Encryption: Security Considerations for Portable Media Devices

With the proliferation of removable media devices, such as iPods and USB drives, large amounts of an organization's sensitive data can easily be removed. The author explores the complexities of protecting networks against removable media, including guidelines for purchasing encryption software.

Faith M. Heikkila
Pivot Group Security Consultant

In the past few years, the workforce has become increasingly dependent on being mobile, and pervasive computing has generated several devices that assist with this mobility, including laptops, USB flash drives, iPods, personal digital assistants (PDAs), CD-DVDs, MP3s, and smart phones. In fact, analysts predict the number of portable or removable media devices will reach more than 100 million by 2008 worldwide.[1] Because these devices can store between 16 to 100 Gbytes of data, organizations face an evolving problem: how to prevent insiders from using these devices to pilfer information, and protect lost or stolen portable devices. In this article, I'll examine how to develop portable and removable media security policies, as well as how encryption can assist in authenticating, authorizing, and auditing removable media devices.

Risks

Let's look more closely at some of the risks involved with portable devices.

The insider threat

Employees pose the greatest threat to the inadvertent or deliberate disclosure of personally identifiable information, trade secrets, intellectual property, and sensitive or confidential information. Additionally, not only can portable media devices used on the organization's network easily and rapidly download massive amounts of data, they can also introduce viruses or malicious code. Moreover, due to their trusted nature, these devices can bypass intrusion detection systems (IDSs) and antivirus protection safeguards. In June 2005, for example, Abe Usher of Sharp Ideas created an application called Slurp.exe specifically to show how easily and quickly data could be copied to removable media devices (in this case, iPods, PDAs, and USB drives). In his effort to raise awareness in the corporate realm of this security issue,[2] he demonstrated that this so-called pod-slurping could download more than 20,000 files per hour.[3] This alarming statistic reveals how critical it is to guard against such seemingly innocuous security threats.

PDAs, iPods, smart phones, and USB flash drives are all items that fit in your pocket—and as a result, they're easily forgotten in taxis, subways, restaurants, or airports. But the consequences of losing a laptop or a large storage device, such as a USB flash drive holding sensitive data about an organization's business, could lead to financial ruin and might destroy its reputation.[2] Despite the devastating consequences of this high risk, a recent Pointsec study indicated that 99 percent of removable media devices don't have encryption capabilities.[1]

Financial loss and compliance

The financial losses associated with inadvertent disclosure of sensitive information can be staggering.[4] In 2006, the Ponemon Institute conducted a study of actual security breach costs of organizations with prescribed regulatory compliance requirements. They found actual company costs ranging from $226,000 to $22 million at a rate of $182 per record or $4.8 million per company per incident.[5] With increasingly more members of the workforce using laptops and portable devices, the risk of inadvertent disclosure increases exponentially. Unencrypted data on laptop hard drives is

also at risk from unauthorized retrieval by disgruntled employees or intruders. Thus, all data on laptop hard drives should be encrypted to provide another layer of protection from such theft.

Regulatory compliance requires companies to adequately safeguard sensitive data from inadvertent disclosure and to provide an audit trail. Laws requiring administrative, physical, and technical safeguards for compliance include the California Senate Bill 1386 of 2002 (SB 1386), the Gramm-Leach-Bliley Act of 1999 (GLB), the Health Insurance and Portability Act (HIPAA), and the Sarbanes-Oxley Act of 2002 (SOX). Additionally, 36 states in the United States now have security breach notification laws requiring notification of unauthorized access to personally identifiable information similar to SB 1386. The European Union (EU) Data Directive also requires that personal information be protected. These laws have steep punishments for data breaches; for example, the HIPAA Security Final Ruling of 20 February 2003 imposes immense requirements on covered healthcare entities with respect to electronic patient health information (ePHI).[6] Its civil and criminal penalties for violating transaction standards range from US$100 per person to more than $250,000 per incident, plus one to 10 years in prison for the sale of ePHI.[7]

Security policy development

According to René Millman, "as long as people are fallible, they will be tempted to look at things they shouldn't or steal things from the companies they work for."[8] With recent news of stolen or lost laptops and misplaced USB flash devices, there's an urgent need to develop best practices and procedures for handling removable media device monitoring.

Security policy and procedure development has always been crucial to organizations, but it's increasingly important to develop security policies that cover portable and removable media devices as well. Such policies help ensure that all employees are on the same page with regard to handling confidential company information and equipment. Furthermore, each employee should sign a document stating they have read the removable media security policy and will abide by its terms. Training sessions concerning how to protect company data are also advisable.

Based on my three years of auditing and assessing information security and making industry best practice and regulatory compliance recommendations, here's several issues companies should consider when developing a portable and removable media device security policy:

- What's the data set the organization must protect from disclosure?
- What user groups need mobile capabilities to perform their jobs and therefore need access to removable media devices?
- What types of removable media devices are allowed to connect with company computers and networks?
- Are there any ramifications for using unapproved storage devices on company computers and networks?
- How many or what type of characters are required for strong password enforcement?
- Will the removable media device's authentication match the current access controls to gain access to the organization's network?
- Will guests be allowed to use removable media devices on company computers or networks?
- Prior to granting access to removable media devices, will the contents be examined and authorized? Which file extensions will produce a failed authorization?
- What are the procedures to follow should the encrypted removable media device be retired or re-issued to another user?
- How does the encrypted data on smart phones or PDAs get shredded; that is, how are all remnants of files and data removed from the device?
- When an employee is about to be terminated, how does the company ensure it can recover the removable media device's data?
- If the encryption software company upgrades its software or no longer supports it, how will the IT department handle this?
- Do audit logs record what an employee downloads, including file name, date, time, and user name sufficiently, or should the organization log a copy of the entire downloaded file?
- Who will receive alerts concerning the downloading of confidential information?
- If a user loses a laptop or removable media device, what are the reporting procedures to report such a loss, including customer notification? This includes reporting the loss not only to the IT department, but also notifying the customers by public means such as via the newspaper, TV, radio, mail, or email.
- Should the organization set a limit on how many sensitive files can be downloaded to a device at one time? Do laptops have different limits?

Once management and IT have discussed these questions and come up with firm decisions, they should draft a security policy outlining policies and procedures, and then have a cross-section of the company review it. The composition of this security policy committee could be people from C-level staff and managers, IT staff, and regular employees—the diversity of the committee will assist with pointing out concerns over how such a policy would affect productivity and aid in employee buy in resulting in better compliance with the policy.[9]

Laptop encryption and software

Encrypting the confidential data on a laptop's hard drive is one avenue of protecting such data should the laptop be stolen or lost. This safeguard can prevent the inadvertent disclosure of sensitive information to unauthorized parties in organizations, as well as outsiders.[1] Readily available encryption software programs can create a virtual drive wherein sensitive data files and programs are automatically encrypted. John Girard and Ray Wagner, in the Gartner Group's 29 August 2006 *Magic Quadrant for Mobile Data Protection*,[10] ranked companies that provide mobile data protection. As of July 2006, the leaders were Pointsec (http://pointsec.com/), Utimaco Safeware (http://utimaco.com/), Credant Technologies (www.credant.com/), and SafeBoot (www.safeboot.com/). Girard and Wagner further identified PGP (www.pgp.com/), Entrust (www.entrust.com), and GuardianEdge Technologies (www.guardianedge.com/) as visionaries. Per Girard and Wagner, "Visionaries have made investments in broad functionality and platform support, but their competitive clout, visibility and market share don't reach that of the leaders."[10] Sybase (iAnywhere) (www.ianywhere.com/), Reflex Magnetics (www.reflex-magnetics.com/), Bluefire Security Technologies (www.bluefiresecurity.com/), Information Security Corp. (www.infoseccorp.com/), and WinMagic (www.winmagic.com/) were identified as niche players and challengers in the laptop and removable media device market.[10] These encryption products have all received US Federal Information Processing Standards (FIPS) certification from the National Institute of Standards and Technology (NIST), which verified the encryption algorithms in the products as conforming to the Advanced Encryption Standard (AES) algorithm.[11] NIST grants FIPS certifications to products conforming to FIPS PUB 140-1 and FIPS PUB 140-2, "Security Requirements for Cryptographic Modules."[12] Table 1 depicts the companies and platforms that use the products.[10]

A plethora of software vendors are developing similar products—so how do you choose one that's right for your organization? When choosing among vendors of removable media encryption software, organizations should consider whether the encryption algorithms have been validated (for assurance that the product will protect their files) and then decide on a product that fits their needs.

To choose the right portable and removable media device encryption software, let's take a look at how the encryption software should work in order to successfully be utilized by your company. File encryption and decryption in a virtual drive should be transparent to users. There should be no degradation of speed when accessing these encrypted files: they're seamlessly encrypted and decrypted in the virtual drive, and whenever the user leaves the computer, access to these files is locked. When working on sensitive files, users should choose the option to purge the system swap files at shutdown to ensure that no files are left behind in temporary resident memory. Furthermore, in this scenario, it's advisable to also hide all other non-encrypted partitions so that users can't accidentally save their work in an unencrypted drive.

Most software installations are intuitive and require only responses to the install dialog boxes. However, it's worth mentioning that network administrators must read the software's installation guides to avoid incorrect responses during the installation process. Network administrators must make several decisions prior to beginning the installation process:

- What percentage of the drive should be dedicated to the virtual drive?
- How many and what type of characters are required for a strong password?
- Should a data shredder be installed?
- Should the laptop's owner be assigned on first logon?
- Which drive should be assigned as the virtual encryption drive?
- How many incorrect logons will be allowed prior to lockout?
- Should non-encrypted drive partitions be hidden?
- Should system swap files purge automatically at shutdown?
- Should the use of tokens be enabled?
- How does the software back up the keys?
- Do users specify their own encryption keys or should the software do it for them?[13]

Moreover, network administrators should review the choices before starting the installation process. The choices should align with the organization's security policies.

Installing virtual drives lets administrators dedicate a set amount of hard drive space to the encrypted drive. I strongly recommend that administrators generate a back-up key, copy it to a removable media device, and store it offsite[14] to ensure that encryption keys can be retrieved when necessary. Assigning an owner at first logon will require the user to create a new password to replace the default.

Once the drive is encrypted, the user will need two passwords when first booting the PC each day—one for the laptop and the other to unlock the encrypted drive. To use encrypted files, both passwords must be accepted, and administrators should set it up so that if the virtual drive password is entered three times unsuccessfully, the drive will lock and the administrator must unlock it personally. This added security feature helps prevent unauthorized users from getting too many attempts to crack the password. In addition, if the laptop is lost or stolen, the new owner won't be able to retrieve the protected data.

Table 1. Portable and removable media device encryption software companies, products, platforms, and Federal Information Processing Standards (FIPS) validation.

COMPANY/PRODUCT	PLATFORM	HIGH-LEVEL VALIDATION
Bluefire Security Technologies Mobile Security	Palm OS and Windows Mobile	FIPS 140-2
Credant Mobile Guardian	Palm OS, Windows Mobile, Research in Motion (RIM), Symbian, and Windows	FIPS140-2
Entrust Entelligence Security Provider and Entelligence Disk Security	Java, Linux, Mac OS9, Windows, Palm OS, Windows Mobile, Research in Motion (RIM), and Symbian	FIPS 140-1
GuardianEdge Technologies Encryption Anywhere Data Protection Platform 8	Windows, Palm OS, Windows Mobile, Research in Motion (RIM), and Symbian	FIPS 140-1 FIPS 140-2
Information Security Corp. SecretAgent and SecretAgent Mobile	Linux, Mac OS, Windows, Windows Mobile, and Unix	FIPS 140-1 with AES
PGP Universal	Windows, Mac OS, and Research in Motion (RIM)	FIPS 140-1 FIPS 140-2
Pointsec Mobile Technologies Media Encryption	Linux, Palm OS, Windows Mobile, Research in Motion (RIM), Windows and Symbian	FIPS 140-1 FIPS 140-2
Reflex Magnetics Disknet Pro and DataVault	Windows (others are supported through Pointsec who recently acquired Reflex Magnetics)	FIPS 140-2
SafeBoot Device Encryption	Linux, Palm OS, Windows Mobile, Windows and Symbian	FIPS 140-1 FIPS 140-2
Sybase (iAnywhere) Afaria	Linux (via Java client), Palm OS, Windows Mobile, Research in Motion (RIM), Windows, and Symbian	FIPS 140-2
Utimaco Safeware SafeGuard Enterprise	Linux, Palm OS, Windows Mobile, Research in Motion (RIM), Windows, and Symbian	FIPS 140-2
WinMagic SecureDoc	Palm OS, Windows Mobile, and Windows	FIPS 140-1 FIPS 140-2

According to the ISO 17799 security standards, passwords should have the following components: [14]

- Password expiration should be reviewed every 90 days, thus supporting the changing of passwords on a regular basis.
- Passwords shouldn't be easy to guess, nor kept on an automated log on process.
- The password should be protected and not written down or shared with anyone.
- For minimum and maximum password character length, the minimum should be set at no fewer than eight characters. Maximum would depend on the software limitations, but usually the longer the better.
- The number of incorrect logons prior to lock out should be set at three.
- Users should be required to choose several different character types for their passwords.

Network administrators should take due care when setting these rules so as to introduce the most secure solution. For example, administrators might want to have a policy that states passwords expire every 90 days, not every year. Further consideration into deciding how often a password must be changed should coincide with the sensitivity of the data being protected and the feasibility of users changing, as well as protecting, their passwords. Strong passwords require a combination of lowercase letters, uppercase letters, and a mix of numbers or other characters. Jeff Yan and colleagues found that using a passphrase or mnemonic to assist with recalling a long password enhanced users' ability to remember a strong password. [15] Their work showed how critical it is that administrators set up strong encryption software password parameters and instruct users how to create them.

Once a user enters a password, the encrypted virtual drive is opened and remains so until the user logs out. Thus, for added protection, a password-protected screensaver should be enabled and the length of time set to an appropriate number of minutes. For highly sensitive information, a shorter time period is recommended. If the computer is used in a public place, then the password-protected screensaver should activate after an even shorter time.

As mobile workers carry laptops into a variety of cul-

A successful planning and implementation process

Figure A shows that encrypting portable and removable media is a continual process. Beginning with risk assessment and regulatory compliance, it's important to first identify the critical assets and assess the organization's risk, which can be achieved through a risk assessment. If the organization is trying to achieve regulatory compliance, its initial step would be risk assessment. Next, the organization must develop a proactive security program wrapped around which encryption technology it selected as well as security policies covering portable and removable media devices. Implementation and training involves the ability to act on the chosen program swiftly by implementing an organization-specific security roadmap properly, including encryption, policies, and training. Once the overall plan is put into action, the organization repeats the entire process with ongoing auditing (via a third-party audit), adjustments for business and technology changes, and revisions to security policies. Information security best practices dictate that this occur on a regular basis.

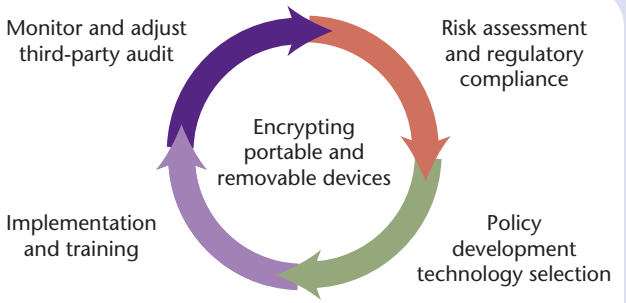

Figure A. Successful encryption of portable and removable media. The first step is a risk assessment and regulatory compliance, followed by a plan through policy development and technology selection, then action by implementation and training, followed by an ongoing third party audit, and continuing through the steps again as an ongoing process.

tures and environments, having an encrypted hard drive and a password-protected screensaver provides another layer of protection from theft or inadvertent disclosure. When laptops return to the office, they're also protected from unauthorized access by colleagues or outsiders.

Removable media encryption and auditing

Another avenue of protecting sensitive data from theft or loss due to the use of removable media is to employ removable media encryption software along with general laptop encryption. This safeguard can also restrict access to a computer's available ports. Available encryption software is capable of implementing authorization standards that allow only the copying of designated files onto removable media and encrypting data residing on these devices using AES 128/256-bit encryption automatically. Refer again to Table 1 for a list of encryption products that are FIPS certified as having correctly implemented the AES 256-bit algorithm.[12] As with the hard drive encryption software, new vendors emerge daily, so verify the desired product's encryption algorithm.

Several complexities surround the usability of encryption to protect data residing on removable media, including

- How will the encryption software for removable media affect the back-up tape encryption?
- Will there be compatibility issues with any existing encryption software currently used in the organization?
- At what level (file or folder structure) should the removable media devices be encrypted?
- What vendors provide platform-independent encryption, if needed?
- Does the chosen software let administrators override the user's password to unlock the encrypted device if the password is compromised or the employee is terminated?
- Will the encryption software include capabilities for completely removing data from the removable media device? This erasure is necessary to comply with regulatory requirements of proper disposal of personally identifiable information.

As noted earlier, encrypting files on removable media devices further protects against the inadvertent disclosure of information to unauthorized users. The encryption software an organization chooses should allow the system administrator to set permissions for each individual or user group using profiles. These profile templates typically integrate seamlessly with existing domain users and group structure to ensure ease of deployment. Whenever employees plug their USB flash drives into an organization's computer, the network must first authorize their devices, check their content, and digitally tag them before granting access. If the removable device contains legitimate files and a rogue executable, the user should have the option to browse the media and delete the unsafe files to permit authorization.

In the Windows operating system environment, a profile approach to creating user permissions that match those on the domain controller is incorporated via encryption software products. Administrators can create a guest account that grants standardized rights

for all guests or roles with corresponding access rights at the domain controller level. The encryption software then enforces these policies whenever a user logs onto the virtual drive or is authenticated to use a removable media device. Sensitive information must be included in the software-provided encrypted containers to be protected.

Once authorized, any files copied to the device should be fully auditable and stored centrally in a database. Audit logs should include what document was copied, date, time, user name, and a copy of the downloaded document. The audit logs can act as a further deterrent to employees from downloading sensitive information onto removable media. If employees know that their actions are tracked in a log, they will think twice before attempting to download files they have no business looking at in the first place. This won't, however, prevent disenfranchised employees from attempting to remove organization files they're not authorized to use, but it will provide documentation for prosecution should they be successful.

Furthermore, the removable media encryption software should enforce a virus scan of the device using the computer's antivirus software. This provides another defense against the inadvertent perpetuation of viruses on the network.

Management and the IT department should address these questions during the encryption software evaluation process and discuss them with encryption software vendors prior to purchase.

With the burgeoning popularity of removable media devices and their disclosure capabilities, it's highly recommended that encryption and auditing capabilities be in place to mitigate the risk of intentional or accidental disclosure of sensitive data. Organizations should develop a security policy for removable media devices prior to making a purchasing decision.

In addition, it's a good idea to have an independent third-party security company examine an organization's information security policies and security plan involving encryption protocols. The company should provide an objective opinion as to the feasibility of the security plan and shed insight on how to develop the appropriate security policies to protect its business assets. This second opinion will confirm that the chosen security plan and policies are indeed aligned with the company's needs. □

References

1. R. Herold, "Lexus Laptop Lockers," *Computer Security Institute Alert*, Mar. 2006, pp. 5–6.
2. A. Usher, "Sharp Ideas' Slurp Audit Exposes Threat of Portable Storage Devices for Corporate Data Theft," 25 Jan. 2006; http://sharp-ideas.net/ideas/?p=16.
3. O. Kharif, "Pod Slurping to Threaten Security," *Business Week Online*, 26 July 2005; www.businessweek.com/the_thread/techbeat/archives/2005/07/pod_slurping_to.html.
4. Y. Yuand and T.-C. Chiueh, "Display-Only File Server: A Solution against Information Theft due to Insider Attack," *Proc. ACM Workshop on Digital Rights Management*, ACM Press, 2004, pp. 31–39.
5. Ponemon Institute, Vontu, and PGP, "2006 Annual Study: Cost of Data Breach," Oct. 2006, pp. 1–24.
6. Centers for Medicare & Medicaid Services, "HIPAA Administrative Simplification—Security: Final Rule," *Federal Register*, Feb. 2003, vol. 68, no. 34, pp. 8334–8381.
7. The HIPAA Academy, "HIPAA Penalties," *HIPAA Academy.net*, 2003; www.hipaaacademy.net/hipaaPenalties.html.
8. R. Millman, "Product Reviews: DiskNet Pro 4," *SC Magazine*, http://scmagazine.com/us/products/productdetails/bb7c85ac-d983-47d7-a994-f13f48bcdc47/disknet-pro-4/ // Oct. 2004, p. 52.
9. M. Metzler, "Promoting Security Policy Longevity," *Computer Security J.*, vol. 23, no. 2/3, 2007, pp. 82–94.
10. J. Girard and R. Wagner, *Magic Quadrant for Mobile Data Protection, 1H06*, 29 Aug. 2006; http://mediaproducts.gartner.com/reprints/credant/141980.html.
11. US Nat'l Inst. Standards and Technology, "Advanced Encryption Standard Algorithm Validation List," 30 Nov. 2006; http://csrc.nist.gov/cryptval/aes/aesval.html.
12. US Nat'l Inst. Standards and Technology, "FIPS 140-1 and FIPS 140-2 Vendor List," 4 Dec. 2006; http://csrc.ncsl.nist.gov/cryptval/140-1/1401vend.htm.
13. Reflex Magnetics, "Reflex DataVault Corporate Edition Installation Guide," London: Reflex Magnetics, July 2003.
14. Int'l Organization for Standardization, "Information Technology: Code of Practice for Information Security Management," ISO/IEC 17799: British Standards Inst., 2000.
15. J. Yan et al., "Password Memorability and Security: Empirical Results," *IEEE Security & Privacy*, vol. 2, no. 5, 2004, pp. 25–31.

Faith M. Heikkila *is a security consultant for Pivot Group and has more than 18 years of paralegal and IT project management experience. Her research interests include secure remote access to organization databases, information security policies/procedures, and privacy issues. Heikkila is a member of the ACM, the Association of Information Technology Professionals (AITP), the Computer Security Institute (CSI), the IEEE, InfraGard, the Information Systems Security Association (ISSA), and the Great Lakes Interactive Marketing Association-Southwest. She's currently a PhD candidate in information systems, specializing in information assurance, at Nova Southeastern University. Contact her at fheikkila@pivotgroup.net.*