Laptop Security, a guide to protecting your laptop.

Security Essentials GSEC Practical Assignment
Version 1.4b, Option 1

Shane Meyer
February 12, 2003

Abstract

Laptop computers are commonplace devices in today's businesses; their mobility and performance make them a logical replacement for the standard desktop computer. This mobility is also the root of many security challenges that today's information security professionals have to address. This paper will focus on these challenges and look at various solutions to address them.

Introduction

The popularity of laptop computers is growing and recent figures show that they make up nearly 25% of total computer sales[1]. The ability to work at the office, at home, while traveling, or while on vacation appeals to many people although they may not be fully aware of the security risks that they face.

Once a computer leaves the office it has lost all the defenses that are in place, from the security guard in the lobby to the administrative assistant outside your office. Physical security is just one form of protection inside the office the other is information security. Many businesses have adopted a defense in depth strategy and use firewalls, routers, anti-virus software, IDS systems, and backup strategies to protect the companies IT assets. The moment the laptop leaves the office you have lost the layer of protection that these technologies provide.

The security challenges can be broken into four categories and we will look at each of the following.

- Physical Security
- Data Security
- Recovery
- User Education

Physical Security.

The greatest threat when out of the office is the theft or loss of the laptop, this is not to say that the laptop would be 100% secure sitting on your desk but its usually safer there than elsewhere. In 2001 Safeware the Insurance Agency reported 591,000 laptops were stolen[2], this is a 53% increase over the year 2000. These figures are disturbing once you consider that they are from only one insurance company, worldwide the total numbers must be much higher.

It seems that every other day you hear on the news that another laptop has been lost or stolen, in recent years we have heard about losses by the British Ministry of Defence[3], the U.S. State Department[4], Qualcomm's CEO Irwin Jacobs[5], PRADA, the Italian team competing in the America's Cup[6], and several agencies under the U.S. Department of Justice including the Federal Bureau of Investigation[7]. This too is disturbing as many of these reported thefts involved laptops that contained very sensitive information.

To minimize the risk of theft a person needs to be aware of where your laptop is at all times, you need to "treat it like a wallet or a purse" according to the Defense Security Service Academy[8]. A person seldom lets their purse or wallet out of their site and should treat their laptop in the same way. If the laptop owner maintains a heightened state of awareness, this alone will help to reduce the risk of loss or theft.

When traveling you should not carry your laptop in a typical laptop carrying case, these cases can draw the attention of potential thieves. The more expensive the carrying case is usually is an indication as to the value of the laptop inside. Carry the laptop in something that makes it less obvious as to what the contents are, a briefcase or a backpack are good choices.

If traveling by car always put the laptop out of site when your away from the vehicle, put it in the trunk where it will be secure or cover it with a jacket or other objects if your vehicle does not have a trunk. If traveling by air or train never include your laptop with you're checked baggage it could be lost, damaged or stolen while it's out of your site, always include it with your carry on bag. If you need to set your laptop carrier down always keep it between your feet so that you're aware of its location. If your unable to keep the laptop bag with you then a laptop bag alarm may be a good choice. Kensington makes the SonicLock™, a motion detecting alarm that will go off with the slightest motion and which is easily enabled or disabled by a user selectable three digit keypad. Similar alarms are available from Targus and others.

Another method to secure your laptop or its carrying case would be a cable lock. There are cable locks that attach to the universal lock slot that is found on most modern laptops, you can then loop the cable around a secure item such as a desk, chair, or some other difficult to move item. A cable lock can also be used to attach your laptop carrying case to a secure point; some cable locks also contain motion-detecting alarms to offer you more protection. Cable locks are offered by many different companies, some examples are Targus, Kensington, Belkin, or PC Guardian.

Theft of laptops at airport security checkpoints has been a concern for years. There have been scenarios where you put your laptop on the X-ray machine conveyer belt and go to step through the metal detector. The person in front of you deliberately delays you by setting off the metal detector and in the confusion his partner has taken your laptop off the conveyer before or some times after it has been X-rayed. With the increased delays at security stations you need to pay extra attention to your laptop to ensure its not taken by thieves or perhaps taken by another passenger as an honest mistake who believed it was their laptop[9]. To prevent confusion after passing through the security station when retrieving your laptop it's a good practice to have your laptop labeled. Something as simple as your business card attached to the bottom can ease the identification of the unit but you may wish to go as far as to have a large non removable label or sticker put on the top of the laptop which will easily distinguish it from others.

Once you're at your destination be it a hotel room, conference room, client site or even at home you should not let down your guard. Install your cable lock or alarm if you're going to leave your laptop unattended for any length of time. When you leave your hotel room or the conference room and your laptop is going to remain behind you should at the least lock it in another bag or case so it's out of site of prying eyes. You may even wish to take your laptop and have it locked in the hotel safe if you wish to have that extra level of security. Some hotel rooms now have small safes and you could secure your laptop in that while you're away from your room, this is something you could inquire about while planning your trip and booking your room.

Data Security

According to the 2002 Computer Crime and Security Survey completed by the Computer Security Institute and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad the average financial loss of a laptop is $89,000[10]. This number is based on the information provided by the 503 companies that replied to the survey. The value of the hardware is a small percentage of the actual cost once the value of the information stored on the laptop is taken into consideration.

The information that you store on your laptop can used for many things including industrial espionage, identity theft, or breaking into your secure network back at the office to name just a few. Ensuring the security of your data may be nearly impossible but you can do many things to minimize the risks.

The first thing to consider is how secure is the operating system on your laptop. Windows 2000 Professional and Windows XP Professional have many security enhancements that would make them better choices over Windows 98 or Windows ME. Windows 2000 and Windows XP also work better in a corporate computer environment where the backbone services usually are Microsoft server centric.

One of the first steps to a secure operating system is to update it and patch it. Microsoft offers its Windows Update Server as a method to apply critical security patches to its operating systems and applications. Updates for the operating system and installed applications are crucial to maintaining a secure system so you should be in the habit of checking for updates often or configuring your system for automatic updates if the application allows for it.

Next your operating system should be running a secure file system such as Microsoft's NTFS. NTFS offers a more control over permissions and access than FAT32 and works in concert with the Windows ACL to prevent unauthorized access to files and folders. If your currently not running a NTFS partition you may wish to consider converting to NTFS using convert.exe program located in the system32 folder of your operating system. Another benefit to having NTFS in place is that you can then enable Microsoft's Encrypted File System (EFS). Enabling EFS allows you to encrypt individual files or folders to prevent them from being accessed buy unauthorized people. The decryption keys for files are also encrypted and stored within the file system for ease of use and administration. If a person gains access to an encrypted file they will not be able to read its contents without access to the proper keys, which are controlled by the operating system.

The first layer of defense on your laptop is the logon screen, here is where a user enters their account name and password to access the operating system. You should minimize the number of accounts that have the ability to logon to the laptop and disable or delete any accounts that may exist that you do not want to have access. Strong passwords should be used for all accounts to prevent unauthorized access by someone who guessed that your password is your pet's name. Strong passwords should be a minimum of 8 characters in length, be a combination of upper and lower case characters as well as alpha, numeric and special characters. The local administrator account should have a strong password assigned to it, renamed, and then never be used except in an emergency. A new administrator account should be created that is a member of the local administrator group and this account should be used for any administrative activities. Your personal account that you use for day-to-day activities should not belong to the local administrator group in order to provide a extra layer of security.

Your laptop should use local and group policies to control unsuccessful logon attempts, prevent the unauthorized installation of software, and to be consistent with your corporate model that would be used on standard desktop PC's. Your companies network administrator will be well versed in these policies and should be able to explain which ones are in place.

You should minimize the amount of data that is stored on your laptop by taking advantage of your network infrastructure in the office and store your data on network drives instead of your local hard drive. Your data will be more secure there and the network backups that are done will also help to protect it. You should also try to avoid storing any personal data on the laptop, as it could aid someone in stealing your identity if they have already stolen your laptop. An often-overlooked form of data that is stored on the laptop is your Internet browser cache and the operating systems swap files. You should change your browser's settings to use a small cache, and use a program like tweakui from Microsoft to purge the cache on shutdown.

Another method to protect the operating system and data on your laptop is to enable the BIOS password and secure it with strong password that is unique from the others that you use. If a user fails to enter the correct BIOS password the computer will not even boot into the operating system, this just provides another layer of defense in your defense in depth strategy to protect your laptop. While setting up a BIOS password on your laptop you may wish to modify the order for boot devices so that it cannot be booted from the floppy drive. Another option it to not even have a floppy drive in your laptop computer. The reason you might not want a drive in the computer or not be able to boot from it is that one can run a password cracking utility like L0pht Heavy Industries LC4 which can be used to crack the passwords out of the local Security Accounts Manager (SAM) database found on the laptop.

If you must take sensitive information with you while you're out of the office there are a number of options you can use to minimize the risk. Consider burning the data to a CD or storing it on a USB Ram Drive. By keeping these separate from the laptop and on your person your data can be relatively secure. If you must store the data on the laptop itself you may want to consider a laptop that has a removable hard drive. Once you remove the hard drive and carry it separately or even on your person you have made the laptop useless to a person if it stolen and more importantly you have protected your data. Systems that allow removable hard drives tend to allow you to assign a BIOS password to the drive itself, so if you do loose the drive it still cannot be accessed without the proper password.

You should consider running a number of applications on your laptop to protect it when away from the office as well as when it is inside the office. These applications will help to protect your laptop as well as your corporate network when your laptop has been reconnected to it.

Antivirus software should be installed and always running on your laptop computer. It will greatly reduce your risk of having a virus infect your system while being connected to the Internet or while accessing your email. Your Antivirus software is similar to your operating system in that in needs regular updates and patches, these updates will ensure that you're protected from the latest viruses that have been released. Most Antivirus software products now offer an automatic update feature which I recommend you use whenever possible. There may be times that you don't have access to the Internet to get these updates, which is when you may have to take extra steps to have the pattern files downloaded on another PC and then put onto a CD, diskette or USB Flash drive so that you can update your laptop.

Personal security software is another tool that you may wish to install on your laptop. This software can function as a firewall as well as a simple IDS system to prevent unauthorized access to your laptop when it's connected to the Internet. Some personal security software such as Zonealarm from Zone Labs act as a application filter in that it monitors which applications have permission to access the internet connection. This feature can be valuable in determining what applications are accessing the Internet and why they may need to do so. Besides Zonealarm other products such as BlackIce from Internet Security Systems and Norton Internet Security 2003 offer similar features. PC Magazine recently did a review of 8 personal firewalls with Norton Internet Security 2003 getting their editors choice[11].

Another software product you may wish to consider running on your laptop is an anti trackware product for removing spyware. Lavasoft the makers of Ad Aware defines spyware as “something that can track your surfing habits, abuse your Internet connection by sending this data to a third party, profile your shopping preferences, hijack your browser start page or pages, and alter important system files.” Spyware is usually installed without your knowledge or permission while another application or utility is being installed, common examples of applications that do this include Kazaa and other personal file sharing programs. Products such as Lavasoft’s Ad Aware, PepiMK Software’s Spybot search & destroy or Pest Patrol Inc.’s Pest Patrol can search and remove spyware that may be located on your laptop, and If your laptop is used at home by other family members this is something that you should consider installing and running on a regular basis.

Another option to protect the data on your laptop as well as the laptop itself would be the Caveo Anti-Theft system from Caveo Technology[12]. Their anti-theft system consists of software and a card that would be installed in a PC card slot in your laptop. This card has a motion sensor, a speaker to issue warning signals or an alarm and a rechargeable battery that allows the card to work while the laptop is on or off. The system can be armed or disarmed from within the operating system or with a unique motion password that you configure. The system can also be configured to auto-arm at various points including startup, screensaver activation or suspend/hibernate. If the system’s alarm is triggered it has various levels of warnings that it can issue before the system will assume theft and will invoke strong responses to prevent access to the operating system and it will secure all passwords and encryption keys. Once this has happened the only way to regain access to the system is to enter a 16 digit master code, without it you cannot access the system even if the PC Card is removed or not.

Recovery

If the circumstances arise that your laptop is ever lost or stolen there are some measures that you can take to assist in its recovery.

Hopefully your laptop was labeled so that it could be returned if found or recovered by the police[9]. A business card glued to the bottom was suggested before but they can easily be removed. You may also wish to engrave contact information on the bottom with a permanent engraver, similar to what many police departments recommend you do with your valuables at home. You may also wish to put a label with contact information inside the laptop where its not visible, perhaps under the panel you remove to add memory or inside the battery or removable drive bays. Some laptops allow you to add inventory information into the BIOS, this field may be a good place to store your name and phone number to aid in having it returned to you.

The first step you should take when getting a new laptop is to record the serial # and other details in a safe place both for insurance purposes and to aid in its recovery. Also take a few moments to register the laptop with the manufacturer, if its ever stolen and the thief puts in a technical support call the manufacturers support group can get valuable information that may assist in its recovery. In the event of loss of theft you should contact the police and the manufacturer to report the missing laptop and to help increase the likelihood of it being returned.

A product like Computrace Plus from Absolute Software may be something to consider. Computrace Plus is a low level disk based utility that is that is undetectable by disk and memory scanning utilities and Antivirus software. The program can survive the formatting of the drive and reinstallation of a new operating system, which is what often happens with a stolen laptop. The program contacts the monitoring center once a day via IP or once every four days via dialup connection to verify that its not been reported stolen. If the monitoring center has a report of a stolen laptop they can monitor its communications and initiate a recovery process with local law enforcement officials. An option they also offer is a data delete service, if the customer requests that the data be deleted it can be initiated the next time the laptop contacts the monitoring center. The data deletion is done in a stealthy fashion so its undetectable to the thief using it, also the option exists to wipe the operating system from the drive in addition to the data. Other companies that offer similar solutions are Z-Trace Technologies, Stealth Signal Inc, and Computer Sentry Software.

User Education

Perhaps the first step in preventing the loss or theft of a laptop computer is by providing the user with the proper education to help increase his or her level of awareness. By ensuring the user is familiar with some of the basic steps outline here you can hopefully reduce the risk of loss or theft.

Another method to increase a users level of awareness is to have security policies in place in your company. A well-written security policy that the user has agreed with can outline his or her level of responsibility in the event of the loss or theft of their laptop. A company should maintain a copy of the security policy where it is easily accessible by the employees, perhaps on an in house web server. Additional information could also be maintained on this web server such as traveling tips, security tips, links to websites with related information, and other forms of preventative measures. Some sites that can provide you with additional information include the Corporate Travel Safety Website, The Defense Security Service Academy's Security of Laptops site as well as their Theft while traveling site.

Conclusion

The user of a laptop has to take full responsibility for it when it's taken out of the office for whatever reason. Fortunately with a little education and common sense we can help the user become more aware of the responsibilities that go along with operating a laptop computer. This paper can be considered a starting point on securing a laptop computer. There is always a new threat or challenge to be met and the only way you can do that is by being ever vigilant. Stay abreast of changes in technology, the latest security alerts, and anything that you feel will help you to do your job better, a little luck can't hurt either.

Trademarks

Microsoft, Windows XP, Windows 2000, Windows 98, Windows ME and Windows are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A and other countries.

All other names are registered trademarks or trademarks of their respective companies.

References

[1] Spooner, John G. "Notebook sales on the go again." May 3, 2002.
URL: http://news.com.com/2100-1040-898370.html (10/02/03)

[2] 2001 Loss Statistics Charts. Safeware, The Insurance Agency, Inc.
URL: http://www.safeware.com/losscharts.htm (10/02/03)

[3] BBC News. "Defense consultant's laptop stolen" April 16, 2001.
URL:http://news.bbc.co.uk/1/hi/uk/1279584.stm (10/02/03)

[4] Gold, Steve. "FBI Laptop Stolen." April 19, 2000
URL: http://www.computeruser.com/newstoday/00/04/19/news2.html (10/02/03)

[5] Schiffman, Betty. "Stolen Qualcomm Laptop Contains Sensitive Data."
September 19, 2000
URL: http://www.forbes.com/2000/09/19/mu5.html (10/02/03)

[6] CNN.Com. “Prada Lawyers’s laptop stolen.” December 3, 2002
URL: http://europe.cnn.com/2002/WORLD/sailing/12/03/prada.laptop (10/02/03)

[7] Lyman, Jay “Feds Report Lost Laptops, Weapons.” August 5, 2002.
URL: http://www.newsfactor.com/perl/story/18889.html (10/02/03)

[8] Defense Security Service Academy “Security of Laptops.” Employee’s guide to security responsibilities. Version 1.0
URL: http://www.mbay.net/~heuer/V1comput/Laptops.htm - Security%20of%20Laptops (10/02/03)

[9] Tom, Pamela. “Have Lost Laptop, Will Travel” February 21, 2002.
URL: http://www.techtv.com/news/culture/story/0,24195,3373022,00.html (10/02/03)

[10] Power, Richard. “2002 CSI/FBI Computer Crime and Security Survey.” Computer Issues and Trends. Volume VIII, No. 1. Spring 2002.

[11] Karagiannis, Konstantinos and Sarrel, Matthew D. “Keep Hackers Out: Part One, Personal Edition” November 19, 2002.
URL: http://www.pcmag.com/article2/0,4149,639280,00.asp (12/02/03)

[12] Caveo Anti-theft PC Card. Caveo Technologies
URL: http://www.caveo.com/ (12/02/03)

Belkin International – Notebook Security Locks
URL: http://www.belkin.com/ (12/02/03)

Targus – DEFCON cable locks and alarms.
URL: http://www.targus.com/accessories_security.asp (12/02/03)

Kensington - SonicLock™ and cables.
URL: http://www.kensington.com/html/1434.html (12/02/03)

PC Guardian – Notebook Guardian.
URL: http://www.pcguardian.com/ (12/02/03)

@Stake’s L0phtCrack
URL: http://www.atstake.com/research/lc/ (12/02/03)

Symantec’s Norton Antivirus 2003
URL: http://www.symantec.com/nav/nav_9xnt/ (12/02/03)

McAfee Security’s VirusScan 7.0
URL: http://www.mcafee.com/myapps/vs7/ (12/02/03)

Symantec’s Norton Internet Security 2003
URL: http://www.symantec.com/sabu/nis/nis_pe/ (12/02/03)

Zonelab’s Zone Alarm
URL: http://www.zonelabs.com/store/content/home.jsp (12/02/03)

Internet Security System’s BlackIce
URL: http://blackice.iss.net/ (12/02/03)

Home PC Firewall Guide
URL: http://www.firewallguide.com/ (12/02/2003)

LavaSoft’s Ad Aware
URL: http://www.lavasoftusa.com/ (12/02/03)

PepiMK Software’s Spybot Search & Destroy
URL: http://spybot.eon.net.au/ (12/02/03)

Pest Patrol Inc.’s PestPatrol
URL: http://www.pestpatrol.com/ (12/02/03)

Tips for Preventing Laptop Computer Theft
URL: http://mpdc.dc.gov/info/consumer/laptop_theft.shtm (12/02/03)

Ztrace Technologies Ztrace Gold
URL: http://www.ztrace.com/zTraceGold.asp (12/02/03)

Absolute Software’s ComputracePlus
URL: http://www.absolute.com/public/products/computraceplus/default.asp
(12/02/03)

Stealth Signal Inc.’s Asset Recovery
URL: http://www.stealthsignal.com/web/main.asp?co=us&lang=en (12/02/03)

Computer Sentry Software’s The CyberAngel
URL: http://www.thecyberangel.com/cyberangel.html (12/02/03)

Elmy-Liddiard, Martyn. “Building and Implementing an Information Security Policy.”
April 30, 2002
URL: http://www.sans.org/rr/policy/building.php (12/02/03)

“Laptop Theft, Know Before You Go: Why Criminals Steal Laptops”
URL: http://www.corporatetravelsafety.com/laptoptheft.html (12/02/03)

Gibson Research Corporation
URL: http://grc.com/intro.htm (12/02/03)

Ryder, Josh “Laptop Security, Part one: Preventing Laptop Theft” July 30, 2001
URL: http://online.securityfocus.com/infocus/1186 (12/02/03)

Ryder, Josh “Laptop Security, Part Two: Preventing Information Loss” August 13, 2001.
URL: http://online.securityfocus.com/infocus/1187 (12/02/03)

“Guide to Securing Microsoft Windows XP.” United States National Security Agency. Version 1.0. October 30, 2002.
URL: http://nsa2.www.conxion.com/winxp/download.htm (12/02/03)

“Windows 2000 Security Recommendation Guides.” United States National Security Agency. Version 1.0.8. October 17, 2002.
URL: http://nsa2.www.conxion.com/win2k/download.htm (12/02/03)