

Is your data at risk?: Why physical security is insufficient for laptop computers

Evaluating the various data security options to protect your PCs can be challenging. This paper examines the options, discusses why passwords alone are not sufficient and makes the case for strong data encryption.

Is your data at risk?: Why physical security is insufficient for laptop computers

New frontiers in computer security

The meaning of computer security continues to evolve. Physical security used to be the main concern. Through the 1980s, expensive mainframe computers were locked in special climate-controlled rooms within secure buildings. Security costs, when they were considered at all, constituted a very small percentage of the overall system costs. Today, such systems are called “server systems”; and although they are important in their own right, they make up a small percentage of all computer shipments each year. According to market researcher Gartner, 2.3 million server systems shipped worldwide in the third quarter of 2008, compared to 80.6 million PCs that shipped in the same period.

The widespread use of PCs creates much greater vulnerability compared to yesterday’s mainframe computers. Although desktop PCs are arguably less secure than centralized servers, such systems probably have physical security identical to that of a company’s other on-premises assets. The least secure computers are those that are mobile. According to the Gartner estimate for 2008, worldwide mobile PC growth is 25% versus 1.2% for desktops. According to its forecast, 293 million PCs would be shipped in 2008.

Whether you prefer the term “mobile PC,” “laptop” or “notebook,” the vulnerable systems are those taken off-premises. In spite of employee diligence, mobile PCs do get lost and stolen. Not convinced? Take a look at www.privacyrights.org, a website listing breaches in data security that involve personally identifiable information (PII). More than half of the states in the United States require disclosure of such breaches. Don’t let your company’s name get added to this list; good solutions are available.

Attacks on laptop data security

To a casual observer, a laptop computer seems secure. To use a computer system, users must type credentials into a window. If users do not provide the correct username and password, they cannot access the system. Like someone who misplaces the keys to a car, someone who forgets a computer password is locked out. Without the proper credentials, access is blocked. Or is it?

Passwords alone do not protect data

The login process prevents unauthorized users from running software. But a password does not, by itself, make the data on hard drives secure. A user without a correct username and password cannot use the services of the operating system as installed and configured on that particular hard drive. However, a tech-savvy person without the appropriate credentials can still attack a computer. There are three possible attack strategies:

- Alternative boot device
- Alternative boot device + alternative boot program
- Moving a hard drive to an alternative computer system

Attack #1: Alternative boot device

One type of attack involves using an alternative boot device instead of the hard drive. Every computer system supports this option. Over many years and many versions, the Microsoft Windows setup disks have been distributed on bootable CD-ROM or DVD discs. A simple way to access a system’s data is to boot to a Windows setup disk and install a new copy of the operating system. This approach makes available any data that resides on a hard drive.

Attack #2: Alternative boot device + alternative boot program

A second attack combines the first attack with special boot programs. For example, many IT professionals use bootable CD-ROMs with software like BartPE (Bart's Preinstalled Environment) as an aid in fixing systems with boot problems. Aside from legitimate uses, unauthorized persons can use this type of tool to mount an attack. In addition to accessing normal user data files, such tools allow access to operating system files that are not available when the operating system is running. Of particular interest is the Security Accounts Manager (SAM) database, an encrypted file with password hashes. Although this is an encrypted file, techniques are widely available to decrypt the SAM and read password hashes. While different from plain-text passwords, a password hash is the result produced when a password is run through a security algorithm. By replacing a password hash for an existing account—maybe one with administrator privileges—a data thief can boot and run the original operating system and any installed software.

Guarding Against Attacks #1 and #2

Support for alternative boot devices enables operating system installation. After the OS has been installed, the use of alternative boot devices can be disabled in the basic input/output system (BIOS). In the same way that you can lock the front door of your house, you can lock out alternative boot devices with the proper BIOS settings. To keep those settings in place, you also need to enable password protection on the BIOS itself. A third step, locking the computer's case, prevents a reset of the BIOS and failure of the above measures.

Attack #3: Moving a hard drive to an alternative computer system

An individual with physical access to a laptop computer can remove the laptop's hard drive using a screwdriver. Once removed from the original system, the laptop's hard drive can be attached to another computer—one on which the individual has valid login credentials. When installed on another computer, the laptop hard drive is not the bootable system drive. Instead, the laptop hard drive appears as a secondary data drive (drive D,

E, etc.). When attached to another system like this, the laptop's data is just as readily accessible as if an authorized user had logged on to the original laptop. At this point, all data is readable; only encrypted data is hidden from view.

What can an intruder use to enable this type of unauthorized access? There are several choices, but the simplest is a hard disk enclosure kit. These kits are available from computer retailers. Hard disk enclosures have a very reasonable and legitimate purpose: to create a portable storage device. A hard disk enclosure allows any hard drive to be portable between computer systems. Such enclosures support both USB connections and 1394 (i.e., FireWire) connections. The cost is nominal—typically less than US\$20 (€15).

Therefore, this legitimate product can have illegitimate uses. A hard disk enclosure enables unauthorized users to read the data on a hard drive taken from a lost or stolen laptop computer. By using this tool, anyone who has physical access to a hard drive can gain full access to the data on that drive. Hard disk enclosure kits also include a screwdriver, which is often the only tool needed to remove a hard drive from a laptop computer.

Securing data requires encryption

True data security requires making data unreadable to persons who are not authorized to access the data. And because file system permissions can be overridden using schemes like the ones described earlier, data encryption is the only truly secure way to hide sensitive data. To unauthorized users, encrypted data is meaningless. Only authorized users with valid credentials can access the encryption keys needed to decrypt and use data.

This section reviews encryption support in Microsoft Windows, and the encryption support in three popular data encryption products from Sophos.

A look inside encrypted files

To understand the protection that data encryption provides, you must understand the difference between data in an unencrypted state and an encrypted state. In both states, the data appears in two forms: (1) numeric values and (2) character

data. Software engineers commonly use both types of displays when they need to understand the exact location of each bit and byte of data.

In an unencrypted “plain-text” display, the text data is clearly readable. Interestingly, even the most sophisticated word processing programs typically store text data in a very readable form. Of course, this helps software engineers when writing the sophisticated programs. From a security standpoint, this practice also makes it easy for anyone—friend or foe—to read data on a hard drive.

It’s a different situation when the same file is saved on a hard drive that is fully encrypted. By comparing an encrypted display with an unencrypted display, it becomes obvious that the two are different. The encrypted data contains nothing that seems even vaguely understandable. And that is the essence of encryption—to make some piece of data unintelligible and unusable to all except those who are authorized to use the data.

Data encryption in Microsoft Windows

Microsoft Windows supports some data encryption. Starting with Windows 2000, Microsoft made available support for the Encrypting File System (EFS), a built-in mechanism for encrypting specific files or entire folders that reside on NTFS partitions. Note that FAT partitions are not supported, which means that files stored on USB memory sticks cannot be encrypted.

Encrypting File System (EFS)

When an individual file is encrypted using EFS, modifications made to that file may result in the creation of unencrypted, or “plain-text,” copies. When a user opens an encrypted file using Microsoft Word, the file is decrypted by the operating system and copied to a temporary location. The plain-text file is used during the editing process, and the contents get encrypted again only when the file is closed. This process can leave unencrypted remnants on disk, opening the possibility that sensitive information may be revealed.

BitLocker full-drive encryption

A more secure alternative to EFS is full-drive encryption. Full-drive encryption protects against both types of attacks described in this paper.

When alternative boot media is used, the contents of the encrypted drive are gibberish. When an encrypted hard drive is connected as a secondary drive (see Attack #3), the contents are still not readable.

A central benefit of full-drive encryption is that the choice of what data to encrypt and what to leave unprotected is taken away from the user. All data on encrypted partitions is encrypted without exception. Microsoft’s full-drive encryption solution is BitLocker. Sophos’s full-drive encryption solutions are SafeGuard Easy and its successor SafeGuard Enterprise. Let’s consider BitLocker.

On Windows Vista, BitLocker can encrypt one disk partition: the one with the operating system (typically the C drive). Compared to EFS, BitLocker provides a more secure way to protect data. On a BitLocker-enabled system, data on the boot partition is unavailable unless a valid password is entered during system boot.

» Note: BitLocker hard drive encryption is supported in two versions of Windows Vista: Windows Vista Enterprise and Windows Vista Ultimate.

As we have described, Microsoft has built in some support for data encryption, starting with Windows 2000. When you need more than what comes with the operating system, we invite you to look at Sophos’s line of data encryption products.

Sophos data encryption products

To help you select the Sophos product that is right for you, we turn our attention to three of our products: SafeGuard Easy, SafeGuard PDA and SafeGuard PrivateDisk.

Sophos SafeGuard Easy/SafeGuard Enterprise

Both BitLocker and SafeGuard Easy/SafeGuard Enterprise provide pre-boot authentication to protect the integrity of the boot partition and the operating system. In addition, SafeGuard performs encryption of all local data drives and is not limited to the partition with the operating system; it applies to all partitions on all hard drives. It also encrypts removable drives including diskettes, zip and jaz disks, as well as USB memory sticks.

SafeGuard Easy can be deployed on versions of Microsoft Windows older than Windows Vista. And so, unlike BitLocker, which requires specific versions of Windows Vista, SafeGuard Easy is supported on the entire family of operating systems from Microsoft, including Windows NT 4.0, Windows 2000, Windows Server 2000, Windows XP and Windows Server 2003.

SafeGuard Enterprise, the successor of SafeGuard Easy, supports Windows XP and also Windows Vista (starting with version 5.20). Besides offering many other enhancements, it adds a central Active-Directory enabled server as well as the ability to manage BitLocker clients in parallel to SafeGuard encrypted clients in a mixed environment if the customer desires to do so.

Sophos SafeGuard PrivateDisk

If you have been using EFS but want just a few extra features, SafeGuard PrivateDisk might have what you are looking for. Both EFS and SafeGuard PrivateDisk allow your data to be secured under digital lock and key. Both require active involvement by a user to identify the specific files to be encrypted. Note that this is unlike whole drive encryption schemes, on which all files are transparently encrypted and decrypted.

Where a user would define a specific system folder for EFS encryption, SafeGuard PrivateDisk generates encrypted “virtual” disk drives. To

authorized users, these disk drives appear with a regular system drive letter (D, E, etc.). To the outside world, a SafeGuard PrivateDisk volume appears as a single file.

Unlike EFS, which is limited to NTFS partitions, PrivateDisk volume files can be copied to a USB memory stick, CD-ROM drives, DVD drives or diskettes. In addition, unlike EFS, PrivateDisk supports Windows NT 4.0.

Conclusion

Is your data at risk? Unless your data is encrypted, the answer is yes. Although you must secure all computer systems, those that leave a company’s physical security perimeter are the most vulnerable. Such computers include laptops used by sales professionals, or those that executives take on visits to remote company sites. Without encryption, your company’s data is at risk. Don’t become the next lost laptop headline.

Boston, USA | Oxford, UK
© Copyright 2009. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any
form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM