Securing a External Drive

Contributed by Dr. Apocalypse

Sunday, 25 December 2005

Note:

I wrote this article and submitted it to 2600. It was published in the Autumn 2005 issue (Volume 22, Number 3).

Intro:

Before I begin let me say that the following techniques only applies to Windows (sorry). What you need in order to follow the steps I'm about to describe: one external hard drive, one USB flash drive, a program called Sentry 2020 [1], Windows XP, and some common sense. First I'll outline the basic steps from a theoretical standpoint and the go into detail. There may be other programs out there like Sentry 2020, but this is the best one I've come across for this so far.

Basics:

What we're going to do is create a virtual drive (called a data file by Sentry so I may interchange the two terms) on our external hard drive. All of our private information should be stored in the virtual drive on our external hard drive. The data file will require an encryption key to decrypt all of the data stored in it before we can see it. Sentry provides us with 10 encryption algorithms ranging from 56 bit all the way up to 1024 bit. The key will be password-protected and we will chose to store it on our USB flash drive. This will make it impossible to access the files on our external hard drive without inserting they USB drive. Obviously, you do not want to leave this USB drive near your computer when you don't need to access these files. I suggest keeping it with you at all times (it's small so it can easily fit in your pocket), so that in the unfortunate event that authorities (or anyone for that matter) try to access your drive they will have no way of decrypting or reading the files on your external drive.

Specifics:

Now we shall dive into the details of doing what I just described. First open Sentry and click the three dots next to the entry field labeled "Key File" to create your encryption key. Make sure you store this on the USB drive. Next, chose where your data file will go. Remember, this is the virtual drive that will hold all of your files so I'd recommend putting this on your external hard drive [3]. I think it would be wise to use maximum capacity on your external hard drive for the data file because someone may come up with a vulnerability for Sentry in the future that allows someone to gain access to the data file if they have access to the unencrypted space on the same drive. Plus, if you underestimate your storage needs and you need more space than you allowed yourself at some future point in time, you will have to resize they data file which erases everything in it at the time of the change. (Technically I think you have to delete the virtual drive and creating a new one with a bigger size.) Now it's time to chose your algorithm of choice and set your password. Use some common sense here: no easily guess able passwords! Choose your drive letter; nothing to really consider here as it's just a personal preference. And finally, set the timeout. I assume this means it will disconnect after a certain amount of minutes of inactivity, but I am unable to test this because I don't have any files large enough to take a an exorbitant amount of time transferring. Don't set this value too high because that would be a security risk. Don't make it read-only at first because Windows will need to format it the first time you mount it, and it needs write access to do this. If you're really paranoid go ahead and make the data file read-only whenever you mount it as long as you don't need to put any new files in it.

Other Security Precautions:

1. Make sure you don't have any viruses, keyloggers, or spyware on your computer because we wouldn't want anyone to know the password we chose.
2. One of the pitfalls of any encryption scheme is that in order to decrypt something your key or passphrase must be loaded into memory. To keep the feds from obtaining a RAM dump from your machine turn off automatic memory dumping and delete any dumps on your system. To do so: right click on My Computer > Properties > Advance > Startup and Recovery Settings > Write debugging information and set it to "none." Delete %SystemRoot%\Memory.dmp to remove the last memory dump. Get rid of any memory dumps that occurred automatically upon receiving the infamous Blue Screen of Death by deleting the folder %SystemRoot%\Minidump [4].

3. As you should know, using the Recycle Bin does not get rid of files permanently! They can still be recovered. To remedy this I recommend wiping the free space on any of your hard drives (with multiple passes) weekly. Many free utilities exist that do this for you.

4. Delete your paging file (sometimes called a swap file) when you shutdown your computer. To do so: click Start and select Run; type "regedit" (sans the quotes) and push enter. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management and change (Right click on it and select Modify) ClearPageFileAtShutdown to 1 (binary for true) [5].

Extention (for the really paranoid):

One technique for added security I thought of one day is creating a data file within a data file. This can be repeated several times [6]. Just make sure that when you create a virtual drive within another virtual drive that you make the second data file slightly smaller in size than the one it's created in [7]. For each data file use a different algorithm in order to slow anyone down that's trying to crack into your secret stash. More importantly, use a different password for each level in your hierarchy (i.e. primary, secondary, and tertiary data files). Make sure you dismount every virtual drive before closing Sentry! In my testing I was still able to access a file inside of a data file that was in another data file, which in turn was inside yet another data file after dismounting the highest level virtual drive and exiting Sentry.

Sources and Footnotes:

[1] http://www.softwinter.com/ Free to try; $50 to purchase.

[2] I use a PQI Intelligent Stick 2.0 (512 MB, about $55).

[3] If you don't have an external hard drive you may use the internal

one in your computer, a zip drive, a floppy, or another USB drive; the only real requirement here is that your storage medium is large enough to hold whatever you want protected. The same goes for the USB drive: it may be replaced by a floppy or CD or something similar, but both of those options are harder to safely and comfortably transport.

[4] 2600: The Hacker Quarterly Volume 21, Number 3, Page 8-9.

[5] http://www.tweakxp.com/tweak31.aspx

[6] Note: Windows was unable to format a 2MB data file I created within a 5MB data file, which was in turn created inside of a 10MB file. I went with the default NTFS setting for the 5MB and 10MB virtual drives and didn't experience a problem; when I tried using NTFS for the 2MB volume I got an error, but Windows correctly formatted the 2MB data file using FAT.

[7] Note: Don't try to access the data file directly by clicking on its icon; use the shortcut to it that was created in My Computer for you.

- Dr. Apocalypse (dr.apocalypse@gmail.com)