



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Securing Information on Laptop Computers

Jim Purcell

December 27, 2000

Introduction

Recent incidents detailed in news accounts have underscored once again the need for special security measures for laptop computers used by executives and others that travel. Irwin Jacobs, the CEO of Qualcomm, had his laptop stolen after speaking at a conference just moments after he stepped away from the podium¹. A laptop belonging to a British (MI5) intelligence agent containing classified material was stolen from the agent in a train station as he stopped to help another passenger². A laptop computer missing from the U.S. State Department containing thousands of classified documents was stolen from a conference room³.

Various estimates of the number of laptop computers stolen each year range from 1 out of 14 to 1 out of 50⁴. The insurance industry reports 319,000 laptops reported lost or stolen in 1999⁵. Clearly the information stored on laptop computers is at risk and special security measures are needed to protect that information.

Much has already been written on how to prevent laptop theft. The SANS reading room contains many good articles (see Basic Travel Security by Aaron Weissenfluh http://www.sans.org/infosecFAQ/travel_sec.htm).

This paper does not address preventing laptop theft, but how to prevent the information on the laptop from falling into the wrong hands when the laptop is lost or stolen. We will look at the value of BIOS/BOOT passwords, hard drive passwords, and data encryption as means to protect the information on a laptop.

BIOS/BOOT Passwords

Almost all laptop computers allow the user to specify a BIOS (or sometimes called a BOOT) password. The Basic Input/Output System (BIOS) is the software that controls the hardware settings for the laptop and allows the laptop to load the operating system. When the laptop is protected by a BIOS password, a thief is prevented from accessing the data on the laptop because the operating system will not load without a correct password. The thief is prevented from booting from floppy or CD as well as the laptop hard disk. The BIOS password provides a basic level of protection, but as we shall see, it has several problems.

Newer laptop systems have more secure BIOS password system than older laptop and desktop systems. But since the user can still forget the password or leave the company, BIOS passwords schemes are made to be compromised in several ways. There are many sources on the Internet that detail how to disable,

crack, or otherwise overcome BIOS passwords. "How to Bypass BIOS Passwords" by Elf Qrin (www.ElfQrin.com/docs/biospw.html) is a good source that is updated regularly. Some methods used to compromise BIOS passwords and get to the data on the hard drive are to remove the hard drive and install it in another computer, use BIOS backdoor passwords or password crackers, or flash the BIOS.

Copy the hard disk

The easiest way for a thief to access the data contained on a laptop with a BIOS password is to remove the laptop hard disk and install it in another computer. Most laptop drives are EIDE drives that can be slaved to another system by setting the appropriate disk jumpers and plugging it into the system disk controller. Then the data can be copied or otherwise accessed. This stolen drive could even be returned to the laptop and the laptop returned to the user without the user knowing that the data was copied.

Guess/Crack password

Just a few companies provide the BIOS systems for all laptop makers. The most prevalent BIOS's are from IBM, Award, AMI, and Phoenix. Each of the BIOS's have factory-set default backdoor passwords. These passwords are posted many places on the web. One of the backdoor passwords for the Award BIOS is simply AWARD_PW. A backdoor password for the AMI BIOS is AMI. The backdoor BIOS passwords for most laptops are well known in the black hat community. In addition, there are several public domain BIOS password-cracking tools available over the Web. The following site contains some tools to crack BIOS passwords and a list of known backdoor passwords - <http://www.crosswinds.net/~passw0rld/bios.htm>.

Flash BIOS

The laptop computer BIOS information is stored in Complementary Metal-Oxide Semiconductor (CMOS) RAM. This memory can be overwritten through a process call flashing. Since the BIOS password is contained in CMOS RAM, flashing (or overwriting) this memory will erase the password. Several hardware and software methods can be used to flash the laptop CMOS RAM.

If the computer is turned on when it is stolen and the BIOS password has already been entered, a software program or technique can be used to change or disable the password. Depending on the BIOS manufacturer of the BIOS, a simple MS-DOS debug script will disable the BIOS password. The following is the code that works for both the AMI and Award BIOS.

```
O 70 17  
O 71 17  
Q
```

A program is available that will accomplish the same. KILLCMOS (7K) is a

utility to wipe the password away and can be obtained at the web site - <http://www.crosswinds.net/~passw0rld/bios.htm>.

In most cases the computer will not be powered on when it is stolen. Several ways are available to flash the BIOS using hardware methods. Some laptop motherboards have jumpers that can be set to enable or disable the BIOS password. The CMOS RAM chip containing the BIOS is powered by a small battery. The password can be erased by temporarily disconnecting the battery. And finally, some BIOS chips can be short-circuited by using a paper clip or small piece of wire to cross the right two pins on the chip. Techniques and diagrams to accomplish these tasks are available on the Internet.

Hard Disk Passwords

Hard disk passwords are similar to BIOS passwords. After setting the hard disk password in the laptop BIOS settings, the user must enter the password during the boot process before that disk can be accessed. The advantage the hard disk password has over the BIOS password is that since the password is stored in the hard drive electronics, even if the hard disk is removed from the laptop, the data is still protected. There is much less information available on the Internet concerning ways to crack hard disk passwords. Data recovery companies will attempt to recover data from a password-protected disk, but most techniques known in the black hat community cause loss of the data. Hard disk passwords do offer increased security over BIOS passwords alone, but if they are forgotten or lost or the employee leaves the company, it is very difficult to recover the data.

Disk Encryption

Since BIOS passwords provide very weak protection for information stored on a laptop and hard disk passwords can be overcome (albeit with much more difficulty) and are hard to manage, we must look for another way to protect the data. Disk encryption provides a stronger method to protect the information and allows for better management and recovery of the information on the laptop.

Disk encryption involves protecting the information on the hard drive by writing it to the disk "coded" using an encryption key or pass phrase. The information can only be "decoded" by a person knowing the key or pass phrase. Several public domain and commercial products are available that allow the user to encrypt the information on the disk. A good list of available programs for Windows, Macintosh, and UNIX/LINUX can be seen at www.stack.nl/~galactus/remailers/index-diskcrypt.html.

A good disk encryption system for use in a corporate environment has the following features.

Strong encryption algorithm

A good disk encryption system uses a strong, modern encryption algorithm.

The SANS Information Security Reading Room has some good information about the different encryption algorithms in use today - (http://www.sans.org/infosecFAQ/encryption/encryption_list.htm). Some of the algorithms used by disk encryption software include RSA, Triple DES, Blowfish, IDEA, and MDC/SHA. All of these algorithms have a common characteristic. They are all very difficult to break providing a strong encryption key is used. It would take a thief months or even years to decode information protected by one of these encryption algorithms.

Key/Pass Phrase Management

In order to prevent information from being lost when a user forgets their password or leaves the company, a key/pass phrase management system must be in place. This system will provide a “master” key known to the company so data encrypted on the disk can be recovered if the user forgets the password to access the disk. The management system also allows for the easy installation and maintenance of the disk encryption software.

Whole Disk Encryption

Products are available that allow the user to encrypt individual files and folders. These products have value, but since most operating systems temporarily store copies of the information in page files and other places on the disk, it is important that all the information on the disk be encrypted. This also allows the encryption to take place transparently to the user. If the whole disk is encrypted, then the user does not have to remember to encrypt an individual file or move the file to an encrypted folder.

Conclusion

Laptop theft is a real and growing problem. Laptop users must be able to protect the information on the laptop in case the laptop is lost or stolen. BIOS/BOOT passwords only provide very limited protection. They are considered trivial to break by the black hat community. Hard drive passwords provide much stronger protection, but they can be bypassed or broken by a knowledgeable attacker, and if the password is forgotten, the information on the laptop is very hard to recover by the legitimate user. Disk encryption implemented with a good key management system provides the highest level of safety provided the user chooses a strong encryption key or pass phrase. The maximum level of protection would be to use a hard disk password and disk encryption and always backup the information before traveling.

References

1. “Police Investigate Qualcomm CEO Laptop Theft.” September 20, 2000. URL: http://www.planetit.com/techcenters/docs/mobile_wireless-wireless_nets_and_devices/news/PIT20000919S0012. (December 27, 2000).
2. Leydon, John. “Cookies cause concern in MI5 laptop theft.” March 24,

2000. URL: <http://www.vnUNET.com/News/601247>. (December 27, 2000).
3. Mufson, Steven. "Missing State Department laptop contained arms secrets." The Washington Post. April 22, 2000. URL: http://seattletimes.nwsOURCE.com/news/nation-world/html98/data22_20000422.html. (December 27, 2000).
 4. "Laptop Theft." Australian Projects Pty Limited. URL: http://www.austprojects.com.au/news/1998sep_a.htm. (December 27, 2000).
 5. Vincent, Christie and Jack Vaughan. "Security experts seek to combat laptop theft." IDG. September 20, 2000. URL: <http://207.25.71.25/2000/TECH/computing/09/20/laptop.security.idg/>. (December 27, 2000).

© SANS Institute 2000 - 2005, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event