File and Disk Encryption

Modern operating systems allow you to use a system of accounts and passwords to limit access to data on a computer. This may be useful when adversaries have casual passing access to your machine, but those accounts and passwords will not protect your data if your computer is stolen or seized — or if the adversaries have more than a minute or two alone with your computer. There are many ways (such as plugging your hard disk into another computer, or booting another operating system using a CD or USB key) that would allow files to be read off the disk. Even deleted files may be recoverable.

The theft or seizure threats can be mitigated by encrypting the data on the disk. Some sort of mitigation is especially important for laptops, which are at high risk of being lost or stolen, but the same measures can be useful for improving the security of any client or workstation-type computer.

Full-disk encryption is meant to protect stored data against this sort of exposure, if the computer is stolen or seized when it is powered off. If the computer is seized while running, there are tricks that sophisticated adversaries could use to read the data regardless of encryption.

File encryption is disk encryption that only applies to certain specific files on your computer. It may be easier to deploy but is vulnerable to several threats that do not apply to full disk encryption.

Hard disk passwords are a feature offered by many laptop manufacturers. These can be enabled within the BIOS of your computer. Hard disk passwords *don't encrypt any data on your drive*, they just prevent the drive from cooperating with the computer until the password is supplied. There are numerous commercial services which will disable these passwords for about $100 per drive. So a hard disk password is useful against a casual thief, but of no use against law enforcement or other non-casual adversaries.

Should I Encrypt My Drive?

Everybody should use either disk encryption or a hard disk password (possibly augmented with file encryption) on their laptops. If your laptop has personal data but you would not regard any of it as sensitive, a hard disk password may be quick and easy, and sufficient protection in case of theft.

If your computer contains a very small and easily quantified set of somewhat sensitive documents, it may be sufficient to use file encryption for those documents, alongside a hard disk password.

If you computer contains a larger (or harder to quantify) set of sensitive documents, or any documents which might be considered *highly* sensitive, it is best to use full disk encryption. In such cases the threat posed by malware should also be taken into account.

Disk Encryption Is Of Little Use in Civil Lawsuits

It is extremely important to note that disk encryption is unlikely to offer much protection against civil litigation. Many of the procedural obstacles which might apply to law enforcement attempts to obtain encrypted data during a criminal investigation would not apply in a civil case. If an adversary in a civil case persuades a judge to issue a subpoena for your data, a failure to decrypt and disclose the data would be held against you in the case.

If your threat model involves civil litigation, it is essential to simply not have the data on a computer in the first place, or to have secure deletion practices in place long before any lawsuit is filed. Once a lawsuit is filed, you will be obliged to preserve any pertinent documents, and the presence of forensic evidence that you deleted data after a suit was filed would have dire consequences.

Choosing Disk Encryption Software

There are many full-disk encryption tools. Using a mainstream one is probably safer than an obscure one, since mainstream disk encryption products have usually received more expert review. Leading disk encryption programs include BitLocker, PGPDisk, FileVault, TrueCrypt, and dm-crypt (LUKS); some of these come with the operating system, while others are third-party add-ons. You can read a detailed comparison of these and many other disk encryption products from a comparison at Wikipedia. This comparison may help you select a disk encryption product to meet your needs, but any of these systems can protect your data better than having no disk encryption
at all.

Things To Know When Using Disk Encryption

Generally, disk encryption software will require you to enter a separate disk password when you turn the computer on or start using the disk (some systems can use a smartcard instead

of or in addition to a password). To be effective, this password must be resistant to all forms of automated guessing. Remember that the disk encryption is fully effective at preventing access to the disk when the computer is turned off (or the encrypted disk is entirely *unmounted* or removed from use); to get the full benefit, you should unmount the encrypted disk or turn the computer off in any situation where the risk of compromise is especially high, such as a computer left unattended overnight or a laptop being carried from place to place. (Using disk encryption without following this precaution scrupulously will still provide more protection against some attackers than not using disk encryption.)

Finally, full-disk encryption can also be used on servers, providing some protection against seizure of the servers. However, even servers with encrypted hard drives could be vulnerable to attackers with specialized techniques if they're seized while they're operating. Proper use of disk encryption on servers can also be a nuisance because the server can't do a fully unattended automatic reboot. (It's not safe to store the password for the disk on the server itself, so an administrator will have to enter the disk password whenever the computer is restarted.)

Plausible Deniability

One interesting property which some disk encryption developers are working towards is **plausible deniability**. The goal of these efforts is to offer users a way to not only encrypt their files, but to prevent an attacker from being able to even deduce the existence of some of the encrypted files. The user will have a way to "plausibly deny" that the files exist.

One example of this concept is TrueCrypt's ability to have an encrypted partition (which can be hidden as any file on your hard drive) and within that partition hide another partition. One password will reveal the outer partition and another separate password will reveal the inner one. Because of the way TrueCrypt encrypts the partition table itself, an observer cannot detect a hidden partition even if she has access to the "regular" encrypted share. The idea is to give the user something to decrypt if a law enforcement officer or Customs official asks, while keeping the rest of their information secure.

In practice, TrueCrypt's first attempt to implement this feature was shown to be ineffective because operating systems and applications leave so many traces of the files they work with, that a forensic investigator would have many avenues by which to determine that the inner partition existed. The TrueCrypt developers have responded to this research by offering a way

to install and boot from an entire separate operating system within the inner partition. It is too soon to know whether their new approach will turn out to offer secure plausible deniability.

Technical issues aside, remember that lying to a federal law enforcement officer about material facts is a crime, so if a person chose to answer a question about whether there were additional encrypted partitions on a computer, they would be legally obligated to answer truthfully.