White Paper

AES Encryption

AES Encryption and Related Concepts

THIS PAPER IS A NON-TECHNICAL INTRODUCTION to the Advanced Encryption Standard (AES) and to important topics related to encryption such as encryption key management, validation, common uses to protect data, and compliance. You will find a resource guide at the end for further research on this and related topics.

Townsend SECURITY

www.townsendsecurity.com

724 Columbia Street NW, Suite 400 • Olympia, WA 98501 • 360.359.4400 • 800.357.1019 • fax 360.357.9047 • www.townsendsecurity.com

What is AES?

The Advanced Encryption Standard (AES) is formal encryption method adopted by the National Institute of Standards and Technology of the US Government, and is accepted worldwide. This paper introduces AES and key management, and discusses some important topics related to a good data security strategy.

A Brief History

In 1997 the National Institute of Standards and Technology (NIST), a branch of the US government, started a process to identify a replacement for the Data Encryption Standard (DES). It was generally recognized that DES was not secure because of advances in computer processing power. The goal of NIST was to define a replacement for DES that could be used for non-military information security applications by US government agencies. Of course, it was recognized that commercial and other non-government users would benefit from the work of NIST and that the work would be generally adopted as a commercial standard.

The NIST invited cryptography and data security specialists from around the world to participate in the discussion and selection process. Five encryption algorithms were adopted for study. Through a process of consensus the encryption algorithm proposed by the Belgium cryptographers Joan Daeman and Vincent Rijmen was selected. Prior to selection Daeman and Rijmen used the name Rijndael (derived from their names) for the algorithm. After adoption the encryption algorithm was given the name Advanced Encryption Standard (AES) which is in common use today.

In 2000 the NIST formally adopted the AES encryption algorithm and published it as a federal standard under the designation FIPS-197. The full FIPS-197 standard is available on the NIST web site (see the Resources section below). As expected, many providers of encryption software and hardware have incorporated AES encryption into their products.

The AES Algorithm

The AES encryption algorithm is a block cipher that uses an encryption key and several rounds of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term “rounds” refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key.

The AES algorithm itself is not a computer program or computer source code. It is a mathematical description of a process of obscuring data. A number of people have created source code implementations of AES encryption, including the original authors.

Encryption Keys

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm. Encryption algorithms that use two different keys, a public and a private key, are called asymmetric encryption algorithms.

An encryption key is simply a binary string of data used in the encryption process. Because the same encryption key is used to encrypt and decrypt data, it is important to keep the encryption key a secret and to use keys that are hard to guess. Some keys are generated by software used for this specific task. Another method is to derive a key from a pass phrase. Good encryption systems never use a pass phrase alone as an encryption key.

Modes of Operation

There are different methods of using keys with the AES encryption method. These different methods are called “modes of operation”. NIST defines a number of modes of operation for AES which include:

- Electronic code book (ECB)
- Cipher block chaining (CBC)
- Counter (CTR)
- Cipher feed back (CFB)
- Output feed back (OFB)
- Galois Counter Mode (GCM)

Each mode uses AES in a different way. For example, ECB encrypts each block of data independently. CTR mode encrypts a 128-bit counter and then adds that value

to the data to encrypt it. CBC mode uses an initialization vector and adds the encrypted value of each block to the data in the next block before encrypting it. Some modes require you to only encrypt data that is a multiple of the 16-byte block size; others allow you to truncate unused data.

It is important to note that you can use strong encryption in a weak way resulting in poor security for your sensitive data. Using an inappropriate mode of encryption, or using a mode of encryption improperly, can leave your data exposed to loss. Fully understanding the implications and management requirements of each mode is a vital part of planning for encryption.

NIST Testing & Validation

Recognizing the need for a method of insuring the quality and correctness of AES implementations, NIST developed a set of tests and a testing protocol for the algorithm. It chartered independent testing laboratories to administer the tests and monitor the results. This set of tests is referred to as AES Validation. To achieve NIST validation a data security vendor must pass hundreds of different tests designed to validate that the vendor is properly encrypting and decrypting data. Only when all tests have been passed does the NIST issue AES Validation certificates. The list of vendors who have passed these tests is located at this link: http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html

Key Management

Many people think that encryption is all about secret methods, or algorithms, for obscuring code. In reality the encryption methods are public and anyone can read how encryption is done and obtain source code for performing the encryption and decryption steps. The secret part is the key used to perform encryption and decryption. For this reason it is important to keep your encryption keys secret, and use secure methods for creating, distributing, and storing your keys.

Key management systems allow you to create keys and keep them secret. Many security professionals believe that the most important part of their data security strategy is the proper creation, management, and protection of their encryption keys.

Key management systems provide a wide variety of functions including:

- Key creation
- Key rotation, or key change
- Key expiration
- Key import and export
- Key usage control
- Secure key storage
- Access controls
- Key escrow, or archival
- Compliance logging

A good key management system is crucial for a good data security strategy.

Encryption In Database Applications

Businesses with sensitive data in database applications want to encrypt the data in order to secure it from loss. Protecting sensitive data increases customer trust and loyalty, reduces legal liability, and helps meet regulatory requirements for data security. Examples of databases that might contain sensitive information are Oracle Database, IBM DB2, Microsoft SQL Server, MySQL, and Microsoft Access. Regardless of the disk or folder encryption technology that might be used, the actual data should be encrypted to prevent loss.

At the time this document was written most database systems do not provide encryption support that meets NIST standards. Additionally, most database systems do not provide cross-platform support for encrypting and decrypting sensitive data. This situation will surely change in the future but, until database systems achieve NIST compliance for security, database users will need to provide encryption in their application programs.

Best Practices

Understanding the best practices for implementing encryption in your business applications is important to achieving good data security. Here are some key points:

- Never store pass phrases or encryption keys in your application source code.

- Use a key management system to secure encryption keys and provide a way to securely back up your keys.

- Use appropriate key generation methods to create encryption keys – never use passwords or pass phrases as keys.

- Use the right mode of encryption for database applications. Cipher Block Chaining (CBC) and Counter (CTR) modes are appropriate for database applications; Electronic Code Book (ECB) and Galois Counter Mode (GCM) are not.

- Adopt data security standards and guidelines for your application developers to follow when creating or maintaining applications.

These are some basic areas of focus for best practices in data security. Be sure you understand the best ways to implement data security before you start.

Encryption in Cloud and VMware Environments

Cloud and VMware users benefit from the many operational, and cost efficiencies provided by these platforms. However, organizations need to choose encryption solutions within these platforms that are based on industry standards. While emerging encryption technologies are available, it is important to only use solutions that have been through NIST validation and are based on standards such as AES.

Choosing A Software Vendor For Data Encryption

When you choose a software vendor for data encryption be sure they are experts in data security and offer support across a broad spectrum of platforms. Your vendor should be able to provide you with a coherent strategy and common encryption methods for securing data. You should be able to ask about encryption keys and encryption modes and get an understandable answer to your questions. The choice of a software vendor for data security may be the single most important decision you make.

Data Security And The Law

A number of federal and state laws have taken effect which require or encourage the encryption of sensitive data. Some examples are the California Privacy Notification law (SB1386), Massachusetts Privacy Protection, and Nevada privacy protection which require companies to notify customers or employees when sensitive data is lost. Other states have passed even more stringent laws. The Sarbanes-Oxley Act (SOX) is a federal law that requires certain types of data security. For banks the Gramm Leach Bliley Act (GLBA) requires that sensitive data be secured from loss. In the medical industry the federal Health Insurance Portability and Accountability Act (HIPAA) requires that patient information be secured from loss. Lastly, through their written agreements with merchants, credit card vendors such as Visa and Mastercard require that credit card numbers and related sensitive information be secured from loss with strong encryption according to Payment Card Industry (PCI) rules.

Alliance AES Data Encryption Products From Townsend Security

The Alliance AES encryption solutions from Townsend Security provide a complete implementation of the AES encryption algorithm and modes of operation for use in database applications, and have passed the rigorous tests of NIST AES Validation. Solutions are available for a variety of platforms including IBM i, IBM z, Microsoft Windows, IBM AIX, Sun Solaris, and Linux on both 32-bit and 64-bit systems. These solutions give the Enterprise customer with the tools the need for a cross-platform approach to data security. Key management is provided including support for third party solutions.

Resources

The National institute of Standards and Technology publishes a list of AES validated applications here:
http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html

The official NIST FIPS-197 publication is available here (you will need the Adobe Acrobat reader):
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

The Wikipedia entry for AES encryption has a good non-mathematical description of the algorithm. Of course, the mathematical references are also available:
http://en.wikipedia.org/wiki/AES_encryption

Payment card industry rules for credit card security can be found here:
https://www.pcisecuritystandards.org/document_library

Townsend Security

We know that data gets out, and that it can and routinely does fall into the wrong hands. When this happens, our solutions for encryption, key management, and system logging ensure that your Enterprise is compliant with regulations and that your sensitive data is protected. Our data security solutions work on a variety of server platforms including IBM i, IBM z, Windows, and Linux. Many of these solutions are currently used by leaders in retail, health care, banking, and government.

You can contact Townsend Security for an initial consultation at the following locations:

Web: www.townsendsecurity.com
Phone: (800) 357-1019 or (360) 359-4400
International: +1 360 359 4400
Email: Info@townsendsecurity.com

A fully functional free trial is available for all Alliance products. You can evaluate Alliance capabilities on your own server systems.