

RANDOM

William Blinn
COMMUNICATIONS

179 Caren Avenue
Worthington, Ohio 43085
614-785-9359
Fax 877-870-4892
www.Blinn.com

May 2007

COMMUNICATIONS WITH A PURPOSE

THOUGHTS

Security that's not secure leads to security that is

I ran across a report in Tweakers.net about a “secure” USB drive that isn’t very secure. Losing a thumb drive with 2GB or more of personal or business data on it can be a huge problem. Those devices are small and easy to lose, so it’s no surprise that a lot of them have been lost.

Sipal International released a thumb drive called Secustick, claiming that it would “self-destruct” if the user entered an incorrect password more than a set number of times. The stick was commissioned by the French government (I’m thinking *Maginot Line* here) and a 1GB thumb drive (\$175, compared to standard 1GB thumb drives at \$10 or so) turned out not to be very secure.

The Tweakers site mentioned an application called TrueCrypt, so I decided to take a look. TrueCrypt can encrypt the data in a file, directory, or an entire device (hard drive or thumb drive, for example) and it can encrypt it in such a way that even if you are captured and forced to give someone the password, the data will still be encrypted.

Hidden in plain view

TrueCrypt creates a virtual encrypted disk within a file and mounts it as a real disk allowing encryption that is automatic, real-time, and transparent. It provides two levels of plausible deniability, “in case an adversary forces you to reveal the password.” These two levels are the option to create a hidden volume and the fact that TrueCrypt volumes cannot be distinguished from random data. That is, they contain no specific header, footer, or other marker.

Reading the manual for this free, open-source application made me think that I had fallen into a James Bond movie and Q had just handed me a manual for the latest high-tech device that would certainly save my life in the next episode.

After installing TrueCrypt, I quickly worked my way through the beginner’s tutorial and created a file on drive C. That file became an drive that I could easily mount and dismount. Mounted, it appeared in the Windows Explorer. Dismounted, it appeared only as a file.

There was nothing to distinguish this file from any other file on the disk, except for its name. I cleverly called the file “TrueCrypt”. Needless to say, this would not be a wise name to use if you want to keep data private.

If you want to hide data, placing the file in a directory with a lot of other files and naming it something that won’t call attention to itself (“devcache.dll” in a directory with an

application or “Wooly Bully.mp3” in a directory stuffed with hundreds of music files would be good choices.) You know where to look for it, but nobody else would know that the file isn’t what it claims to be.

Each drive needs a password

When I created the encrypted drive, I used a relatively short (8-character) password and TrueCrypt asked if I wanted to proceed. The longer a password is, and the more types of characters it contains, the more secure it is.

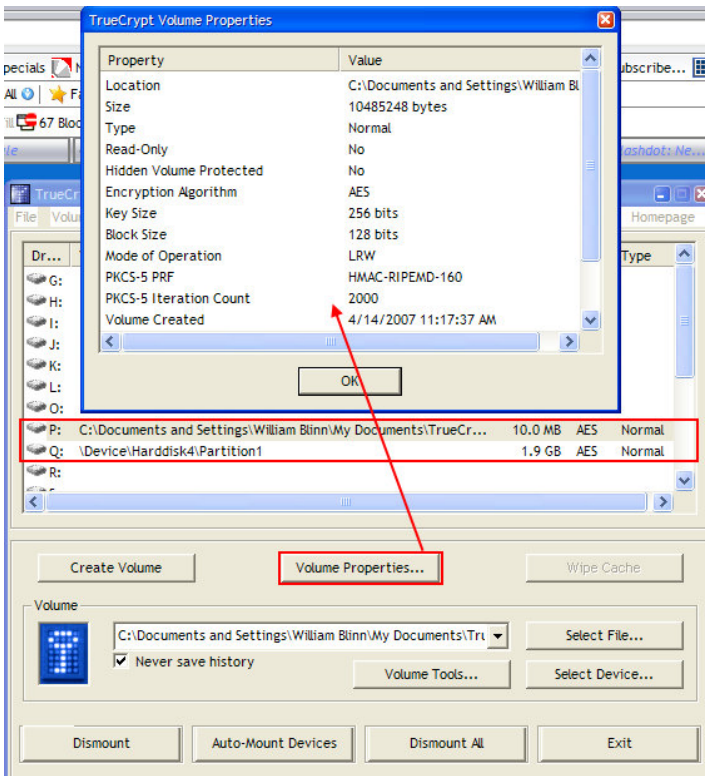
A password can be long and still be memorable. It can even be something that you can write a reminder for without making it something that others can decipher. *Yellow3755Submarine4cats* is a password nobody would guess even if you left a note to yourself: *We all live in the Beatles song at my childhood street address and how many animals lived with us?*

TrueCrypt is not a particularly good choice if you want to take a thumb drive to another computer and use it, but there

TrueCrypt precautions

If you download TrueCrypt, read the instructions. If you just run the program and follow the on-screen instructions, you might choose to encrypt an existing file, folder, partition, drive, or USB device. If you do that, any data that was on the device will be erased. In other words, TrueCrypt does not encrypt files in place. You create an encrypted device or directory and then you put files there. Files placed in the special directory are encrypted.

And what about terrorists? If you think an application such as TrueCrypt might be valuable to a terrorist, you’re correct. That can’t be helped. Any technology can be used for good or bad. Stones can build a house or be a murder weapon. Fire can warm us or kill us. If we ever manage to find a way to instill tolerance in all the people of the world (including ourselves), then devices and technologies will be used only for good. Until then, TrueCrypt exists and if you have information that you want to protect, this is the way to do it.




malfunctions can cause files stored on a TrueCrypt to become corrupted, so you should backup all important files regularly.

At the very least you should backup the volume header, which contains the master key because a damaged volume header will make the volume impossible to mount.

A file system within a TrueCrypt volume may become corrupt in the same way as any normal unencrypted file system. When that happens, you can use file system repair tools supplied with your operating system to fix it (chkdsk for Windows users.) TrueCrypt provides an easy way to use this tool on a TrueCrypt volume: First, make a backup copy of the TrueCrypt volume (that's because chkdsk may make the damage even worse) and then mount it. Right-click the mounted volume and select Repair File system.

Need security? Use TrueCrypt.

The cost (nothing) and the power (amazing) of TrueCrypt combine to make this an application a must-have if you ever take sensitive data home from the office. Even FBI agents lose laptop computers, thumb drives, and guns. TrueCrypt is a good way to make sure that the data you're responsible for doesn't go astray.

For more information, visit the TrueCrypt website at www.TrueCrypt.org. 

is a "Traveler Disk Setup" option, but that option will probably leave some traces of TrueCrypt in the Registry.

It's possible, but somewhat difficult, to use TrueCrypt without leaving any traces. Doing this requires using TrueCrypt's "traveler mode" under BartPE, "Bart's Pre-installed Environment", which is essentially the Windows operating system prepared in a way that it can be stored entirely on and booted from a CD or DVD. The Registry, temporary files, and such are all stored in RAM. The host computer's hard disk is not used and does not even have to be present.

The freeware Bart's PE Builder can transform a Windows XP installation CD into BartPE. As of TrueCrypt 3.1, you do not need any TrueCrypt plug-in for BartPE. Simply boot BartPE, download the latest version of TrueCrypt to the RAM disk (which BartPE creates), extract the downloaded archive to the RAM disk, and run the file 'TrueCrypt.exe' from the folder 'Setup Files' on the RAM disk (the 'Setup Files' folder should be created when you unpack the archive containing TrueCrypt).

Oddities and concerns

For encrypted USB devices, I sometimes see the message that tells me the device is still in use when I try to eject it even though I have dismantled the encrypted drive.

This is a Windows and Linux application. If you use a Mac, you will not be able to use the application.

Corruption happens


You're probably wondering what happens when part of a TrueCrypt volume becomes corrupt. When you're dealing with encrypted data, one corrupted bit usually corrupts the whole ciphertext block in which it occurred. The ciphertext block size used by TrueCrypt is 16 bytes (128 bits) so that if data corruption occurs within a block, the remaining blocks are not affected. Hardware or software errors and

I have to admit that I've been a bit slow at adopting some modern technology. Until last month, invoices went out by mail even though it's been possible (even easy) to send invoices electronically. Starting in April, invoices went out electronically, but payment still required a check. Now that has changed.

Starting this month, you'll notice a message on your invoice that directs you to an on-line payment page. There's no requirement that you use this method. Send a check if you wish. Or bags of quarters. I'm not picky when it comes to accepting payment.

But if you'd prefer to pay on-line because it's faster or easier or because you don't have to prepare and mail a check, you can now do that with any major credit card (American Express, Discover, Master Card, and Visa) or with your PayPal account.

Payments are processed by PayPal, but paying via the Web based form doesn't require that you have a PayPal account.

Also new this month: *Random Thoughts* (which was not published last month) is now entirely an electronic publication, which means that the time between my sending it and your receiving it is about 5 seconds. 

on the market by A.J. Stinnett

CORNER

"Successful managers praise employees when they do high-quality work, ensure that employees who do the same type of work receive equal pay, and reward employees for superior performance."