ITL BULLETIN FOR NOVEMBER 2017

GUIDANCE ON TDEA BLOCK CIPHERS

Elaine Barker, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

As computing power becomes faster and cheaper, cryptographic methods that were reliable and secure yesterday become less so today. Only a few years after Gordon Moore, co-founder of Intel Corporation, noted that the number of transistors in a dense integrated circuit doubles approximately every two years, in 1977, the Data Encryption Algorithm (DEA) was adopted. A few decades later, computers had sufficient power to allow a successful brute force attack rather quickly. Fortunately, that same increase in power enabled stronger encryption, and the Triple Data Encryption Algorithm (TDEA) was introduced. TDEA provides a straightforward method for using three keys but remains compatible with DEA in one mode of its use. These three keys are collectively called a key bundle. But today, brute force attacks on TDEA are practical and inexpensive.

With ciphers, it is important to consider the suitability of the algorithm for the intended purpose. The strength of a physical padlock may be sufficient for a gym locker but should not be used to lock the gate to Fort Knox. The National Institute of Standards and Technology (NIST) periodically provides recommendations about conditions under which a cryptographic algorithm should be applied. This guidance, while useful for anyone, is mandatory for federal agencies, federal contractors, and other organizations that process information on behalf of the federal government. To that end, NIST has created Special Publication (SP) 800-67, Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, which describes TDEA and the DEA cryptographic engine, and provides restrictions on TDEA usage.

TDEA

NIST SP 800-67, Revision 2 (the “Recommendation”) provides a description of a mathematical algorithm for encrypting or authenticating binary coded information. The algorithm described in this

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

Recommendation specifies cryptographic operations that are based on the use of three keys, each of which is a binary number.

Authorized users of computer data that was cryptographically protected using TDEA need the key bundle that was used to process the protected data. The cryptographic algorithm specified in the Recommendation is commonly known among its users. The cryptographic security of the data depends on the security provided for the keys used to protect the data and the amount of data protected by a single TDEA key bundle.

Data that is determined to be sensitive, that has a high value, or that *represents* a high value should be cryptographically protected if it is vulnerable to either unauthorized disclosure or undetected modification during transmission or while in storage. A risk analysis should be performed, under the direction of a responsible authority, to determine potential threats. The costs of providing cryptographic protection using this Recommendation, as well as providing alternative methods for this protection, should be projected. A responsible authority can then decide, based on these analyses, whether to use this Recommendation for cryptographic protection.

DEA was originally specified in FIPS 46, *The Data Encryption Standard,* which became effective in July 1977. It was reaffirmed in 1983, 1988, 1993, and 1999. FIPS 46-3 was withdrawn in May 2005 because it no longer provided the security needed to protect federal government information. With the withdrawal of the FIPS 46-3 standard (the final revision of FIPS 46), implementations of the DEA function are no longer authorized for the protection of federal government information. The use of DEA is allowed only as a component function of TDEA.

NIST SP 800-67, Revision 2 specifies an alternative to DEA, based on the DEA "cryptographic engine" that was originally specified in FIPS 46 and is included in the Recommendation. The Recommendation applies to all federal agencies, contractors of federal agencies, and other organizations that process information on behalf of the federal government to accomplish a federal function. Each federal agency or department may issue internal directives for the use of this Recommendation by their operating units, based on their data security requirement determinations.

DEA Cryptographic Engine

A ciphertext collision occurs when two different plaintext inputs using two different key bundles produce the same ciphertext. For a cipher composed of 64-bit data blocks, such as TDEA, a ciphertext collision will likely occur when about 2^{32} (4,294,967,296) 64-bit data blocks are encrypted with a single key bundle. A collision in ciphertext blocks, once found, reveals information about the corresponding plaintext blocks.

For the probability of a collision to be small, the amount of data would have to be significantly below 2^{32} blocks. This security weakness motivated the requirement for the 128-bit block size in the development of the Advanced Encryption Standard (AES). AES is specified in FIPS 197, Advanced Encryption Standard (AES).

Usage Guidance

The security of TDEA is affected by the number of blocks processed with one key bundle. One key bundle must not be used to apply cryptographic protection (e.g., encrypt) more than 2^{20} 64-bit data blocks. This limitation applies to a key bundle with three unique keys (that is, 3TDEA). The use of TDEA with only two unique keys (that is, 2TDEA) must not be used to apply cryptographic protection.

In the previous version of SP 800-67 (dated January 2012), 3TDEA was limited to processing 2^{32} 64-bit data blocks, and 2TDEA was limited to 2^{20} 64-bit data blocks. These prior limitations should be considered when processing information already protected using the previous and original versions of SP 800-67. For example, users should determine the risk of accepting the decrypted information when the limit provided in this revision for 3TDEA is exceeded or when the information was encrypted using 2TDEA.

Looking into the Future

In response to known security weaknesses, NIST plans to reduce the maximum amount of plaintext allowed to be encrypted under a single TDEA 3-key bundle from 2^{32} to 2^{20} (64-bit) blocks. Also, because these weaknesses make TDEA unsuitable for some applications, NIST plans to disallow the algorithm for Transport Layer Security (TLS), IPsec, and possibly other protocols.

NIST is developing a draft deprecation timeline for the 3-key variant of TDEA, including a sunset date, so while this Recommendation allows the continued use of TDEA under certain conditions, NIST urges all users of TDEA to migrate to the more secure and cost-efficient AES as soon as possible.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov


INFORMATION
TECHNOLOGY
LABORATORY