Homeland Security
Science and Technology

TechNote

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

For more information on this and other technologies, contact the SAVER Program Support Office.

RKB/SAVER Telephone: 877-336-2752
E-mail: saver@hq.dhs.gov
Website: https://www.rkb.us/saver

This SAVER TechNote was prepared by the National Urban Security Technology Laboratory for the SAVER Program.

NUSTL

Encryption Software Tools

Emergency responders often store sensitive information on portable computers and handheld devices, and transmit sensitive information through e-mail, instant messaging, and other forms of digital communications. Encryption software tools prevent this information from being disclosed when a computing device is lost or stolen or when a message is intercepted by a third party.

Technology Description

Files and messages can be encrypted using a software algorithm known as a cipher. Ciphers use a numeric key to convert readable, plaintext messages to an encoded form of the original message, called ciphertext. Ciphertext contains all the information in the original plaintext message, but cannot be read by humans or computers without access to a decryption cipher and its corresponding key. Stream ciphers, which are used mostly for real-time communications, encrypt data one bit or byte at a time. Block ciphers break data into larger blocks, typically about 64 bits, before encrypting it. Both techniques employ a long series of mathematical operations or substitutions involving the data and a numeric key to convert the plaintext to ciphertext. An opposite set of operations decrypts the data by converting the ciphertext back to plaintext.

Symmetric Key Ciphers

Symmetric key encryption ciphers use the same key to encrypt and decrypt a message. These algorithms are fast, efficient, and well suited to applications for storing encrypted documents. They are not often used for communications, however, because they require both parties to have access to a single key that must be kept secret before a message is sent.

The National Institute of Standards and Technology (NIST) evaluated many proposals during a lengthy selection process for a standard symmetric key cipher approved for encrypting sensitive information by U.S. government agencies. In November 2000, NIST chose a variant of the Rijndael[1] cipher as the Advanced Encryption Standard (AES). The AES algorithm uses 128-byte blocks of data and allows key sizes of 128, 192, or 256 bits. Although having been subjected to great scrutiny, AES has proven to be resistant to all known forms of attack. For instance, a supercomputer running a brute force attack, in which the key is repeatedly guessed at until decryption is successful, would require 10^{18} years in order to determine a 128-bit AES key. Other more sophisticated forms of attack have also proven to be computationally infeasible. AES has replaced the Digital Encryption Standard (DES), which originated in 1977 and uses a 56-bit key. With recent advances in computers, a DES key can now be broken in less than 24 hours. Triple DES, a cipher that employs three DES keys in succession, is more secure and is still commonly in use.

[1] Rijndael is pronounced "Rein-dahl" and is named after its inventors, Vincent Rijmen and Joan Daemen.

Asymmetric Key Ciphers

Asymmetric key encryption (also called public key cryptography) allows parties that do not regularly communicate to send each other encrypted messages. It works by generating pairs of mathematically related keys. One key is used to encrypt a message, and a separate key is used to decrypt the message (Figure 1). Each party that wishes to receive messages is assigned its own key pair, with each pair comprising one public and one private key. A sender encrypts a message using the receiver's publicly available key. The message is then decrypted with the receiver's private key. This is analogous to a locked mailbox with a slot for receiving messages. Anyone who knows the address of the mailbox (the public key) can insert a message, but only the owner of the mailbox can read the message (using the private key).

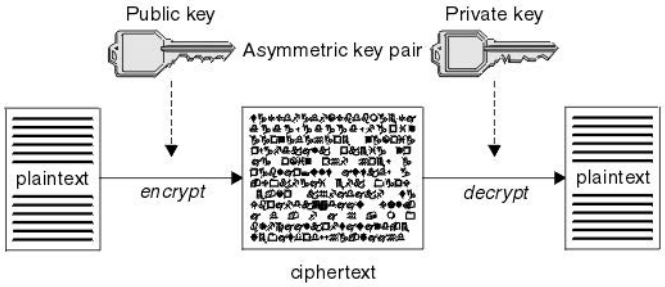

Figure 1. Asymmetric key encryption with public and private keys.
Reprint courtesy of International Business Machines Corporation,
© 2012 International Business Machines Corporation.

A *de facto* standard for asymmetric key encryption is the RSA[2] algorithm. The Transportation Layer Security (TLS) protocol, which is used as the basis for secure Web-based transactions, uses the RSA algorithm to encrypt data. RSA is also one of several algorithms supported by common e-mail encryption protocols such as Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME).

A disadvantage to asymmetric key encryption is that the algorithms are complex and require large keys. Key sizes of 1,024 bits or more are needed for high-strength encryption. The RSA algorithm allows variable key sizes, and its inventors recommend 2,048-bit keys for messages that must remain secure until 2030 and 3,072-bit keys for data that must remain secure beyond that year. The mathematical operations needed to encrypt messages with such large keys create a large workload for computer processors. As a result, asymmetric encryption can by very slow for large messages. PGP and other encryption tools send long messages by first randomly generating a symmetric key and transmitting it by RSA or some other asymmetric key cipher. The rest of the message is then transmitted with symmetric key encryption.

Public Key Infrastructure

With asymmetric encryption, a method is needed for exchanging public keys and ensuring that they belong to a certain individual or organization. Public key infrastructure (PKI) is an arrangement in which digital certificates are issued and made publicly available by a certificate authority (CA). The CA may be an entity within an organization or a trusted third party that allows two organizations to engage in secure communications.

Digital Signatures

A digital signature is a data stamp that can be added to a message to uniquely identify the sender. Senders use their private key to encrypt the signature, and receivers use the sender's public key to decrypt it. When a digitally signed message is properly implemented, a sender cannot deny having sent the message, and the receiver cannot deny having received the message.

Applications

File encryption and e-mail encryption comprise the two main applications of software encryption tools. File encryption programs allow sensitive data to be stored on a computer in ciphertext, so that the data cannot be read without a password that allows for decryption. Most products on the marketplace use a symmetric cipher such as AES with at least a 256-bit key. Having a strong key protects the data even if the computer is stolen. Many of these products come with additional features such as file compression, file shredding (so that deleted files can never be recovered), stealth mode (so that encrypted data is hidden), and biometric identification.

E-mail encryption tools are widely available for sending secure messages and attachments. These programs can be used throughout an organization on servers, desktop computers, and handheld devices. They generally use proprietary technologies, but also support common encryption protocols and work compatibly with common applications such as Outlook, Lotus Notes, and Gmail. Most programs support user-initiated encryption or policy-based encryption, in which software at a network gateway encrypts e-mails automatically based upon criteria such as message content and destination. An e-mail encryption program should generate and register keys with a CA, allow digital signing, and allow for secure connections to other organizations. These tools are generally installed and maintained by an agency's information technology (IT) department and are used according to an agency-wide IT policy.

[2] RSA was named for its developers Ron Rivest, Adi Shamir, and Leonard Adleman. It was made publicly available in 1977.