypted data.

Annex D of Ref.[2] discusses in detail the design choices for XTS, including the resistance to manipulation of the encrypted data, and their ramifications for the incorporation of XTS-AES into an information system. 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 Ref. [2]:

1) a secret key,
2) a single, fixed length for the data units that the key protects,
3) an implementation of 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} AES blocks. Note that Subclause 5.1 of Ref.[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 length requirement for a data unit, in addition to all of the requirements in Clauses 1-6 of Ref. [2].

Key management is important for XTS-AES, as for any keyed cryptographic algorithm, but the representation of a key backup structure in the Extensible Markup Language (XML) that is specified in Clause 7 of Ref. [2] is outside the scope of this Recommendation.

Consistent with the 2^{20} block limit for a data unit, an implementation of XTS-AES may further restrict the length of the data units for any key. 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 Ref. [2].

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

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

Conformance testing for implementations of XTS-AES is conducted within the framework of the Cryptographic Module Validation Program (CMVP), a joint effort of NIST and the Communications Security Establishment Canada.

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 Ref. [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-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-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-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-1}, and C_{m-1} is derived from P_m, concatenated with the discarded bits from the truncation.

Subclause 5.1 of [2] indicates that an implementation of XTS-AES should include a mapping between the pairs of indices that define the blocks (and possibly a single partial block) of a data unit and their physical location in the storage device, but that the mapping itself is outside the scope of the standard.

Thus, if every external interface to the data retrieves the data in a manner that is consistent with the ordering specified in Ref [2], then the last block and the partial block may be stored in any convenient locations in the storage device. In other words, if necessary, a mechanism for swapping the last complete 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.