Technology Paper

Can Your Computer Keep a Secret?

Why All Laptop Data Protection Methods Are NOT Created Equal

Hard Drive Passwords Easily Defeated

It can be surprisingly easy to pull sensitive data, such as thousands of names and social security numbers, off laptops that are thought to be encrypted and secure. Recent data leakages (TSA, TJ Maxx) prove embarrassing and costly, and illustrate the necessity for robust security solutions. IT security research and advisory leader Trusted Strategies[1] put the most prevalent hard drive data protection solutions to the test—and show how easy it is to crack frequently used technologies and get to valuable secrets.

The Truth About Data Protection

Companies may rely on password protection to safeguard data stored on their computer's hard drives, but in nearly all cases an attacker can easily disable the password lock and gain full access to the data on the drive.

Theft of sensitive information from personal and enterprise computing systems is one of the fastest growing crimes in America.[2] Ameriprise Financial, Ford Motor Company, the Department of Veterans Affairs and many others have lost millions of sensitive records stolen from their laptop computers.[3] The costs in incident response handling, legal fees, corrective actions, loss of reputation and loss of customers can be crippling. Another daunting fact is that company management can be held personally liable for security breaches.

A significant and increasing percentage of corporate data now resides at the edges of the enterprise on home office PCs and the laptop computers of mobile workers. Wherever it resides, protecting sensitive data is critical to an organization's business practices and overall success. Consequently, individuals and organizations are struggling to find cost-effective and user-friendly ways to keep sensitive data from falling into the wrong hands.

[1] Trusted Strategies, LLC, www.trustedstrategies.com
[2] National Crime Prevention Council, www.ncpc.org
[3] Privacy Rights Clearinghouse, www.privacyrights.org

Can Your Computer Keep a Secret?

Why All Laptop Data Protection Methods Are NOT Created Equal

Comparison of Hard Drive Data Protection Methods

There are a number of methods available to protect data on a hard drive. *BIOS and operating system passwords* are frequently used, but they only provide very minimal security and can be readily removed by unskilled attackers without requiring sophisticated tools. *Hard drive password locking* is one of the most relied-upon security methods today. It is stronger than BIOS or operating system passwords, but this common protective measure can be easily defeated as well.

Software-based full drive encryption is significantly stronger than BIOS, operating system or hard drive password locking. Unfortunately, software-based encryption must run under the operating system and in the CPU, which can have an impact on the overall performance of the PC, as well as cause an exposure to the security methods used to safeguard the information on the PC itself. This means that there can be stealth processes running on the PC that can capture the encryption keys and even the non-encrypted data—which of course is not a very good scenario to have.

Hard drive-based security provides some of the best and strongest encryption solutions for personal computers. No sensitive data or keys are available to the CPU or to other applications running under the operating system. In addition to the security advantages, encryption done in the drive's hardware offers other attractive advantages. First, hard drive-based encryption has clear performance and reliability advantages. Second, because the encryption is integrated into the drive read/write function, it is transparent to the user. And finally, "factory" encryption significantly reduces the costs of acquisition, deployment and administration.

Comparison of Hard Drive Data Protection Methods

BIOS Password Very minimal protection	Available on nearly all PCs. Prevents the computer from fully booting unless the correct password is provided. Does not encrypt any data. Very easily thwarted, no special skills needed. For example, the hard drive can simply be moved to another device with the BIOS lock turned off.
Operating System Password Very minimal protection	Access to general OS functions is denied unless the correct password is given. Does not encrypt any data. Easily defeated by moving the hard drive to another computer. No special skills needed. Offers very minimal protection.
Hard Drive Password (using ATA) Minimal protection	Available on most notebooks and some desktops. Prevents the drive from retrieving data unless the correct password is provided. Does not encrypt any data. Easily defeated but requires specific skills or hiring someone with those skills. Stronger than BIOS or OS passwords but still weak protection and not suitable for data worth more than US$100.
Software-Based Full Drive Encryption Good protection	Add-on security product that modifies the hard drive drivers and encrypts all data as it is written to the drive. Requires correct password before the data is decrypted. Offers good protection but expensive to purchase and deploy, and impacts system performance which sometimes leads end users to turn it off. There is a potential for malware, trojans or rootkits to remotely turn off the software protection (the same as end users) without proper methods of protecting the software itself from attacks. Also worth noting, some software-based products require the encryption to be turned off whenever an operating system update must be installed—causing an administration burden and also risk of exposure.
Next-Generation Encrypting Hard Drives Excellent protection	The hard drive contains built-in cryptographic hardware that encrypts all data as it is written to the drive. Requires the correct password to decrypt any data. Built into the computer so it's not an add-on, and totally transparent to the user. Does not impact performance. Extremely difficult to defeat when good passwords are used. Offers excellent protection.

Hard Drive Password Locking

Most hard drive manufacturers offer a feature officially called the "ATA security feature set" but commonly known as "ATA hard drive password locking." As the name implies, this feature allows users to lock their drive with a password. Unlike BIOS or operating-system password protection, ATA password locking is implemented at the drive. Even if the operating system password and any BIOS-level password protection is satisfied (or removed), an ATA protected hard drive will not retrieve data unless the correct ATA password is presented to the drive. This password-locking feature is marketed under a variety of names by various manufacturers, including ATA password locking, DriveLock, HDD Password, HDP and Security Lock.

On the surface, hard drive password locking appears to provide great protection, and many individuals and organizations are using this method to safeguard sensitive data stored on their computer hard drives. Unfortunately, in nearly all cases an attacker can easily disable the password lock and gain full access to the data on the drive.

Michael Crooker learned the hard way that hard drive password locking is not secure. He purchased a personal Compaq computer in September of 2002 specifically because of its DriveLock ATA password-locking security feature. According to Crooker, the computer's manual claimed that if one were to lose both the master and user passwords, the hard drive is useless, and not even Compaq can access the data[4].

However, after being arrested for selling a rifle with a silencer, Crooker's computer was confiscated. Law enforcement agents who did not have the hard drive password quickly removed the security mechanism and had full access to Crooker's data. They found plenty of incriminating evidence. The case received considerable attention because Crooker sued both the retail establishment that sold him the computer and the computer manufacturer for false advertising.

Hardware Tools Easily Remove Hard Drive Passwords

The details of how the password security on Crooker's PC was disabled were not disclosed, but one need not search very far to find numerous methods to defeat this security mechanism. In Crooker's case, law enforcement agencies most likely used a hardware tool specifically designed to remove hard drive passwords.

One such tool, the HDD Rock from YEC, sells for a little over US$1000. The product documentation states: "Instantly removes unknown passwords from locked hard drives. Total process time under 2 minutes[5]. In addition to the HDD Rock, a number of vendors offer similar products, including Ultrec[6], Vogon[7], AFF Laboratory[8] and others.

YEC and the other companies listed in this article sell their password recovery tools to law enforcement agencies and data recovery firms that are in the business of assisting legitimate owners in recovering their own data. These companies validate drive ownership before they will unlock a drive. However, there are other firms that will sell unlocking tools or provide unlocking services to anyone, no questions asked.

Hard Drive Password Removal as a Service

There are many companies that have the equipment and skills to unlock a password-protected hard drive. Bob Weiss, CEO of Password Crackers said that for around US$100 his company can easily recover 90 percent of password-locked drives, and US$1000 will remove the password security from *any* drive. Datatrack LABS, located in the United Kingdom will also remove hard drive password protection for a service, as will a number of other firms. Datatrack LABS also claim the ability to unlock any drive whatsoever.

[4] Information Security News, May 1, 2006, *Your Computer Is Not Secure*
[5] HDD Rock Password Removal Tool www.yec-usa.com/products/hddrock.htm
[6] Ultrec LTD www.ultratec.co.uk./services/harddisk_password_removal.asp
[7] Vogon Password Cracking POD www.vogon-forensic-hardware.com
[8] AFF Laboratory's *Repair Station* www.hdd-tools.com/products/rrs/drives

Can Your Computer Keep a Secret?

Why All Laptop Data Protection Methods Are NOT Created Equal

How Hard Drive Password Security Is Defeated

Although hard disk password drive locking conforms to an industry standard, different drive manufacturers implement the security feature in slightly different ways. Authors of password removal tools use a variety of methods to determine how to remove the hard-drive ATA password from the various drives. Once the technique has been mastered for a particular drive model, the same method can be applied to all drives of the same model. Over time the tools have become smart enough to quickly and easily remove the password lock from nearly all models of hard drives.

Encryption Is the Only Secure Protection

The problem with relying on hard-drive ATA password security is that the data itself remains unprotected. Because password locking does not encrypt any data, once the lock is defeated the data can be read and stolen.

The solution is to encrypt the data. If the data on the hard drive is encrypted, it remains protected even if the password lock on the drive is defeated. A drive with its password lock beaten will retrieve data, but that data is useless if it is securely encrypted.

Fortunately good, transparent encryption solutions are becoming available. Gone are the days when one had to be a techno-geek to install, configure and manage encryption. Software-based full disk encryption products have been available for several years from companies like GuardianEdge[9], SafeBoot[10] and Pointsec[11] (recently acquired by Checkpoint). Although these are aftermarket solutions that must be installed on existing systems and require a significant effort to deploy at large organizations, their use is much better than relying on hard drive password locking.

However, the best news by far is that full disk encryption is starting to be built right into drives. Seagate® is the leader in this area with its newly released Momentus® 5400 FDE.2 drive. Seagate is also heading up a standards-based initiative in conjunction with the Trusted Computing Group (TCG), which will, if successful, make encryption performed within hard drives ubiquitous. The initiative, run by the TCG Storage Workgroup, has wide industry participation, so the prospects are promising.

Full disk encryption performed within the hard drive itself provides the best solution for protecting data stored on the hard drive.

Conclusions

The risks to organizations of losing confidential data stored on hard drives in PCs and servers cannot be ignored. Utilizing password security to protect data on hard drives is better than relying on BIOS or operating system passwords, but it is not strong enough for most organizations. Hard drive password security can be easily defeated by an attacker, either through a service or by obtaining password-cracking tools from any number of sources. Because hard drive password systems do not encrypt the actual data, a broken password routine allows full access to the data on the drive. This means that hard-drive ATA password security alone is not secure enough for protecting anything but casual data.

For most organizations, obtaining adequate protection of sensitive data on their hard drives requires encrypting that data. Software-based full drive encryption systems are one solution, but the next generation of encrypting hard drives have important advantages over the software-only solutions and will certainly be of value to any organization with high-value or regulated information.

[9] GuardianEdge Technologies Inc. www.guardianedge.com
[10] SafeBoot International, www.safeboot.com
[11] Pointsec Mobile Technologies, www.pointsec.com

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 130–136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00