The XTS-AES Validation System (XTSVS)

Updated: March 2, 2011
Previously Updated: August 30, 2010
Original: March 31, 2010

Sharon S. Keller

Timothy A. Hall

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

Update Log

3/2/11

- Remove the requirement for obtaining assurance for this statement:
  - The XTS-AES key SHALL NOT be associated with more than one key scope.

  This is out of scope of the CAVP testing.

1 Introduction

This document, *The XTS-AES Validation System (XTSVS)* specifies the procedures involved in validating implementations of the XTS-AES algorithm as specified in SP 800-38E*, Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices* [1]. The XTSVS is designed to perform automated testing on Implementations Under Test (IUTs). This document provides the basic design and configuration of the XTSVS.

This document defines the purpose, the design philosophy, and the high-level description of the validation process for XTS-AES. The requirements and administrative procedures to be followed by those seeking formal validation of an implementation of XTS-AES are presented. The requirements described include a specification of the data communicated between the IUT and the XTSVS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the XTSVS. Additionally, an appendix is also provided containing samples of input and output files for the XTSVS.

A set of XTS-AES test vectors is available on the http://csrc.nist.gov/cryptval/ website for testing purposes.

2 Scope

This document specifies the tests required to validate IUTs for conformance to the XTS-AES algorithm which is a mode of operation of the Advanced Encryption Standard (AES) algorithm. When applied to an IUT, the XTSVS provides testing to determine the correctness of the implementation of XTS-AES. The XTSVS is composed of validation tests that verify the functionality of the XTS-AES encrypt and the XTS-AES decrypt functions for both the XTS-AES key sizes supported – the 256 bit key size (denoted XTS-AES-128) and the 512 bit key size (denoted XTS-AES-256).

The XTS-AES algorithm validation process requires additional prerequisite testing of the underlying AES implementation via the AESVS. For XTS-AES Encrypt, the AES validation referenced shall include an AES mode of operation that uses the forward cipher function. For XTS-AES Decrypt, the AES validation referenced shall include an AES mode of operation that uses the forward and inverse cipher function (i.e., AES-ECB or AES-CBC).

3 Conformance

The successful completion of the tests contained within the XTSVS and the AESVS is required to be validated as conforming to the XTS-AES algorithm standard. Testing for the cryptographic module in which the XTS is implemented is defined in FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* [3].

4 Definitions and Abbreviations

4.1 Definitions

DEFINITION	MEANING
Advanced Encryption Standard	The algorithm specified in FIPS 197, *Advanced Encryption Standard (AES)*
CMT laboratory	Cryptographic Module Testing laboratory that operates the XTSVS

4.2 Abbreviations

ABBREVIATION	MEANING
AES	Advanced Encryption Standard specified in FIPS 197
AESVS	Advanced Encryption Standard Validation System
FIPS	Federal Information Processing Standard
IUT	Implementation Under Test
XTS-AES	Mode of Operation specified in IEEE Std. 1619-2007 and approved by SP800-38E with one additional requirement on the lengths of the data units.

5 Design Philosophy of XTS-AES Validation System

The XTSVS is designed to test conformance to the XTS-AES specification rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

The XTSVS has the following design philosophy:

1. The XTSVS is designed to allow the testing of an IUT at locations remote to the XTSVS. The XTSVS and the IUT communicate data via *REQUEST* and *RESPONSE* files. The XTSVS also generates *SAMPLE* files to provide the IUT with samples of what the *RESPONSE* files should look like.

2. The testing performed within the XTSVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the standard.

6 XTSVS Test

- The XTSVS tests the implementation of XTS-AES for its conformance to the XTS-AES standard. An instance of an XTS-AES implementation is defined by the following three elements as specified in [2]:
  - A secret key. The key sizes supported include a 256-bit key size (denoted XTS-AES128) and a 512-bit key size (denoted XTS-AES256).
  - A single fixed length for the data units that the key protects. The XTS-AES implementation may support data unit lengths of only complete block sizes or it may support partial block sizes.
  - 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.

6.1 Configuration Information

To initiate the validation process of the XTSVS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of XTS-AES. The vendor's implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the XTSVS to perform the specific tests. More specifically, the request for validation includes:

1. Vendor Name;
2. Product Name;
3. Product Version;
4. Implementation in software, firmware, or hardware;
5. Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;
6. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and
7. Configuration information for the XTS-AES tests, including:

   a) XTS-AES key sizes supported – XTS-AES-128 (256 bit key size) and/or XTS-AES-256 (512 bit key size);

b) For each XTS-AES key size supported, indicate a sampling of data unit lengths supported

   - If data unit lengths of complete block sizes are supported, specify two message lengths divisible by the 128-bit block size.

   - If data unit lengths of partial block sizes are supported, specify two message lengths not divisible by the 128-bit block size.

   - Specify the largest block size supported by the implementation or check the 2^16 box, whichever is larger.

c) Indicate the format of the tweak value input

   - 128-bit hexadecimal string

   - Data Unit Sequence Number

d) Obtain assurance from the vendor that the IUT satisfies the assurance:

   - The length of the data unit for an instance of an implementation of XTS-AES SHALL NOT exceed 2^{20} blocks

6.2 The XTSGenAES Test

The XTSVS generates a separate file for each key size tested for the IUT. The possible file names are XTSGenAES128 for IUTs supporting the XTS-AES-128 key size and XTSGenAES256 for IUTs supporting the XTS-AES-256 key size.

Within this file, there is a section for each supported state (Encrypt and/or Decrypt) being tested.

Within each section, for each data unit length provided, the XTS-AES validation test provides 100 combinations of data unit length – key – tweak value (*i*) or data unit sequence number (*DataUnitSeqNumber*) – plaintext/ciphertext. The tweak value *i* is a 128-bit random string represented by 32 hexadecimal characters. The *DataUnitSeqNumber* is a base-10 number ranging between 0 and 255.

An implementation may support a data unit length that is not a multiple of 8 bits. In this case, the plaintext (PT) and ciphertext (CT) will be represented in the request, sample, and response files by a bit string padded with zeros on the right to the next byte boundary, in hexadecimal. For example, suppose an implementation supports a 137 bit data unit. The first 128-bit block consists of the first (i.e., leftmost) 128 bits. If the second, nine-bit partial block is 011011011, then in the request and sample files it will be padded with seven zeros on the right – 0110 1101 1000 0000 – and represented as 6d80 (hex). Response files values should be formatted the same way.

The IUT performs the applicable function (encrypt or decrypt) on the data using the information provided and generates the result (ciphertext/plaintext). The XTSVS verifies the correctness of the IUT's response.

The XTSVS:

A. Creates a *REQUEST* file (Filename: XTSGenAES{AESKeySize}.req) containing:

1. The CAVS tool version;

   2. The implementation name being tested;

   3. The states being tested (encrypt and/or decrypt);

   4. The key lengths being tested (AES128 or AES256);

   5. The data unit lengths being tested;

   6. Format of the tweak value;

   7. The length of the data unit, the key value, the tweak value (or the Data Unit Sequence Number), and the plaintext or ciphertext value to be used as input to the XTS-AES algorithm.

Note: The CMT laboratory sends the *REQUEST* file to the IUT.

B. Creates a *FAX* file (Filename: XTSGenAES{AESKeySize}.fax) containing:

   1. The information from the *REQUEST* file; and

   2. The resulting ciphertext (if encrypting) or plaintext (if decrypting) generated by the XTS-AES algorithm.

   Note: The CMT laboratory retains the *FAX* file.

The IUT:

A. Generates the requested results (ciphertext or plaintext) using the data specified in the *REQUEST* file.

B. Creates a *RESPONSE* file (Filename XTSGenAES{AESKeySize}.rsp) containing:

   1. The information from the *REQUEST* file; and

   2. The resulting ciphertext (if encrypting) or plaintext (if decrypting) generated by the XTS-AES algorithm.

   Note: The IUT sends the *RESPONSE* file to the CMT laboratory for processing by the XTSVS.

The XTSVS:

A. Compares the contents of the *RESPONSE* file with the contents of the *FAX* file.

B. If all values match, records PASS for this test; otherwise, records FAIL.

Appendix A References

[1] *Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*, Special Publication 800-38E, National Institute of Standards and Technology, August 2009.

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

[3] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.