Global Information Assurance Certification Paper

GSEC Assignment v1.3
Thomas Ventura

Laptop Security Recommendations

Summary

The purpose of this paper is to discuss precautions that should be taken with the laptop computers in your organization. All security implementations should start with a security policy, which is the backbone of the entire security strategy. From there, a good laptop security strategy should focus on three main areas: Theft, Data Backup/Management, and Operating System Security. Theft was one of the earliest problems with laptops due to their high monetary value in a small package. Data backup is important in order to prevent data loss in the event of damage to or theft of the laptop. Data management is especially important in regards to retention, particularly after the recent focus on data retention in the post-Enron world. Finally, OS security is important to protect the laptop and its data in the many different LAN/WAN/Broadband/Wireless environments it will be placed in. Overall, laptop security requires extreme scrutiny in order to protect your mobile computers in the multitude of environments in which they operate.

Introduction

According to the Maine Antique Digest, in 1979, the Grid Compass claimed to be "the first ever lap-top computer." With "340K byte bubble memory lap-top computer with die-cast magnesium case and folding electroluminescent graphics display screen,[1]" this machine is a far cry from the laptops of today with 1000 times the amount of memory. At the time of the Compass' development, security was probably not the principle goal of the final architecture. Of course, as the technology continues to expand, the amount of potential vulnerabilities also continues to expand. Today, security is becoming a major design goal with some of the latest generation of laptops being shipped with integrated security devices [2].

The first step in any security implementation is a solid security policy. "An effective security policy is as necessary to a good information security program as a solid foundation is to a house[3]." Without a laptop security policy all of the recommendations in this paper will be short-term solutions. A large part of

[1] McKay, http://www.maineantiquedigest.com/articles/l030896.htm
[2] http://www.pc.ibm.com/ww/resources/security/index.html
[3] King, et al, p.13

security is limiting access and, in the eyes of your users, making their ability to work more difficult. Why should a user allow a personal firewall, which disables the use of their favorite file-swapping tool, to be installed on the laptop? A policy is required to grant the authority to implement security measures which may appear intrusive to the user. A policy must also be enforceable—for example, without police enforcement, most people would drive much faster than the posted speed limit. However the amount of accidents and deaths related to speeding would most likely increase in parallel. Therefore, develop a solid laptop security policy first and then apply the recommendations in this paper in order to comply with the established policy. A good place to obtain some sample security policies is at http://www.sans.org/newlook/resources/policies/policies.htm. Once a laptop security policy is in place your security strategy needs to be aligned with this policy. A good laptop security strategy should attempt to address three important issues:

- Theft
- Data backup/Management
- Operating System Security (protection from viruses, hackers, etc.)

When developing your strategy it is very important to keep the concept of defense in depth in mind. Todd McGuiness wrote,

> Implementing a strategy of defense in depth will hopefully defeat or discourage all kinds of attackers. Firewalls, intrusion detection systems, well trained users, policies and procedures, switched networks, strong password and good physical security are examples of some of the things that go into an effective security plan. Each of these mechanisms by themselves are of little value but when implemented together become much more valuable as part of an overall security plan.[4]

When determining a solution to each security problem, try to think of multiple ways to accomplish the same goal and implement both if possible. Both solutions need not be technical—for example, in order to prevent password theft, require that users only login in areas where they cannot be observed *and* enforce strong passwords and short password expirations.

According the Jones International, some of the earliest electronic computers were half the size of a football field and required enough electricity to power a

[4] McGuiness, http://rr.sans.org/securitybasics/defense.php

city[5]. There was very little concern that someone would simply pick up this computer while no one was looking and walk away with it. Today, the equivalent computing power can be packaged in a device the size of a notepad. This leads us into the first issue with laptop security, Theft.

Theft

The Computer Security Institute reported that approximately 57% of corporations experienced a loss related to laptop theft and an insurance industry estimate states that over 319,000 laptop were stolen in 1999[6]. In addition, according to a Gartner Group estimate, each laptop theft incident costs over $6000, not including the value of the data contained on the computer's hard drive[7]. Thus, the cost for the entire industry in one year can be approximated at nearly two billion dollars. A famous example of a laptop theft involved the laptop of Qualcomm's CEO, Irwin Jacobs. According to an article at usatoday.com, "Jacobs left the computer unattended on a podium or an adjoining table in the Hyatt Regency-Irvine ballroom on Saturday for 15-20 minutes". More valuable than the actual hardware, the data on the laptop consisted of "proprietary information that could be valuable to foreign governments." Had Jacobs followed some of the basic precautions detailed below he would not have had much to worry about.

In most cases, laptop theft can be prevented. 95% of laptops are equipped with a hole designed for use with a lock yet, according to Cathie Smithers of Kensington Technology Group (a maker of laptop locks), only 10 locks are sold for every 100 laptops[8]. These cables can be used to lock the laptop to a desk or other stationary piece of furniture wherever the laptop is in use. If Jacobs had locked his laptop to the podium it would have made it much harder for a thief to walk away with it.

Laptops can also be stolen while the user is in transit. Ask users not to carry their laptop in standard laptop bags. These bags are the equivalent of wearing a sign on your back that says, "I'm carrying thousands of dollars worth of computer gear". Instead, recommend padded backpacks or other inconspicuous briefcases. One problem, which has increased dramatically since the post-September 11th security measures were implemented at US airports, is the requirement that laptop computers be removed from their cases and be placed on the x-ray machine conveyor belt by itself[9]. At the same time as the laptop is

[5] LaMorte, http://www.digitalcentury.com/encyclo/update/comp_hd.html
[6] Vincet, et al, http://www.cnn.com/2000/TECH/computing/09/20/laptop.security.idg/
[7] Ploskina, http://zdnet.com.com/2100-11-503957.html?legacy=zdnn
[8] Ploskina, http://zdnet.com.com/2100-11-503957.html?legacy=zdnn

passing through the scanner the owner is being scanned extensively. If the scanning of the owner takes longer than the scanning of the laptop then laptops begin to gather at the end of the conveyor belt. This provides an opportunity for either intentional or accidental theft of the laptop. In order to help prevent accidental theft, laptop owners should place a clear label on top of the machine with their name and tape a business card to the bottom for return to the proper owner. Preventing intentional theft is much harder. The only real way to prevent theft while passing through airport security is to personally carry your laptop through the scanner—a nearly impossible task with today's new airport security measures.

Laptop theft is difficult to avoid. However, there are many steps that can be taken to minimize the loss. In many cases the biggest concern regarding laptop loss is the confidentiality of the data on the missing computer. The best way to mitigate this risk is via the use of encryption.

Encryption can be used in many different manners depending on the sensitivity of the files on the machine. If very few documents are considered sensitive, then simple file encryption tools such as PGP[10] can be used to encrypt individual files. For more extensive file system encryption, Windows 2000 and XP now include EFS (encrypting file system[11]), plus many tools are available to encrypt Unix file systems such as CFS (Cryptographic File System[12].) For advanced file encryption, products from companies such as Authentica[13] provide "file shredding," the ability to recall documents even if it is already on a client's local hard drive. These products function by encrypting each file with a key that is stored on a server accessible via the Internet. Every time the file is accessed, it checks with this server to determine if the user still has permission to access it. If access is denied, then the file is useless unless someone can crack the encryption on the file. The use of bios and hard drive passwords is another layer of defense, although simply removing the CMOS battery can erase most bios passwords. Of course most encryption, in order to function in the mobile world of laptops, rely on a single, weakest link: passwords.

When users are left up to their own means they choose weak passwords. According to a British study, "around 50 percent of computer users base them on the name of a family member, partner or a pet.[14]" The best way to eliminate

[9] http://www.faa.gov/apa/tipbroch.htm
[10] http://web.mit.edu/network/pgp.html
[11] http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/efsguide.asp
[12] http://www.ensta.fr/internet/unix/sys_admin/CFS.html
[13] http://www.authentica.com/products/default.asp

this risk is to implement strong password policies that require a minimum of 10 characters, frequent changes, and the use of a mix of numbers, letters and special characters. One way to help ease the acceptance of longer passwords is the start using the term "passphrase." This encourages users to pick a sentence from a favorite book or a famous quote with which they can inject some special characters and numbers into to provide a very strong password. Since users frequently take advantage of the check boxes that offer to "Save Password," another recommendation is the requirement for two-factor authentication for remote access dial-in or VPN connections.

Two-factor authentication basically requires that the user provide two different means of proving who they are—usually a combination of a secret password and such things as a non-reusable token-based password, a smart card or even biometric authentication. RSA's SecurID[15] product line provides non-reusable token-based passwords via devices that generate a new code every 60 seconds in sync with the RSA server on your network. This generated code is combined with the user's password to provide a unique password for authentication into your network. RSA's SecurID product line also includes smart card authentication that requires that the user insert their unique smart card into the machine as an additional level of authentication. Finally, biometric authentication can be used to guarantee the identity of the user. Targus produces a Fingerprint scanner that can be attached to a laptop computer via a USB port[16], which allows the user to use their finger as the second factor for authentication.

One aspect of laptop theft that is not discussed very often is theft by the user. How many users who claim to have forgotten their laptop in a taxi actually shipped it to their daughter in college? How do you force a terminated employee to return their laptop without a lengthy legal battle that inevitably costs more than the laptop itself? The first step is to make sure that every piece of computer equipment owned or leased by the company is insured against theft and damage. Companies should also require users to sign agreements when laptops are issued acknowledging that the laptop is the property of the company and must be returned immediately when requested to do so. Some corporations have turned this situation around and require that the user buy or lease the laptop directly and either expense leasing costs or the employer provides a written agreement to purchase the laptop from the employee upon their

[14] Brown, http://www.cnn.com/2002/TECH/ptech/03/13/dangerous.passwords/index.html
[15] http://www.rsasecurity.com/products/securid/
[16] http://www.targus.com/accessories_security_specific.asp?title=TARGUS+DEFCON+AUTHENTICATOR+WITH+USB+HUB&sku=PA460U

termination or for hardware refreshes. Even though the laptop is insured the mindset that the user "owns" the computer helps to discourage "misplacing" it.

Data Backup/Management

So now that the laptop is stolen and all of the data is unreadable, how do you get the data back? Many people use removable storage such as CD-Rs or Zip disks for backups, but they inevitably store the backups in the laptop bag that was stolen with the laptop! A more robust solution is available via products that provide remote backups over the Internet or LAN connections to a central server. Products such as Connected TLM[17] can automatically backup data securely to a remote server when a connection to the Internet is detected. This eliminates the worries of managing backup media, which can be lost or stolen as well. These products also allow users to restore files from any location connected to the Internet in case a file becomes corrupt.

Another challenge, which has recently been put into the spotlight with the recent Enron debacle[18], is that of data retention. Users need access to their documents and e-mail messages while on the road so they copy the data from the controlled environment of a file or e-mail server down to their desktop or e-mail personal folders. Keeping track of these files is nearly impossible without some sophisticated desktop management solutions. The best solution is the implementation of policies that ban the use of personal folders for e-mail and require that users check files back into file servers whenever possible. In order to enforce the policy, random audits need to be undertaken on laptops and re-imaging of laptops with standard images should be performed often to erase any files that may have been "lost" in the operating system.

Operating System Security

The final step in laptop security is the securing of the operating system on the laptop in order to protect the user from attacks from viruses, trojan horses, hackers and crackers in the various environments where they will use their laptop. The biggest difference between desktop computers and laptops is that, in most cases, desktops are used in a controlled environment where the local LAN is monitored and protected with a network security policy. Laptops are constantly being plugged into various environments—whether it is a DSL connection at the user's home, a LAN at the client site, or a LAN at a Hacker's conference! There are hundreds of documents available on how to lock down various operating systems from such sources as SANS[19] and the US National

[17] http://www.connected.com/products/index.htm
[18] http://www.washingtonpost.com/wp-dyn/business/specials/energy/enron/

Security Agency[20] which should be implemented on any computer, regardless of the use of desktop of laptop hardware. However, extra measures need to be taken on laptops.

Every computer should be running antivirus software. In a corporate LAN environment antivirus software can be centrally managed and antivirus pattern updates can be deployed and verified with relative ease. Managing traveling users is a much harder task. Train users how to check their antivirus software for functionality and updates. Products such as InfoExpress CyberGatekeeper[21] can actually monitor remote users when they connect to corporate LAN and verify they have the proper antivirus updates before permitting them on the network.

Another standard component for mobile users is the use of software-based personal firewalls in conjunction with personal hardware-based firewalls. Darrell Keller wrote,

> There are a lot more hackers in the world today, because of the increased access to computers and because of the scripts that have been made, allowing anyone with the desire to try to hack the ability to do so. It takes little real hacking knowledge for most attempts. Script Kiddies download their favorite hacking tool and start playing. Because most people don't protect their home network or their laptops when on the road, the Script Kiddies can have a field day. So what about personal firewalls? That is probably the best answer for these travelers and not a bad idea for home users, even if they have a Linksys box (defense in depth).[22]

The hardware firewall can be easily configured to prevent inbound connections to a personal network and provide basic packet filtering. One configuration for a personal hardware firewall could disable all inbound-initiated traffic and only allow outbound communications on port 80 and port 443 (HTTP and HTTPS) as well as allow IPSec and/or PPTP pass-through for VPN connections. A software-based firewall can provide egress filtering, stateful inspections and basic intrusion detection as well as provide redundant packet filtering. Some software firewalls can be configured for different security profiles and apply specific profiles depending on the network the computer is attached to. For example,

---

[19] http://www.sans.org
[20] http://nsa1.www.conxion.com/
[21] http://www.infoexpress.com/products/gatekeeper/index.html
[22] Keller, http://rr.sans.org/firewall/corp_laptops.php

you probably want to allow RPC communications for Windows clients while connected to the office LAN so users can access MAPI-based e-mail, Windows file servers, and most other Microsoft Back Office products. However, when users are connected to a foreign network it is probably a good idea to disable all RPC communications to prevent file and null shares from being exploited on the machine. The combination of the two firewalls can hopefully provide a safe haven for your mobile users.

One very important piece of preventing attacks is to disable administrator or superuser access to mobile users on their laptops. This helps to avoid the "shoot yourself in the foot" attacks where users install a piece of malware that wreaks havoc on their machine. Create a standard corporate image for each type of user in your organizations (sales, engineering, customer service, etc.) and install the appropriate software for each user. Also create a simple request for software installation form to prevent users from trying to circumvent this policy.

A simple change that should that should be made on all computers, but is especially important on laptop computers, is the use of password protected screen savers with short activation timers. If a laptop is left unlocked at a client location then anyone who walks over to that laptop has anonymous access to every file and e-mail sitting on that computer. The real user of the laptop could never know that someone had been reading his or her client list or even a proposal for a competitor.

Another change that should be made on laptops is the configuration of the web browser on the machine. The standard configuration of the most used browser in the world[23], Internet Explorer 5, permits ActiveX, Java, and JavaScript to be run on the local machine. Performing a search for "IE and (Java or ActiveX) at NTBugtraq.Com turned up over 50 hits discussing various security holes in Internet Explorer[24]. Disabling ActiveX, Java and JavaScript would eliminate the risk but this can cause another issue-many trusted applications rely on ActiveX, Java or JavaScript to provide advanced functionality. The best way to control which sites can run ActiveX, Java or JavaScript in Internet Explorer is through the use of Web content zones. Internet Explorer has a four separate security zones: Internet, Intranet, Trusted Sites and Restricted Sites. In order to mitigate the risk to traveling users all zones can set to Custom with all ActiveX, Java and Scripting set to Disabled. All internal web sites and other trusted web sites can be added to the list of Trusted Sites. Security for the Trusted sites zone could be then set to allow ActiveX, Java and/or JavaScript to be enabled. In order to

[23] http://www.websidestory.com/cgi-bin/wss.cgi?corporate&news&press_1_173
[24] http://www.ntbugtraq.com

standardize the configuration for all client machines, a Windows 2000 Group Policy can automatically configure the zones when users login, or a login script can be utilized in other environments (such as Unix or Netware.) Unfortunately, the latest version of Netscape Navigator (v.6.2) does not support multiple zones. Netscape Navigator 6.2 does not provide ActiveX support but Java and JavaScript is enabled by default. The only option for Java and JavaScript in Navigator is either enabled or disabled, with no option to configure their support exclusively for trusted web sites. Due to the lack of flexibility in Navigator it is recommended that Java and JavaScript simply be disabled.

The final piece of Operating System Security is the management and installation of software patches, hotfixes and updates. Performing a keyword search at Microsoft.com for "security" for Windows 2000 and all dates returned over 200 results containing OS updates and security tools[25]. It is very hard to keep up with all of the patches that are released on any type of computer. In most corporations it is manageable to perform software updates on desktop computers because they are always in the office and are usually not in use for 16 hours of the day. Using system management software, jobs could be scheduled to perform installations and, in smaller organizations, software installations can be performed manually by the IT staff during off hours. Laptop users cause a problem because they are most likely using the laptop for 8 hours a day then they take the machine home or on the road the remainder of the day. At the minimum, schedule monthly maintenance checkups with every laptop user and, for urgent patches, have a mechanism in place to deploy updates to users in the field. This could be simply sending out the update as an attachment to an e-mail message or it could be sending out a voicemail directing users to an externally accessible web site to download and install the patches.

Conclusion

As we can see, securing mobile computers should not be taken lightly. Laptop computing is one of the few areas of IT security where the worst-case scenario is usually the most common scenario. Also, as technology evolves, laptops are becoming desktop computer replacements. The problem will only get bigger and the risks will be greater as more and more users are taking their computer out of the office. As mentioned earlier, the start to any security endeavor is the creation of a sound security policy. From there a strategy needs to be developed to enforce the policy, keeping in mind the philosophy of defense in depth. If the time is taken to create a solid strategy and it is implemented in a consistent fashion then the goal of secure, mobile computing is attainable.

[25] http://www.microsoft.com/downloads

References

King, Christoper M., Dalton, Curtis E., Osmanoglu, T. Ertem. Security Architecture: Design, Deployment & Operations.Berkeley:Osborne/McGraw-Hill, 2001

McKay, Ian. "The First Laptop?" 1996. URL: http://www.maineantiquedigest.com/articles/l030896.htm (3 April 2002).

"IBM Client Security Solutions." URL: http://www.pc.ibm.com/ww/resources/security/index.html (3 April 2002).

"Security Tips for Air Travelers." URL: http://www.faa.gov/apa/tipbroch.htm (3 April 2002).

"MIT Distribution Site for PGP." URL: http://web.mit.edu/network/pgp.html (3 April 2002).

"Step-by-Step Guide to Encrypting File System." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/efsguide.asp (3 April 2002).

"Products. "URL: http://www.authentica.com/products/default.asp (3 April 2002).

"RSA SecurID." URL: http://www.rsasecurity.com/products/securid/ (3 April 2002).

"Connected TLM." URL: http://www.connected.com/products/index.htm (3 April 2002).

"Enron Probe" URL: http://www.washingtonpost.com/wp-dyn/business/specials/energy/enron/ (3 April 2002).

"SANS Institute." URL: http://www.sans.org (3 April 2002).

"National Security Agency: Security Recommendation Guides." 27 December 2001. URL: http://nsa1.www.conxion.com/ (3 April 2002).

"InfoExpress Products." URL: http://www.infoexpress.com/products/gatekeeper/index.html (3 April 2002).

McGuiness, Todd. "Defense in Depth." 11 November 2001. URL: http://rr.sans.org/securitybasics/defense.php (3 April 2002).

LaMorte, John. "Computers: History and Development." 1999. URL: http://www.digitalcentury.com/encyclo/update/comp_hd.html (3 April 2002).

Keller, Darrell. "Protecting Your Corporate Laptops from Hackers, While they are on the Road." 29 May 2001. URL: http://rr.sans.org/firewall/corp_laptops.php (3 April 2002).

Vincent, Christie and Vaughan, Jack. " Security experts seek to curb laptop theft." 20 September 2001. URL: http://www.cnn.com/2000/TECH/computing/09/20/laptop.security.idg/ (3 April 2002).

Ploskina, Brian. "Laptop theft causing global havoc." 2 August 2001. URL: http://zdnet.com.com/2100-11-503957.html?legacy=zdnn (3 April 2002).

"CFS." 1996. URL: http://www.ensta.fr/internet/unix/sys_admin/CFS.html (3 April 2002).

Brown, Andrew. "UK study: Passwords often easy to crack." 13 March 2002. URL: http://www.cnn.com/2002/TECH/ptech/03/13/dangerous.passwords/index.html (3 April 2002).

"Popularity of Microsoft Internet Explorer 6 Pushes Netscape to an All-Time Low." 27 March 2002. URL: http://www.websidestory.com/cgi-bin/wss.cgi?corporate&news&press_1_173 (6 April 2002).

URL: http://www.ntbugtraq.com (6 April 2002).

"Microsoft Download Center." URL: http://www.microsoft.com/downloads (6 April 2002).

"Targus DEFCON Authenticator with USB Hub." URL: http://www.targus.com/accessories_security_specific.asp?title=TARGUS+DEFCON+AUTHENTICATOR+WITH+USB+HUB&sku=PA460U (7 April 2002).