Title:
Is Your Data Encryption Really Secure

Word Count:
1521

Summary:
An article about various types of data encryption and how you might have a false sense of security

Keywords:
Data Encryption, File Encryption, Folder Encryption, Volume Encryption, E-mail Encryption

Article Body:

How Do You Know Your Data Encryption is Really Secure

There are various types and methods of data encryption. Some of the most popular forms of data encryption include single file encryption, folder encryption, volume encryption, whole disk encryption, and of course email encryption.

The Windows XP operating system has the ability to perform file and folder encryption. There are 3rd party tools, like PGP Desktop, which can perform whole disk, logical disk, file, and e-mail encryption.

If you routinely deal with confidential or sensitive information, or if you are concerned about private information falling into someone else's hands, encryption may be the way you want to go. However, there are a few things you should be aware of so you don't have a false sense of security.

First, What Is Data Encryption

Throughout ancient and modern history people have come up with ways to mask, hide, and verify that information is secure or valid. For instance; the ancient Babylonians in 4000 B.C. used something call intaglio, a process in which images and writing were carved or etched into stone that identified certain Babylonian merchants when they were trading. Each trader, or merchant, had a specific intaglio to make his mark, this way his customers would know that what they were purchasing belonged to, or was produced by, a specific merchant. This is a bit different then encryption, more like today's digital signature, another process typically part of data encryption.

Encryption today is much more advanced and complex. It is used for everything from securing military secrets to keeping intellectual property confidential. There are various forms of encryption techniques, some stronger or more secure than others. In it's basic form, encryption can be thought of as the masking, or the scrambling of original human readable information. The person who is masking the information must provide the person he is sending the information to with some sort of key that allows them to unscramble the information so they can make sense of it. For instance; I use encrypted e-mail messages so I can correspond with my customers on a regular basis. I do this because during certain types of projects my customers and I discuss private information such as security holes discovered during security assessments. This type of information is obviously not something we would want to fall into someone else's hands.

Most Data Does Not Start Out Encrypted So Be Careful

The primary reason I am writing this article is to point out a couple specific issues with data encryption. During a recent discussion with a friend of mine he told me that he was using Windows XP folder encryption to secure some of his confidential information. He asked me if I thought this was a secure method of storing important documents. My response was yes and no. The data encryption used by Windows XP is relatively secure, but the issue is that the majority of the data that is now encrypted in the folder did not start out that way.

Let's take for example, a word document that contains your personal financial information. You may have written this document so you have a central location where account numbers, social security numbers, and other private and individual identification information is easily retrievable. After you are finished writing the document, you then transferred it to your secure encrypted folder. Since it is now in a secure folder, only you are able to access it because only you know the pass-phrase that was used to generate the encryption key. For the most part, this assumption is correct.

While you were writing that document, you probably hit the save button several times. Or if you are like me, many times. I've lost lengthy documents several times in the past and have trained myself to hit the save button pretty frequently. Every time you hit the save button, a new temporary version of the file is created. This is typically saved in the c:\documents and settings\"profile name"\local settings\temp directory. This is done for recovery and undue purposes. For instance, if you make a mistake while writing the document and need to undue your actions, one of these temp files may be used to undue the action. Also, if your system or application crashed while writing the document, you can recover it from the temp files stored in this directory. You may have had to go through this before and it works very well.

Now that you have finished your document and copied or moved it to the secure folder, your document is secure, right? Wrong. Chances are the temporary files in your temp directory are still there. Even if you were to delete them, there is a significant chance they can be recovered using open source or very inexpensive undelete or data recovery software. If someone where to get hold of your computer, hard drive, or gain remote access to your system somehow, there is a significant chance the unencrypted original version of your document can be located. So what can you do to make sure that your encrypted version of your file and data is the only version. There is not a clear or 100% secure answer to this question but I will share with you how I deal with the issue.

Changing The Location Of Unencrypted Temp Files

The primary way applications like Microsoft Word determine where to store temporary versions of your files is by looking at two user environment variables. One called "tmp" and one called "temp". They can be accessed by right clicking on "my computer", choose properties, then choose the "advanced" tab and click "environment variables". Here you can edit or change the default location for temporary files. One thing I have to point out is even though a large number of software packages use these locations for temporary storage, it will be hard to determine if they all do or if they save temp files in other locations. You will have to do a little investigating to determine where various applications store their temp files. On my system, I have changed these variables to point to an encrypted disk where I store my encrypted data and files. This way, I can be reasonably sure that temporary or working versions of the files are also encrypted.

Encrypted Files May Not Stay Encrypted When Copied or Moved

Another thing you should be aware of is what happens to encrypted files or folders when they are copied or moved to another location. If a file or folder that has previously been encrypted is copied or moved to another Windows NTFS partition or volume, the encryption is preserved (under most circumstances). However, if you move or copy the encrypted data to volume or partition that is not NTFS, the file is automatically decrypted. Also, just because a file is encrypted on your hard disk it does not mean that this file will be encrypted when you e-mail it to someone. E-mail encryption is a totally different procedure. Also, keep in mind that encrypted files are decrypted when they are transmitted over a network connection.

Make Sure Deleted Unencrypted Files Are Really Gone

Because data that is deleted from disk may be recoverable for quite some time, I use another procedure to limit or reduce the risk of this possibility. As I mentioned earlier, data that has been deleted can in many cases be easily recovered using off the shelf software. In order to be reasonably sure deleted data is not easily recoverable, you need to write over that portion of the disk where the file and it's fragments were located. Actually, you most likely need to do this multiple times just to be sure the data is unrecoverable. The PGP Desktop software I use to create encrypted file systems, send encrypted e-mail, and create encrypted zip files also has a tool called "Wipe Free Space". This tool will write random patterns of data to all space on a drive that is flagged as free. You can tell the software how many times to perform this procedure but the default it usually three passes. My primary system performs this task every night. This way I can be reasonably sure the unencrypted versions of my encrypted files are not just sitting around waiting to be recovered.

Conclusion

If you are concerned about keeping important data confidential, file, folder, or disk encryption is a good solution. If configured properly you can be reasonably sure that your private information will remain private. Just remember that most data does not start out encrypted and that remnants of the original information may still exist in an unencrypted state. There are many options with regard to data encryption; Windows XP native file and folder encryption, open source encryption solutions, or commercial encryption solutions such as PGP (Pretty Good Privacy). Do some research up front to determine which may be the best method for you.

Original URL (The Web version of the article)

http://www.defendingthenet.com/NewsLetters/IsDataEncryptionReallySecure.htm