Global Information Assurance Certification Paper

Defense-In-Depth Applied to Laptop Security: Ensuring Your Data Remains Your Data

Chris Grant
October 14, 2003
GIAC GSEC Practical – Version 1.4b, Option 1

Table of Contents

Abstract

As the use and need for mobile computing grows in the global, interconnected economy, so does the need for mobile data protection. This paper illustrates how to apply a Defense-In-Depth strategy to protect laptop systems.

Security topics addressed in this paper are confidentiality, integrity, availability, identity, authentication, and authorization, with specific focus given on how to achieve functional, convenient and effective security utilizing hardware and software available on the market today.

This paper will review security-specific hardware and software applied to mobile computing. Several laptop manufacturers, such as Acer[1], Compaq[2], MPC[3] and IBM[4], have added security focus features to certain models. Other vendors have focused on augmenting laptop vendor's systems with hardware-based encryption engines, such as CryptCard[5], and security-specific authentication and encryption software, such as SafeBoot[6].

Introduction

The greatest attribute of a laptop is its portability; however, it is also its greatest weakness as laptops are easily lost or stolen. As the weight and price of laptops have decreased and their computing power and ease of use increased, so has their popularity for use as primary computers for personal and business situations[7]. Naturally, more and more personal and business data is being kept on laptop systems. These factors alone should be cause for concern for private

citizens and even greater concern for business organizations. In recent years, the media has reported on several high-profile computer thefts that have resulted in either known, highly sensitive information being lost or worse, information of unknown severity being lost to an unknown party.[8, 9]

While technologies and methods for laptops have existed for several years[10], advances in technological capability along with the economic viability of providing portable security devices have allowed organizations and laptop manufacturers alike to implement more security-focused capabilities into mobile computing platforms. A Defense in-Depth strategy specifically to the unique and specialized needs of laptop security is now more easily implemented and managed, as well as being less noticeable to the end user and more secure.

Special Security Considerations Needed for Laptops

Securing laptops to ensure the confidentiality, integrity and availability of both data and security applications requires special consideration to be paid to the typical, mobile environment in which a laptop would typically be utilized. (While the security of laptop devices is addressed here, these same technologies and concepts can often be applied to other mobile platforms, such as PDAs and desktop systems which contain sensitive data.)

First, the security infrastructure of the laptop must be able to be operated in a local, single machine without connectivity to the primary security infrastructure. As an example, the laptop must be able to operate the local security systems without the aid of the native security of an available, network-connected Windows domain architecture. This is important to ensure there is no compromise made in user identification, authentication and authorization while the system is not connected to the home network.

Secondly, the protection of the device and all running software is more critical because, again the laptop's greatest strength is also its greatest weakness, the portable nature of a laptop. A laptop is easily moved from a public location to a 'safe', private location where attempts to gain access to the system can be performed at the discretion of the thief. Security must be strong and multi-tiered to prevent access, because time to perform cracking attempts is practically unlimited.

Thirdly, security is more critical because of the demographics of a typical laptop user. Most mid to high-end laptops are significantly more expensive than their standard desktop counterpart. The economics of purchasing laptops for users most often drives companies to only purchase laptops for employees who truly need them. Employees who truly need laptops are those who travel often (another significant expense for companies, which is also typically reserved for those employees who truly need to travel). These reasons will typically dictate laptop purchases being reserved for those in upper level management or other

higher level positions where access to the home office, along with all the data and applications associated with their position, is required from a remote location. In these types of job positions, data is not typically the type which is already published to the world, but highly proprietary or confidential internal company information which is being used to guide the company forward, potentially revealing future acquisitions, mergers or reorganizations. All damaging information to the companies involved if made available to the public or competitors.

Lastly, one of the main benefits of having a personal laptop is for the convenience of having computing and networking resources easily accessed, wherever the user is located. In order for security to be universally and effortlessly adopted (over the more popular convenience of not having security), security features must be simple to implement, use and manage. Enabling security features must not significantly inconvenience the user of the system, furthermore the user must not have the desire (or even presented the option, ideally) to disable security features. Security features are only as good as they are functional.

Identity, Authentication and Authorization

On any computer system, the user presenting identity is the starting point to establishing what rights and privileges, or authorization, if any, is granted the user. Obviously, if an unauthorized person can falsely authenticate him or herself as someone who is trusted, all security measures are irrelevant. The goal of strong authentication systems is to ensure the person authenticating is exactly, and in all cases, the person who should be authenticating. In a secure environment, presenting identity should consist of at least two of the following:

1) Something You Know, a password, passphrase or other memorized information (typically matched with a user name)
2) Something You Have, a hardware token or smart card
3) Something You Are, biometrics such as fingerprint, retinal or facial recognition

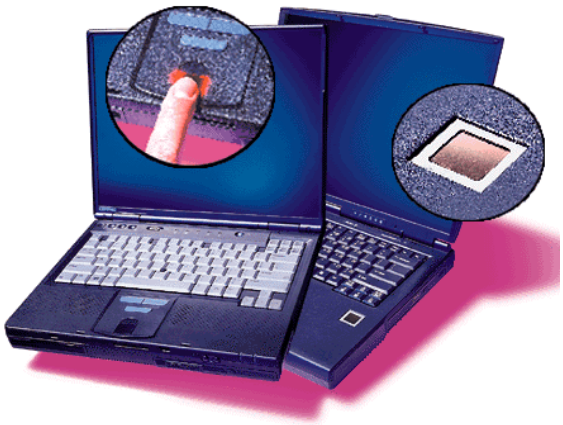
The first, most commonly used method of identification is the combination of User Name and password. Identification is provided as 'something you know'. The User Name should consist of a unique identifier, such as combining the first initial of the user with their last name, as well as a strong, not easily guessed password. (Although one could argue having an easily guessed user name is not desirable either.) Ensuring the password is strong is most commonly established through a password complexity policy defined in the security infrastructure. In a Microsoft Windows based security infrastructure, the policy is defined at the domain controller level, however, the User ID, password and login environment (profile) are cached locally, enabling the user to identify,

authenticate and receive authorization to the local system even if the corporate security infrastructure is not available.

The most common method to achieving two-factor authentication is by augmenting the standard user name and password, as 'something you know', through the use of hardware tokens or smart cards (examples pictured above[11,12,13]), or 'something you have'. Tokens and/or smart cards are available from vendors such as RSA[14], Authenex[15], eAladdin[16] and ActivCard[17].

Each vendor has a different approach to their respective solutions for adding 'something you have' to 'something you know'. RSA has several types of tokens which involve an algorithm generated passcode that shifts each minute. Authenex provides a USB-based token that interacts with software installed on the local machine to authenticate VPNs, web sites and logins. Smart cards, provided by many vendors, including eAladdin and ActivCard, provide the physical media to integrate with smart card aware operating systems and applications, such as Microsoft Windows 2000 and Control Break's SafeBoot (more detail to follow).

In order to be effective, however, all solutions need to be managed effectively in an enterprise environment to remain consistently utilized and administered. Microsoft began actively supporting the trusted public key infrastructure (PKI) model and therefore smart cards when Active Directory was implemented as a part of the Windows 2000 security infrastructure.[18] As a result of Microsoft's greater emphasis on secure computing, Windows Server 2003 enables enhanced management and stronger ties to the public key infrastructure (PKI) used in smart cards' two-factor authentication technologies.[19]

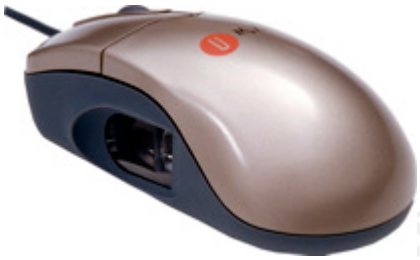


Biometrics can be used to augment 'something you know', such as a user ID and password, with 'something you are', namely something unique to your person, such as fingerprints, retinal or facial recognition. Adding biometrics creates a second tier of identity and authentication which is easy for users to utilize.

For example, identity and authentication can be improved through the use of the built-in biometric fingerprint scanner in some models of Acer, Compaq and MPC laptops

(representative pictures on previous page and left[20]). When the biometric identification devices are built into the laptop proper, without requiring additional external hardware, the biometric scanner hardware and authorization software can be used earlier in the boot up process, denying access more quickly to invalid attempts to boot the system.
1000001
Pre-boot identification and authentication ensures no access will be gained through operating system or application vulnerabilities, or potentially other backdoors such as remote control software, keyboard loggers or viruses/worms that could be exploited after the system is booted. As an example, biometric identification and authentication could be implemented at the BIOS level as simply another form of BIOS password. Choices in the BIOS such as '[text password] off', '[text password] on', or 'fingerprint'. The MPC laptop BIOS has additional features to protect against brute force attempts to disable the biometric authentication. After three invalid attempts to identify and authenticate, the BIOS will prevent you from attempting again without a reboot. If attempts are made to remove the boot password (text or fingerprint identification), the system will eventually hard lock and will require shipping the laptop to the vendor to unlock it.

1



1Once the operating system is booted, options typically exist to use the stored biometric information or match it with a user ID/password for login purposes, as well as providing authorization to applications which may not have native biometric or other application security. After market hardware is available for those laptops which do not have biometrics built-in, providing the fingerprint reader within a mouse[21] or PCCard[22], for instance. Biometrics at this level will not secure the laptop hardware itself, but may provide additional software-only authentication services, such as the operating system login and/or individual program execution.

Confidentiality, Integrity and Availability

Ensuring the confidentiality, integrity and availability (CIA) of data is a core principle of network and computing security. While providing strong identity and authentication mechanisms is important to prevent unauthorized access to the system and networks, it is also important to defend against other methods of gaining unauthorized access to sensitive data, including the possibility of removing the hard drive from one system to be analyzed and attacked in another

system. Hardware and software solutions exist to help defend against this type of attack.

At the hardware level, users of IBM laptops can enable a special hard drive locking safe guard. IBM is utilizing a little used command built into the IDE specifications called an IDE password[23]. The password is stored in both the BIOS of the machine and the firmware of the hard drive[24]. When the BIOS passes the correct password to the drive utilizing the IDE password command, the drive allows the system to utilize the other IDE commands. While adding password security will thwart unmotivated thieves, companies exist which provide unlocking services for these drives[25], for a nominal fee. Of course, paying a fee would be a trivial set back to a knowledgeable and determined thief.

Following the defense-in-depth philosophy, another method of ensuring data CIA must be employed. The addition of encryption technologies will help ensure only those who have provided proper identification receive the authorization to access protected data. Typically encryption products implement several possible encryption algorithms, but many, at a minimum, will support either AES or 3DES (triple-DES). AES[26]-(Rijndael)-based encryption is chosen most often because of its resiliency to brute-force password attacks, as well as its encryption speed at high bit levels. Encryption technologies are most commonly implemented in full disk, volume and/or file and folder encryption.

The most comprehensive method of ensuring data is encrypted is to implement full disk encryption. Encrypting all partitions of a hard drive will ensure, in the event the hard drive is removed from the system and placed into another system, that no information is easily accessible which can be gathered through analyzing the data on the disk. Not only will the data be encrypted, but the software and configuration needed to connect to corporate network resources will also be protected.

Volume encryption is generally accomplished by creating a virtual disk volume in the operating system. The virtual disk is usually kept on the operating system file system as a single file. Typical access is controlled by the encryption software, which encrypts and decrypts all data being copied to or out of the encrypted volume. Relying on this method of ensuring data encryption is not recommended because the level of protection achieved is only as good as the users' will follow the procedure of copying all sensitive data to this volume. Users' can accidentally or intentionally leave data outside of the encrypted volume. Unencrypted data can be easily copied from the file system by both authorized and unauthorized users.

File and folder encryption is utilized by the user to encrypt files individually, or specific folders individually. The primary weakness of file and folder encryption is the same as volume encryption in that the level of protection achieved is only as good as the users' taking an active role in keeping their data protected.

SafeBoot[27] is an example of a product that approaches full disk encryption from a software-only solution. SafeBoot will encrypt the entire contents of the hard drive with RC5-1024 or AES-256 bit encryption. Additionally, SafeBoot will provide pre-boot identification and authentication through a user ID and password, and optionally augmented by USB-tokens and smart cards. SafeBoot is packaged as SafeBoot Professional, for stand-alone installations, as well as SafeBoot Enterprise, which adds enterprise-level encryption management tools, such as Windows Active Directory integration, group policies and key revocation and recovery. SafeBoot can provide full disk, volume or file/folder encryption.

CryptCard[28] provides a powerful, hardware-based encryption engine within an add-on PCCard. Unlike a software-only solution, the vendor states the CryptCard is more secure as a result of the encryption keys being retained on a separate, physical device from the device being encrypted, the hard drive. To retrieve the keys necessary for decrypting the hard drive a thief would be required to interface and break into the CryptCard hardware. CryptCard can provide full disk encryption as well as 'partial disk encryption', which is not fully explained in the informational materials but could presumably be either volume or file and folder encryption or both.

Both MPC and IBM implement encryption which integrates with built-in security hardware. MPC integrates the built-in fingerprint scanner with software which can encrypt and decrypt volumes and files/folders using a fingerprint for identification[29]. IBM's file/folder encryption implementation is provided by software integrated with the IBM Embedded Security Subsystem (ESS). The ESS stores encryption key information utilized in encryption processes as well as some types of network authentication.[30] Holding the private keys used to decrypt files in hardware embedded on the laptop motherboard enhances security in the same manner CryptCard achieves higher security, by storing the keys on a separate hardware device from the data being encrypted. Brute-force attacks against encrypted files are much more difficult since the private key would not be held in a file on the hard disk.

Other laptop security tools

Other innovative security devices have been produced that integrate features of previously mentioned functions, but also add unique security features.

The Targus DEFCON MDP[31] provides hardware-based encryption functions combined with motion detection. The PCCard has motion detectors that can tell when a laptop is being moved or reoriented, which typically occurs during a theft situation. If the system is moved without being deactivated, whether its powered on or off, an alarm is triggered which increases in volume as the system is in motion. Uniquely, a motion-based password can be entered to activate or deactivate the system. Specific tilts of the laptop will be recorded by the device

and can be used in conjunction with other authentication mechanisms on the system. The alarm can be an effective deterrent, barring the alarm doesn't trigger unnecessarily. Car alarms suffer from this same issue. If the alarm is triggered to often, it will be ignored by the owner and others around the system.

WaveTrend offers an identification product based on radio frequency identification (RFID) tags[32]. The RFID tag transmits unique identification information when the holder of the tag is within a certain perimeter of the reader attached to the system. Optionally, the system can be outfitted with a 'location tag'[33] that will disable functionality of the system if it is removed from the specified location.

A low technology deterrent against laptop theft, or at least resale, would be to add permanent asset tags, such as the STOP asset tags provided by Secure It[34]. The tags are semi-permanent and will 'tatoo' the laptop when the tag is attempted to be removed. This simple, obvious method of indicating the security and seriousness taken by an organization about the laptop system may provide enough to deter most petty thieves. The STOP system also provides asset recovery services and a convenient bar code to assist in corporate inventory tracking.

Conclusion

Companies need to address the security challenges of portable systems using a comprehensive defense-in-depth strategy. No single security solution will keep a determined thief from the goal of compromising the hardware or software given enough time and resources. Applying multiple layers of system security will slow the progress made by a thief, and hopefully, force the thief to abandon the pursuit, at the least, resale of the stolen property, and at worst, of confidential corporate data.

As described by this paper, many security technologies exist in both hardware and software to provide an 'off-the-shelf' solution for multiple-factor (up to three) authentication and encrypting confidential data in a portable and convenient manner. Security only needs to be one step stronger than the thief is willing to pursue. Having a defense-in-depth strategy will provide many layers of security and will ensure that your defenses are strong enough to protect your data.

List of References:

[1] Fenton, Andrew. “Security at Your Fingertips – New Notebooks Offer Biometric Protection.” March 2001 PC World Magazine. URL: http://www.pcworld.com/news/article/0,aid,38898,00.asp (10 October 2003)

[2] Fenton, Andrew. “Security at Your Fingertips – New Notebooks Offer Biometric Protection.” March 2001 PC World Magazine. URL: http://www.pcworld.com/news/article/0,aid,38898,00.asp (10 October 2003)

[3] “MPC: Presentation. Bio-Metric Fingerprint Scanner.” MPC corporate web site. URL: http://www.buympc.com/presentations/biometrics.html (01 June 2003)

[4] “Learn about IBM Embedded Security Subsystem.” IBM corporate web site. URL: http://www.pc.ibm.com/us/think/thinkvantagetech/security.html (01 June 2003)

[5] CryptCard product information. GTGI corporate web site. URL: http://www.gtgi.com/products_cryptcard.php (15 June 2003)

[6] “SafeBoot – Mobile Data Security – Security & Encryption Software for Laptop, PDA and Tablet PC” Control Break International corporate web site. URL: http://www.safeboot.com/safeboot.asp?page=productdetails&area=b2boverview&name=Enterprise&id=13 (01 July 2003)

[7] Spooner, John G. “Notebook Sales Hit New Highs.” 2 July 2003. URL: http://zdnet.com.com/2100-1103_2-1022905.html (14 September 2003)

[8] Dean, Joshua. “Lost Laptops Compromise Secrets.” 1 October 2001. URL: http://www.govexec.com/features/1001/1001managetech2.htm (14 September 2003)

[9] Bedell, Doug. “Lock Your Laptops.” 20 June 2002 URL: http://www.dougbedell.com/laptopsecurity.html (14 September 2003)

[10] Mueller, Andrew. “Laptop Security: Past, Present.” GIAC Reading Room, Travel Security. 10 July, 2001. URL: http://www.sans.org/rr/paper.php?id=409 (1 September 2003)

[11] RSA hardware token picture. RSA Security corporate web site. URL: http://www.rsasecurity.com/products/securid/images/SD200_standard.gif (01 September 2003)

[12] Authenex hardware token picture. Authenex corporate web site. http://www.authenex.com/img/018.gif (15 August 2003)

[13] ActiveCard smart card picture. ActiveCard corporate web site. URL: http://www.activcard.com/images/products/smartcard_markmartin_150x100.jpg (15 August 2003)

[14] “RSA Security Hardware Tokens.” RSA Security corporate web site. URL: http://www.rsasecurity.com/products/securid/hardware_token.html (01 September 2003)

[15] "Authenex: Products." Authenex corporate web site. URL: http://www.authenex.com/products.cfm?menu3variable=products (24 September 2003)
[16] "USB Token Authentication Device." eAladdin corporate web site. URL: http://www.ealaddin.com/etoken/default.asp?cf=tl (24 September 2003)
[17] "ActivCard | Solutions | Corporate Access Card Solutions (CAC)." ActivCard corporate web site. URL: http://www.activcard.com/solutions/id_cards.html (24 September 2003)
[18] "Windows 2000 Security Services Features." Microsoft corporate web site. 19 April 1999 URL: http://www.microsoft.com/windows2000/server/evaluation/features/security.asp (4 September 2003)
[19] "Security Innovations in Windows Server 2003." Microsoft corporate web site. 8 April 2003 URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/secinnovation.mspx (5 September 2003)
[20] "MPC: Commercial Sales: Notebooks: Transport." MPC corporate web site. URL: http://www.buympc.com/commercial/store/notebooks/overview_transport.html (01 June 2003)
[21] "Computer security – Computer Access Control through fingerprint biometric fingerprint verification and authentication." Secure-It corporate web site. URL: http://www.secure-it.com/products/umatch/index.htm (7 July 2003)
[22] "Targus Defcon Fingerprint Security Authenticator." Electronic Gadget Depot corporate web site. URL: http://www.electronicgadgetdepot.com/t/Targus/index4.htm (01 October 2003)
[23] "ThnkPad Mailing-list Archive: Re: Hard Drive password." 15 March 1995 URL: http://zurich.ai.mit.edu/hypermail/thinkpad/1995-03/0139.html (15 July 2003)
[24] "How to Bypass BIOS Passwords." LabMice.net Computer and Network Security. URL: http://www.labmice.net/articles/BIOS_hack.htm (16 July 2003)
[25] "Nortek Computers Ltd: ThinkPad Password Solutions." Nortek corporate web site. URL: http://www.nortek.on.ca/hdd_pw.html (15 July 2003)
[26] "ADVANCED ENCRYPTION STANDARD (AES) Fact Sheet." Cryptographic Technology Standards and Guidance (CTSG) Cryptographic Toolkit. URL: http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html (22 July 2003)
[27] "SafeBoot – Mobile Data Security – Security & Encryption Software for Laptop, PDA and Tablet PC." Control Break International corporate web site. URL: http://www.safeboot.com/safeboot.asp?page=productdetails&area=b2boverview&name=Enterprise&id=13 (01 July 2003)
[28] CryptCard product information. GTGI corporate web site. URL: http://www.gtgi.com/products_cryptcard.php (15 June 2003)
[29] "STMicroelectronics' TouchChip Fingerprint Biometrics Suite Protects MPC's Newest Laptops." STMicroelectronics corporate web site. 12 May 2003 URL: http://us.st.com/stonline/press/news/year2003/t1313n.htm (12 August 2003)

[30] "Learn about IBM Embedded Security Subsystem." IBM corporate web site. URL: http://www.pc.ibm.com/us/think/thinkvantagetech/security.html (01 June 2003)
[31] Targus Defcon MDP – Motion Data Protection. Targus corporate web site. URL: http://www.targus.com/us/product_details.asp?sku=PA480U (01 October 2003)
[32] "Computer security – PC and computer access control using rfid and radio frequency id tags." Secure-It corporate web site. URL: http://www.secure-it.com/products/linkit.htm (01 October 2003)
[33] "Computer security – PC and computer access control using rfid and radio frequency id tags." Secure-It corporate web site. URL: http://www.secure-it.com/products/accessories.html (01 October 2003)
[34] "Computer security and asset tracking by STOP permanent ID Trackign Tags." Secure-It corporate web site. URL: http://www.secure-it.com/products/stop/stop.htm (01 October 2003)