

Introduction to Encryption

Chad Cook 2000-11-06

Introduction to Encryption

by Chad Cook (ccook@illusive.org)

last updated Nov. 6, 2000

Introduction

A secure computing environment would not be complete without consideration of encryption technology. The term encryption refers to the practice of obscuring the meaning of a piece of information by encoding it in such a way that it can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it.

The use of simple codes to protect information can be traced back to the fifth century BC. As time has progressed, the methods by which information is protected have become more complex and more secure. Encryption can be used to provide high levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection.

The goal of this article is to present the reader with an introduction to the basics of encryption, its role in the small office/ home office environment and the benefits and drawbacks of encryption to the non-professional user who is concerned about information security.

Encryption

Encryption is said to occur when data is passed through a series of mathematical operations that generate an alternate form of that data; the sequence of these operations is called an **algorithm**. To help distinguish between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as ciphertext. The security of encryption lies in the ability of an algorithm to generate ciphertext that is not easily reverted to the original plaintext.

In a very simple example, encryption of the word "secret" could result in "terces." Reversing the order of the letters in the plaintext generates the ciphertext. This is a very simple encryption - it is quite easy for an attacker to retrieve the original data. A better method of encrypting this message might be to create an alternate alphabet by shifting each letter by

some arbitrary number. This is known as a substitution cipher, a form of encryption that is still used in puzzle books today. For example, encrypting the word "secret" with an alphabet shifted by 3 letters to the right (Figure 1.) produces "vhfuhw." A substitution cipher simply exchanges one letter or word with another. This particular algorithm is called the "Caesar Cipher"

Normal alphabet:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alphabet shifted by 3:	d e f g h i j k l m n o p q r s t u v w x y z a b c

Figure 1. The Caesar Cipher and the encryption of the word "secret"



Keys

In the quest for a more secure method of protecting information, the introduction of a [key](#) adds another level of security. A key is a piece of information that allows only those that hold it to encode and decode a message. Keys come in many different forms such as passwords, numbers generated by an algorithm, digital fingerprints and even electronic devices that work like door keys. It is a series of numbers or symbols that are used to encode a message so that it can only be read by someone in possession of that key or a related key. A key allows both the sender and the recipient of the message to understand how the message has been encrypted and assures them that nobody else knows how it has been encrypted. It is the key that enables the recipient to properly decode the message.

Using the previous example of a substitution cipher, anyone who knows the Caesar Cipher can decrypt all messages encrypted with it, regardless of who actually encrypted the message. One could strengthen the substitution cipher with a key, by choosing an arbitrary number and using that as the number of letters by which to shift when creating their alternate alphabet. That number therefore becomes the key by which the message is unlocked.

The individual who is sending the message communicates the key to the recipient of the message, allowing them to unlock it. One disadvantage of this system is that an attacker can decrypt the message if the key is intercepted. To protect the key, encryption can be used during communication or the key can be sent in a separate communication.

Symmetric and Asymmetric Encryption

There are two general categories for key-based encryption - symmetric and asymmetric.

Symmetric encryption uses a single key to encrypt and decrypt the message. This means the person encrypting the message must give that key to the recipient before they can decrypt it. To use symmetric encryption, the sender encrypts the message and, if the recipient does not already have a key, sends the key and ciphertext separately to the recipient. The recipient then uses the key to decrypt the message. This method is easy and fast to implement but has weaknesses; for instance, if an attacker intercepts the key, they can also decrypt the messages. Furthermore, single key encryptions tend to be easier for people to "crack", which means that the algorithm that is used to encode the message is easier for attackers to understand, enabling them to more easily decode the message.

Asymmetric encryption, also known as **Public-Key encryption**, uses two different keys - a **public key** to encrypt the message, and a **private key** to decrypt it. The public key can only be used to encrypt the message and the private key can only be used to decrypt it. This allows a user to freely distribute his or her public key to people who are likely to want to communicate with him or her without worry of compromise because only someone with the private key can decrypt a message. To secure information between two users, the sender encrypts the message using the public key of the receiver. The receiver then uses the private key to decrypt the message. Unlike with single or shared keys, in the asymmetric key system only the recipient can decrypt a message; once the sender has encrypted the message he or she cannot decrypt it. The private key is never distributed, therefore an attacker cannot intercept a key that decrypts the message.

Common Uses of Encryption

Authentication

Authentication is the process of logging in, signing on or otherwise presenting information or oneself in a manner that proves his or her identity. The most common example of authentication is the use of a username and password to gain access to a system, network or web site. The username and password combination is often referred to as a person's credentials and it is frequently sent over networks. Encryption is used to protect these credentials. If no encryption is used to protect the information as it is sent over the network, an attacker could capture those credentials and assume the identity of the originator.

Validation ? Fingerprints and Digital Signatures

Validation describes the ability to provide assurance that a sender's identity is true and that a message, document or file has not been modified. Encryption can be used to provide validation by making a digital fingerprint of the information contained within a message. A digital fingerprint is a code that uniquely identifies a file or a message by reflecting the content of the file with tremendous specificity.

The encryption program produces the digital fingerprint by performing a byte-by-byte mathematical analysis of the message. Any attempt to modify the message will change the fingerprint. Comparison between a fingerprint known to be good and one sent to the recipient can indicate whether or not the message has been modified. While a fingerprint can indicate that the message has not been tampered with, it does not assure the recipient of the identity of the sender. For that assurance, the sender can utilize a digital signature.

A [digital signature](#) is a piece of information that proves the identity of the sender. It is a digital stamp or personal seal that is made using a private key. A sender can electronically or digitally sign a message and its fingerprint before delivery to a recipient. Upon receiving the message, the recipient verifies this signature, using the public key that the sender has previously communicated, indicating that the sender is the expected person. The recipient can verify the fingerprint of the message. Upon validation, the recipient can be reasonably sure that the message came from a trusted person and that the contents of the message have not been modified.

Data Protection

Probably the most widely-used application of encryption is in the area of data protection. The information that a business owns is invaluable to its productive operation; consequently, the protection of this information is paramount. For people working in small offices and home offices, the most practical uses of encryption for data protection are file and email encryption.

Encryption of files protects the data that is written to the hard disk on the computer. This information protection is vital in the event of theft of the computer itself or if an attacker successfully breaks into the system. However, file encryption becomes more difficult to use and manage if the office has multiple employees. Because each employee needs the encryption key, protection of the key becomes a more difficult task. The more people who have access to

encryption keys, the less effective encryption becomes. The risk of loss, theft or compromise of information rises as the number of users increases. Files that have been encrypted are also vulnerable to employees who leave the organization or who are disgruntled and may want to cause the organization harm.

Email encryption can be used more easily in office environments as private encryption keys are not generally shared among users and each user has a separate mailbox. When sending a message to multiple recipients, it can be encrypted for each person individually. The encryption key is therefore still private to the sender.

Secure Socket Layers ? Encryption for E-Commerce

While we have discussed encryption in the context of file protection and e-mail security, it is also a valuable security resource for web-based information exchange. The small office/ home office or personal computer user often sees this when doing business via web sites. E-commerce web sites use [SSL \(Secure Sockets Layer\)](#) to protect important information such as credit card numbers as they travel across the network. SSL creates a private communication path between the web browser and the web server, encrypting all information that goes between the systems. Most common web browsers have SSL support built in and e-commerce companies can purchase or get freely available web servers that support SSL.

Virtual Private Networks

The use of encryption has been extremely valuable in the increase of people who are able to work from home. Encryption provides a secure means for users to connect to their employer's network from outside of the home or office. [Virtual Private Networks \(VPN\)](#) allow remote users to connect to the home- and small-office network from distant places via the Internet by creating an encrypted path to that network. This is useful when cooperating with other organizations, working from remote locations or allowing remote users access to the local network.

Security, Encryption and the Small Office/ Home Office User

The use of encryption alone does not guarantee security; rather, it is one piece of a more complex security puzzle. Encryption can provide a higher level of security when implemented in

conjunction with other security measures as it protects data during storage and when communicating information between parties. It is important to note that encryption does not protect the user or network from other security threats such as viruses, network attacks and system compromise. Encryption can be very useful in protecting information that is being transmitted from one computer to another; however it does nothing to protect the integrity of the channels along which those messages travel. As such, it has no bearing on [denial of service attacks](#), [port scanning](#) and other network attacks.

Encryption and Viruses

[Viruses](#) infect computers many different ways, some of the most common methods are via file transfer and email. In and of itself encryption does not prevent the transmission of [malicious code](#) of any kind. However, the use of encryption as a validation mechanism can provide a higher level of trust when receiving files and information from other people by ensuring that the source and contents of the message are trusted. Digital signatures and message fingerprints can provide reasonable assurance that the file originates from the expected party and that it has not been tampered with. Encryption does not necessarily solve the problem completely though - a trusted source may unsuspectingly send an already infected file that is then validated.

Denial of Service Attacks

Encryption can protect a user's credentials from capture, but is somewhat helpless against attacks that are intended to compromise a system. System compromise results from attacks against an operating system feature or service, and can only be rectified by secure development practices and analysis of the software. Encryption does not protect against network attacks such as [denial of service](#), port scanning and other information gathering tactics. These attacks are generally independent of the use of encryption within a [network](#) or system.

Encryption for Small Offices/Home Offices ? Pros and Cons

Implementation and Use

When working in or establishing a small office and home office environment it is important to

establish the need for security of company files, data and information. Encryption can help provide a high level of security, but there are other pertinent factors that can help users decide if it is the best solution for their needs.

Aside from the technical aspects and benefits of its encryption technology, it is important to consider the surrounding business issues with the use of encryption. Cost and technical support along with ease of implementation and use are factors that merit consideration. Encryption technology is very complex and requires deep technical knowledge to be implemented properly. The implementation often requires additional hardware and software, as well as the aid of technical experts to setup the system. As well, as a business enterprise grows, costs for encryption may also increase. It is vital that small office and home office users decide whether or not encryption is necessary or justified for their security purposes before undertaking the monetary and time commitments required to implement encryption properly.

There are many commercial packages that provide data encryption, network security and other features. Commercial vendors make encryption technology easy to use by helping them with installation, setup and the support of experts. They also provide simple user interfaces that make them easy to use. The cost for this level of involvement and support is high.

As an alternative to these commercial applications, free encryption technology can be found on the Internet; however, they may require a high degree of technical understanding because the installation, setup, use and management falls on the shoulders of the business and its users. Users must rely on Internet mailing lists and newsgroups for information, as dedicated support resources are often unavailable. In short, there are monetary and complexity costs that need consideration with both commercial and alternative packages.

For an introduction of encryption technology, a good starting point is the [Pretty Good Privacy \(PGP\)](#) software application. This package provides the user with capabilities to encrypt, digitally sign and verify data including files and email. A version of the software is available free of charge for private, non-commercial use from Network Associates at www.pgp.com. Commercial organizations are required to purchase the software. A freely available alternative to PGP called GNU Privacy Guard is available at www.gnupg.com. Other encryption software can also be downloaded freely from the Internet.

A listing of these and other encryption products and product reviews is available at [SecurityFocus.com](http://www.securityfocus.com) in the products menu in the 'Home' Focus Area.

Relevant Links

[Deciphering Encryption Technology: How it works and how you can use it](#)

By Andrew Brandt and Alexandra Krasne, PC World

[Encryption and Authentication](#)

From the Trans-European Research and Education Networking Association

[The Eagle Flies at Midnight](#)

From PC World

[Stored File Encryption: Boiled Eggs And Scrambled Data](#)

By Philip Carden, Network Computing

[Privacy Statement](#)

Copyright 2006, SecurityFocus