

Laptop Security, Part Two: Protecting Information on a Stolen Laptop

Josh Ryder 2001-08-13

Laptop Security, Part Two: Preventing Information Loss

by Josh Ryder

last updated August 13, 2001

In the [first installment of this series](#) on Laptop Security we discussed methods of preventing laptop theft using both hardware and software solutions. This article will cover some good methods of mitigating loss when a laptop has been stolen. As was stated in the first article, while a the software and hardware that makes up a laptop can be replaced at a limited cost, the information that may be lost when a laptop is stolen or lost may be invaluable or irreplaceable. This article will discuss ways in which to limit the loss of information.

Let's assume for a moment that your laptop has been stolen, how worried would you be? Would you be able to rest easy at night knowing that nothing short of a full-blown NSA sanctioned attack against your machine would result in any useful data being uncovered, or do you rely on the vagaries of password protection? This article will endeavour to introduce readers to techniques that will allow readers to sleep easy, secure in the knowledge that their valuable information is protected, even if they do happen to lose a laptop.

Preventing Your Stolen Laptop From Being Used

Once your laptop is out of your possession you probably don't want whoever took it to use it. There are several methods of making a thief's life more difficult when they try to access your machine.

Set a BIOS password

If the very first thing a thief sees when they turn on a machine is "Please enter boot password: " they'll know that they are in for a load of trouble. If memory serves, some older Sun workstations had a small EPROM in them that would, after receiving the incorrect password three times, fuse themselves solid, physically preventing the machine from continuing operation. While this level of security is not available today (to the best of my knowledge), most computers offer a similar degree of protection by allowing the owner to set a boot password. Typically most will prompt the user three times to enter a password, then refuse to boot if there are three failures (however, if you restart the machine, you will once again have

three guesses). Removing a password-protected BIOS and boot-sequence typically involves physically opening the computer and removing the CMOS battery (which may clear the BIOS information) or shorting some jumpers to reset the BIOS to a default state, a process which is both time consuming and risky to the thief (playing with screwdrivers and an open computer is often a recipe for disaster).

Set a Login Password

If you are running an operating system that supports proper logins (Windows NT/2000, Linux, or BSD to name a few) setting a password is not only a good idea, it is required. To successfully login to the computer, you must provide a login name and password. If the information entered is incorrect, the operating system will refuse to allow you to become an active user.

As implied in the introductory section of this article, passwords should not be relied upon as the sole piece of security on your machine. Under Linux, a brute-force attack can be staged on your password file, or more simply a person could use boot and root floppies to bypass your password and logins completely, having unfettered access to all of your information. The password situation for Windows is just as bleak. If your computer is not using NTFS, accessing the data on your hard disk is trivial. A simple DOS boot disk will allow anyone to view the contents of your hard drives.

Running NTFS doesn't necessarily protect you either. While NTFS isn't directly readable from a DOS floppy, you could use a utility such as NTFSDOS that will allow you to mount an NTFS drive (allowing the user to manipulate your information as they see fit). A further vulnerability when using Windows NT/2000 is a little program called NTPASSWD which can create and modify existing logins and passwords without prompting for the original password. This is detrimental as someone could potentially change the Administrator password to be whatever they wanted, allowing them full access to everything stored on your computers hard disk.

Authentication Gestures

As discussed in the previous article, there are hardware solutions that require gestures to be made on a laptop before unlimited access is granted. As was stated in Part One: A third option is [Caveo's Anti-Theft PCMCIA card](#), which will passively monitor the position of a laptop computer. When the system is armed, if the sensors detect that the laptop has been moved outside of the designated work zone, several events can occur. Of course, an alarm can sound

(if it has been enabled), but more importantly, Caveo can shutdown and effectively lock the computer by preventing it from booting without a proper authentication action (more on this in a moment.) It can also optionally secure the keys to your encrypted files. The Anti-Theft card contains motion sensors that monitor the angle and velocity of your laptop. Using these extremely sensitive sensors, users can create a unique gesture password that can be used to arm and disarm the system. For example, my "password" could be a tilt forward, left, back, and right. If those four movements were not performed in sequence, the system would not unlock (and may even sound the alarm).

Preventing Unauthorized Data Retrieval

Let's assume that the thief has bypassed your first line of defense (password protection). What now? Even if an unauthorized user gains access to your laptop, there are still means of protecting the information that is stored upon it.

Encrypted File Systems

Before we can really discuss encrypted file systems, we must first understand what a file system is. Each operating system uses some method to store and retrieve data from your hard disk, and when you format your hard drive, you are basically preparing the drive to accept data from a piece of software that knows how to read and write information in a specific method. Under MS-DOS, your hard drive would be formatted to the FAT (File Allocation Table) standard, under Win95b/Win98 you would format to an updated version of FAT called FAT32. Windows NT and 2000 both have the capability of using a higher performance file system called NTFS (NT File System - original no?). Under Linux and BSD there are several options for the user to choose from, though ext2 seems to be one of the more popular options for a home user.

Without a file system, it is almost impossible for an operating system to read and write data from the hard drive. Normally, if you know how to read a specific format of file system you can generally read the information off of media that contains information stored using that standard. For example, let 's say that you have a computer with a BIOS password, and I don't know how to get around it, but I still want to get the information off of your hard drive. If I was to remove the hard disk from your machine, and place it in mine, I would most likely be able to read all of the information without any difficulty once I mounted the volume on my computer.

Encrypted File Systems typically layer themselves on top of an existing file system. In some

instances you can encrypt an entire partition on your hard disk, and in others you can encrypt individual files or directories. Once your file system has been encrypted, only someone who knows or can guess your password will be able to access the information stored on the encrypted partition (minus those parties who have enough processing power to brute-force break the encryption).

The benefits to running an encrypted file system are fairly straightforward: Only those parties who have permission, and hence the password, are able to read your sensitive information. Even if every computer you own is stolen tomorrow, no one will be able to casually retrieve/view/copy your data stored on the encrypted partition. The drawbacks are somewhat more complicated. Encrypting/decrypting files is a processor-intensive task, and this added computational overhead will cause system performance to lag whenever you need to read/write to an encrypted file system. Some unofficial benchmarks under Linux show that up to a 100% increase in wait times can be experienced when using an encrypted file system. Another drawback is that if the person in charge of the machine somehow forgets or loses the password to the encrypted partition, retrieving the data is extremely difficult. This risk is amplified when dealing with employees leaving or being discharged from the company.

To mitigate the performance hit, many users choose to create an encrypted partition where they store only their data files. By doing so, all of the program-centric operations can occur at normal speed, and only reading and writing of the actual data files will be slower. Unfortunately, this method is not as secure as full file system encryption as the temporary files created by most applications will default to the local unencrypted partition - meaning that it is theoretically possible for a determined individual to find an almost complete copy of your data by reading the "freed" sectors on your unencrypted hard drive.

Encryption

If you don't want to go full-bore and encrypt your file system, encrypting individual files or directories manually may still be a viable option. Programs such as those included in the PGP tool suite will allow you to use strong encryption to protect information that you have stored on your hard drive. As long as your private key is kept safe, no one but you and your intended recipients will be able to view your data. Herein lies the problem. Most users keep their private keys locally on their machine so they can easily encrypt and decrypt files. If someone was able to get a copy of your private key, it is possible to largely bypass the encryption on the files, and read them.

Biometrics

Biometric authentication mechanisms can be used to replace or supplement passwords on most operating systems. The driving idea behind biometrics is to use the uniqueness of certain features of a user, such as retinal pattern, fingerprints, and even typing characteristics, to accurately identify and authorize persons. This type of device would provide a hardware level of authentication that would be required before the machine would even boot up.

As biometric authentication devices become more affordable and portable it is conceivable that every laptop will come with one or two biometric scanners (say finger print and retinal pattern.) However, current biometric technology leaves quite a bit to be desired. Finger prints can be smudged or duplicated, voice prints can be faked with a decent voice recorder, retinal scans are accurate but time consuming, and DNA samples are a long ways off from being practical. Size, speed and expense are all concerns that must be addressed before this technology can become mainstream. And of course, even if this type of technology evolves to the point where it can be widely implemented, it will at that time be subjected to real world testing by thieves and hackers trying to gain unauthorized entrance. Needless to say, if the authentication mechanism is easy to bypass it is useless.

Tracing and Tracking

As discussed in the previous article, there are several worthwhile tracking programs available. Once a computer is reported stolen, the tracking companies will wait for the laptop to send them a location signal (sent whenever the machine is connected to the Internet). When a signal is retrieved, the program will be instructed to broadcast as much information as it can about the current connection (originating phone number, IP address, service provider etc.). When enough information has been collected, the tracking company will notify the appropriate authorities, which will in turn, obtain a search warrant and hopefully retrieve your stolen property.

Some of the more popular tracking companies provide the user with the ability to execute commands remotely to their stolen machine (when it is connected), theoretically allowing the user to delete all of the important information contained on the hard drives. In the best case this ability to execute remote commands would be taken a step further, and you would be able to remotely mount the storage devices on your machine?giving you the ability to run PGP's

Wipe or encryption to totally remove or protect your data.

Computrace has some well developed solutions to assist you with the detection, location and recovery of your stolen machines. The installation footprint is relatively small, configuration is fairly straightforward, and the yearly operation fees are quite reasonable. They also provide asset management software that will allow your IT department to track vital statistics like hard drive usage, which programs are currently installed etc.

Common Sense Practices for Protecting Laptop Data

As mentioned in the first article of this series, it is fine to rely on technological solutions to security problems, but the first thing that people should do to secure any aspect of their information systems must be to implement secure, common sense computer usage habits. The following is a list of a few things that can be done to minimize the potential loss of information in the case of laptop loss or theft.

Protect Your Password

The password is the cornerstone of all computer security. The first and most common sense rule for passwords is to not give out your password. Giving out your password is the informational equivalent of giving away the dead-bolt key to the front door of your house. This one is self-explanatory. A little less obvious, but equally as important is to not write your password somewhere on your laptop, or keep it written on something stored in the laptop case.

In case your laptop falls into the wrong hands, at least make the would-be intruder work for his or her booty. Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower case letters, are not based on words in the dictionary, and preferably that contain some numbers. Don't use the same password for everything. We want to make data retrieval as difficult as possible for the thieves, and using the same password for your login and for files is just making it easy.

Store a Minimal Amount of Data on the Laptop

We should assume, given their portability and value to potential thieves, that laptops are inherently insecure vessels of information. As such, store as little valuable data as possible on them. If you are using a laptop for business, take only those files that are essential for your trip. Why give away more than you absolutely have to? If possible, store the information on a

removable medium, such as a floppy, cd or zip disk.

When not using the laptop, remove the disk and store it separately, away from the laptop. Remember, the hardware and software of a laptop can be easily replaced - not necessarily cheaply, but easily. The information stored upon often cannot be replaced. If you are traveling with proprietary information that may be crucial to the success of your organization or if you are traveling with personal files that are crucial to your own well-being, do not keep those files stored on the laptop. Store it on media in a secure place that is unlikely to be the target of thieves looking for shiny objects.

Of course, the best way to protect your data is to never let it fall into the wrong hands. It is hoped that this two-part series has offered readers to some steps to help avoid this fate.

Relevant Links

[Laptop Security, Part One: Preventing Laptop Theft](#)

Josh Ryder

[Privacy Statement](#)

Copyright 2006, SecurityFocus