Worst case scenario - protecting your computer

How to keep sensitive information safe

John Locke

In my last article my laptop had died a spectacular death from a full cup of coffee. I had to send it into the IBM depot, where they replaced nearly everything but the battery. Including the hard drive.

My files were all properly backed up, and I was even able to retrieve the few files I had worked on that day by connecting the drive to another computer. So when the service depot called and said they wanted to replace the drive, I said go ahead.

Now, from a security point of view, the rule of thumb is to destroy all data on hard drives before passing them on. However, if your computer gets stolen you may not get the opportunity. Let's take a closer look about what you can do, why and how.

If you have financial files that include account numbers, or store passwords on your computer, you definitely want to have protection for them

Who cares if someone gets my hard drive?

You may not care. Many people don't. In this day of identity theft, however, being too cavalier about your data may be foolhardy. While there are plenty of other ways that misanthropes have found to hijack your identity, getting financial details off your computer is one of the easy ways, if they get hold of your hard drive. There are basically three reasons to protect data on computers that could be stolen, in increasing levels of paranoia:

1. Because you might get sued or go out of business if the information falls into the wrong hands
2. To prevent identity fraud or theft
3. To protect your privacy

In my business, I work with a lot of different clients. For some of them, I have signed a confidentiality agreement, agreeing not to reveal any of their internal product or business lines. If my laptop were to be stolen with confidential material on it, I could be held liable. This type of information absolutely must be protected.

If you have financial files that include account numbers, or store passwords on your computer, you definitely want to have protection for them. Any geek with a computer could find this stuff on your hard drive, and if the temptation is great, and their ethics loose, they might put your information to misuse.

Even your non-confidential stuff - email, letters, and spreadsheets - may be enough for someone to impersonate you and get credit in your name, or assume your identity when they commit a crime.

What should I pay attention to?

Okay. Let's not get too alarmist here. There are risks involved with setting foot outdoors. In my house, there can

be risks involved without going outdoors. Worrying about the security of your data should not keep you up at night - if it does, I highly recommend you stop reading right now, unplug your computer, run it over with your car, hack it up with an axe, and move to a teepee in Manitoba. I hear there's plenty of deer running around up there, and with our climate changes, there should be some good farming up there soon.

But if you're determined to stay online, just take a moment to think about the kind of data you have on your computers. The same data I considered in my disaster recovery article, and before that, in my password strategy article. Do you have any data you absolutely don't want to have fall in the wrong hands?

Don't bother with email - it has already gone unencrypted through that filthy, spy-infested internet. But do pay attention to your financial records, and especially to any files you've copied (securely, I hope!) from any company file share. If you're responsible for keeping any of that secret, you'd better not leave it unencrypted on a laptop hard drive, especially not in public places.

A general rule of thumb is that increasing security directly hampers convenience. On certain systems, however, encryption has been made very easy to do

For all of the employees out there carrying laptops owned by your employer, you can relax - it's the job of your IT department to make sure their data is properly secured, not yours. But if you have client data, you could be held responsible if it falls into a competitor's hands.

Encryption to the rescue

Luckily, there are some very secure ways to protect your data, using one of a few different types of encryption. I'm not going to get into detail about how encryption works, or what varieties are out there. But I am going to look at three different systems that can be used to encrypt data on your hard drive. They vary based on who can decrypt the data, where you can apply the different encryption types, and how automatic the whole process is.

A general rule of thumb is that increasing security directly hampers convenience. On certain systems, however, encryption has been made very easy to do.

Windows Encrypted File System

This is one area where Microsoft gets it right, with their "Encrypted File System," or EFS. EFS comes with Windows XP Professional, but not XP Home. If you have XP Pro, and your hard drive is in NTFS format, you can encrypt any file or directory by following these steps:

1. In Windows Explorer, right-click the file or directory, and choose *Properties.*
2. Click the *Advanced* button.
3. Check the *Encrypt* checkbox, and click OK.

That's it. Whatever you have encrypted, is now completely secure, even if your hard drive is stolen - unless the attacker guesses your password. EFS works by using strong encryption to hide the data, and then it uses a certificate associated with your login to protect the key. If you log in using another user account, or try to read the files from Linux, you won't be able to get to them.

The downside is, if your administrator resets your password, you lose all access to the encrypted files because the certificate is deleted. It's possible to create a recovery disk *before* you reset your password, but otherwise you're hosed. Another drawback is that you can't back up an EFS file or directory while it's encrypted.

EFS works well for laptops, and I encourage you to turn it on for specific directories, to keep anything you store there safe should you lose control of your hard drive. This system depends upon having a strong log-in password, though, and disabling automatic logins.

Mandrake DrakLoop

Encrypting files, and entire hard drive partitions, is built into most modern Linux distributions. Mandrake provides a nice graphical utility for creating an encrypted drive, called DrakLoop. If it's installed, you can find it under System -> Archiving -> Other. If it's not there, go to the Mandrake Control Center to install software, and search for a package named "mountloop". You'll probably be asked to choose

Fig. 1: Finding DrakLoop in the Mandrake 10.1 menu

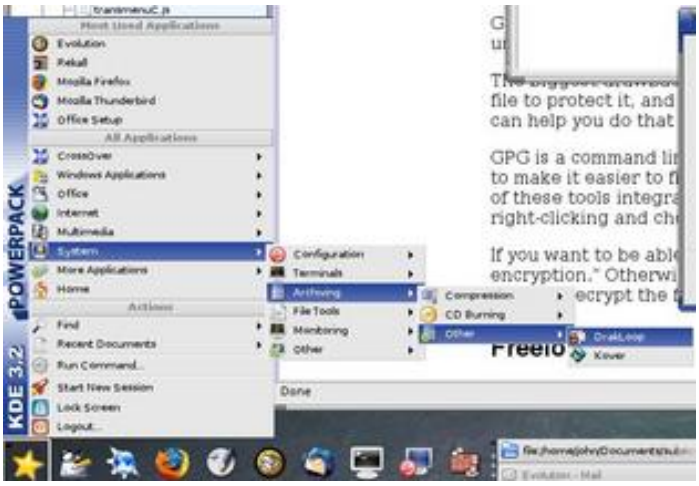


Fig. 2: Setting up an encrypted directory in Mandrake Linux

between a couple of different packages for asking for your passphrase - I've found the "openssh-askpass-gnome" package to be slightly nicer to use.

With DrakLoop, you create a big file of a fixed size, and it is mounted on your system very much like a disk drive. When it's mounted, you can use it like any other directory, storing files, running programs, or whatever you want from this file. When it's unmounted, it's just a single encrypted file, and nobody can determine its contents.

The entire contents of the file is encrypted using a passphrase that you provide. Anybody with the passphrase can decrypt the file and get to its contents. Without the passphrase, it's protected. One advantage of this system is that it's super easy to use, and can be safely backed up in encrypted form with little extra effort. A disadvantage is that you always have to type in the passphrase to mount the file. Another disadvantage is that if you set up additional encrypted directories, you have to type in the passphrase for each one.

To set up an encrypted directory with DrakLoop:

1. Click the Mandrake star, point to **System**, point to **Archiving**, point to **Other**, and click **DrakLoop**.
2. Click the **Add** button.
3. For Directory, type a new path. If you use an existing one, it may delete data in there. For example, I used **Documents/encrypted** for mine.
4. For Size, make it big enough to contain as much data as you'd like to encrypt. If you plan to back up to CD, and have enough disk space, you could make it around 650 MB to make this simple.
5. You can choose between different levels of encryption, from aes128 to aes256. The larger numbers provide even more secure encryption, at the expense of more processing involved. I've stuck with the minimum aes128 for mine.
6. Finally, type in a good strong passphrase in both the password and confirmation boxes. Even though it says password, this should be a passphrase of five or six words, at least 20 characters. Try Diceware (`http://diceware.com/`) for a good way to generate a secure, memorable passphrase.

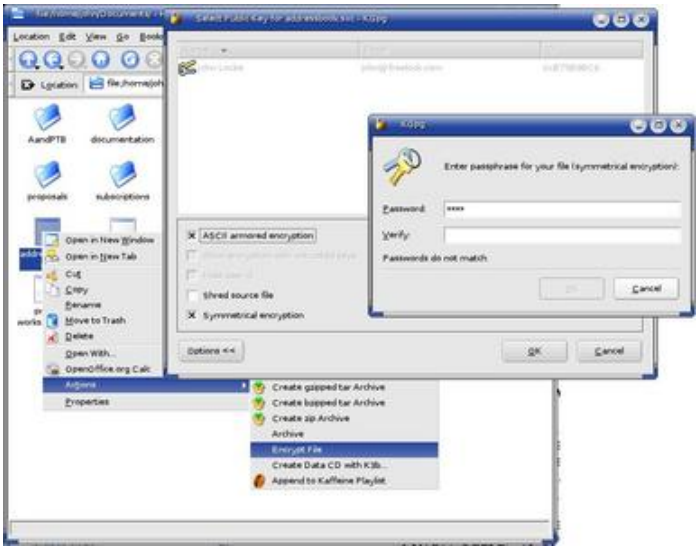
Click **OK**, and you're done!

With DrakLoop, you can always open this program to mount or unmount your encrypted directories. Mandrake will automatically ask for your passphrase when you log in, allowing you to automatically mount the encrypted directories at the start of your session. To encrypt files, simply copy them into the directory you specified, when it's mounted.

KGPG and Windows Privacy Tools

So what if you don't have Windows XP Professional, or Mandrake Linux? The underlying system that DrakLoop uses is available in pretty much any modern Linux system, there just isn't necessarily a nice interface for setting it up. It's also possible to set entire disk partitions to be encrypted, requiring a passphrase to unlock them when you boot the computer. I'll leave it to Google to help you with that.

Fig. 3: Using KGPG to encrypt a file. In Konqueror, right-click the file, and find the encryption option. The figure shows Symmetrical encryption, which uses a passphrase for encryption, instead of a key



But an entirely different way of encrypting files is worth mentioning here. A system called "GNU Privacy Guard", or GPG, provides a way for you to encrypt any file on any operating system. You can encrypt it in such a way that anyone with the passphrase can read it, or so that only specific people can decrypt it. It's based on an earlier system called "Pretty Good Privacy", which infringed on some patent rights and got pulled from the market.

"GNU Privacy Guard", or GPG, provides a way for you to encrypt any file on any operating system. You can encrypt it in such a way that anyone with the passphrase can read it, or so that only specific people can decrypt it

GPG is available for every operating system in wide use, and it's completely cross-platform. The system is used to encrypt email as well as files, and provides several different types of encryption.

The biggest drawback to GPG is that it takes manual intervention to use - you have to explicitly encrypt a file to protect it, and decrypt it before you can use it. But if you have data you need to keep secure, GPG can help you do that *and* share the file with other specific people.

GPG is a command line tool, but it is built into several other programs that can provide a graphic interface to make it easier to figure out. For Windows, try Windows Privacy Tools (`http://winpt.sourceforge.net/`). For Linux, give KGPG a shot - use the software installer with your distribution to install it. Both of these tools integrate right into the file manager, making it so you can encrypt or decrypt files by simply right-clicking and choosing the action in Windows Explorer or Konqueror.

If you want to be able to decrypt the file with a simple passphrase, make sure you choose "Symmetrical encryption". Otherwise you need to select a person to encrypt the file to, and only the person with that key can decrypt the file.

Encryption is easy

I've only scratched the surface of encryption technologies in this article. It certainly gets a lot more complicated than this, and there are many different systems and ways of using them than I've mentioned here. But what I've shown is that you don't have to be a security expert to use encryption technologies to protect sensitive files.

Copyright information

About the author

John Locke is the author of the book *Open Source Solutions for Small Business Problems.* He provides technology strategy and free software implementations for small and growing businesses in the Pacific Northwest through his business, Freelock Computing (`http://freelock.com`).