Encryption Options for Secure Portable Media

By Faith M. Heikkila

Pivot Group Information Security Consultant
And
Ph.D. Candidate at Nova Southeastern University

Introduction

- What is portable or removable media?
- Human threats
- Regulatory compliance
- Encryption software for removable media
- Security policy for removable media encryption
- Conclusion

Portable/Removable Media

- Workforce has become more dependent upon being mobile
  - – the risk of inadvertent disclosure increases
- Pervasive computing has generated a number of devices to assist with mobility
  - – Predicted by IDC 2005 Worldwide Handheld QView Report:
    - Small highly portable (read pocket-sized or smaller) storage devices will grow from 18 million in 2004 to <u>over 100 million</u> in 2008 (CSI Alert, Herold, March 2006, p. 5).

Portable/Removable Media

- USB pen drives (thumb drives, flash drives, etc.)
- CDs and DVDs
- Floppy Disks
- Laptops

CSI Alert March 2006

Storage Device Facts (Herold, 2006, p. 5)

- USB pen drives and flash drives
  - Easy to conceal – look like pens
  - Easy to lose or steal
  - 16 GB or more of storage
- USB pocket-sized storage devices
  - 100 GB storage
- Cell phones
  - 100 GB storage soon
- MP3 and mobile video players
  - 100 GB storage

Portable/Removable Media

- PointSec survey
  - – 99% of mobile device users use no encryption to protect data (Herold, 2006, p. 6).
- The financial losses associated with the inadvertent disclosure of sensitive information can be staggering (Yu & Chiueh, 2004).

Human Threats

- With the proliferation of removable media devices
  - The battle of protecting sensitive information from employees within the organization has begun in earnest.
  - According to Millman (2004), “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” (p. 52).

Human Threats

- Insider Threats
  - **Information must be protected**
    - Personally identifiable information
    - Trade secrets
    - Intellectual property
    - Sensitive and confidential information
  - **Removable and portable media devices**
    - Deliberately or unintentionally introduce a virus or malicious code into network or individual computer
    - By-pass IDS and anti-virus protection safeguards
    - Easily remove massive amounts of data
    - Employee theft of sensitive data

Regulatory Compliance

- Requires that sensitive data:
  - Be adequately safeguarded from inadvertent disclosure
  - An audit trail is available (Milas, 2004).
- Laws requiring administrative, physical, and technical safeguards for compliance
  - California Senate Bill 1386 of 2002 (SB 1386)
  - Gramm-Leach-Bliley Act of 1999 (GLB)
  - Health Insurance and Portability Act (HIPAA)
  - Sarbanes-Oxley Act of 2002 (SOX)

HIPAA Compliance

- HIPAA Security Final Ruling dated February 20, 2003 Technical Safeguards (CMS, 2003):
  - **Protection of electronic patient health information (ePHI)**
  - **§164.312 (a)(1) Access Control & (a)(2)(iv) Encryption and Decryption (addressable)**
    - ISO 17799 10.3 Cryptographic Controls
    - ISO 17799 10.3.2 Encryption
  - **Authentication measures must be applied to ensure that data is protected from corruption**
    - Encryption is a feasible method to achieve this requirement

HIPAA Compliance

- **§164.312 (e)(1) Transmission Security & (e)(2)(ii) Encryption (addressable)**
  - ISO 17799 10.3 Cryptographic Controls
  - ISO 17799 10.3.2 Encryption
- **Transmissions Utilizing Removable Electronic Media**
  - If the transport of data is on removable electronic media such as a CD-ROM, floppy, memory card, magnetic tape drives, etc, the sender must verify the following:
    - The data is encrypted
    - The party that is receiving the data is authenticated
    - Only the minimal amount of electronic patient health information (ePHI) necessary to accomplish the task is included

HIPAA Compliance

- **HIPAA penalties for such disclosure**
  - Civil penalties
    - $100 per person for violating transaction standards
    - Up to $25,000 per person per violation
  - Criminal penalties
    - From $50,000 up to in excess of $250,000 per incident
    - Plus, prison time from one to ten years for the sale of ePHI (The HIPAA Academy, 2003).
- Thus, the stakes are high in the event that sensitive data is compromised.

Encryption Solutions

- Insider Threat and Mobile Workforce Security Solutions
  - **Encryption of sensitive data at rest on computers**
    - Encrypts/decrypts hard drive
    - Difficult for the curious or malicious unauthorized user to access information
    - Laptops lost or stolen would not reveal highly confidential information
  - **Removable media encryption**
    - Removable media encryption/authentication software
      - Log created in a database to monitor documents downloaded
    - CDs, floppy disks, USB flash drives – must be authorized and authenticated prior to downloading information

Key Features of Removable Media Encryption

- Encryption of data
- Strong passwords enforced
  - How many/what type of characters will be required for the strong password
  - Conformity to company policies
- Authentication of device
- Authorization of removable media on network
- Alerts
- Auditing logs available with the software

Authentication

- Profile approach to creating user permissions
  - Roles are created with corresponding access rights
  - Match those on the domain controller
  - Incorporated by a number of encryption software products
  - Guest account creation that grants standardized rights for all guests

Authentication

- Administrator override of the user’s password for unlocking the encrypted device
  - In the event that a password is compromised
  - If an employee is terminated
  - This flexibility allows for the immediate denial of access to a terminated employee or the resetting of a forgotten password.
- This is also an appropriate and necessary regulatory compliance requirement

Authorization for Removable Media

- Authorize and Review Contents
  - Prior to allowing access to the organization’s computer and/or network
  - If there are any unwanted or unsafe file types on the removable media:
    - Fail authorization
    - Not provide access to any of the removable media files on the removable media device

Authorization for Removable Media

- **In the event that there are legitimate files on the removable media files and a rogue executable is also downloaded on it:**
  - Must be an option available to browse the media
  - Ability to delete this executable so that authorization will be granted
- **Enforcement of a virus scan** of the device using the anti-virus scanning software available on the computer
  - This provides another defense against the inadvertent perpetuation of viruses on the network.

Removable Media Software

1. DeviceLock® – http://www.protect-me.com/dl/
2. PointSec® Media Encryption – http://www.pointsec.com/products/removablemedia/
3. SecureWave Sanctuary Device Control – http://www.securewave.com/sanctuary_DC.jsp
4. Reflex Magnetics Disknet Pro – http://www.Reflex Magnetics.com/products/disknetpro/
5. True Crypt – Open source on the fly encryption – http://www.truecrypt.org/

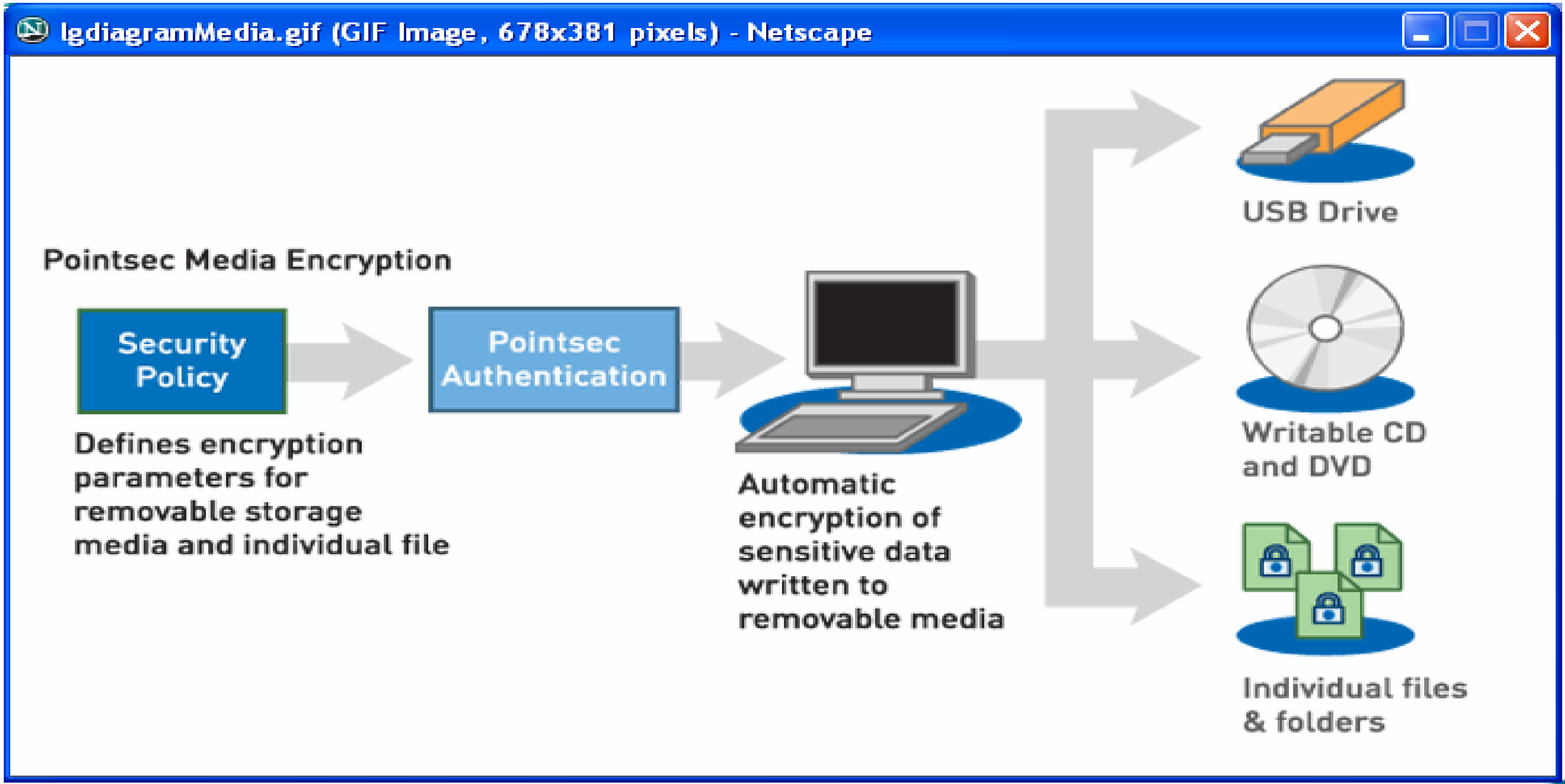
DeviceLock®

- Russian company
- Device auditing
  - Records download/upload activity
  - Customizable reports in Excel
- Group policy and Active Directory integration
  - Generate a report showing permissions
- Lock out plug-n-play devices
  - White list authorization available

Pointsec Media Encryption

- North American headquarters are located in Lisle, Illinois (outside Chicago).
- European headquarters are in Stockholm, Sweden.
- Transparent encryption
- Administrator controls
  - What information must be encrypted
  - Password length and strength
  - Maximum number of failed authentication attempts

Pointsec Media Encryption



lgdiagramMedia.gif (GIF Image, 678x381 pixels) - Netscape

Pointsec Media Encryption

Security Policy → Pointsec Authentication →

Defines encryption parameters for removable storage media and individual file

Automatic encryption of sensitive data written to removable media

USB Drive

Writable CD and DVD

Individual files & folders

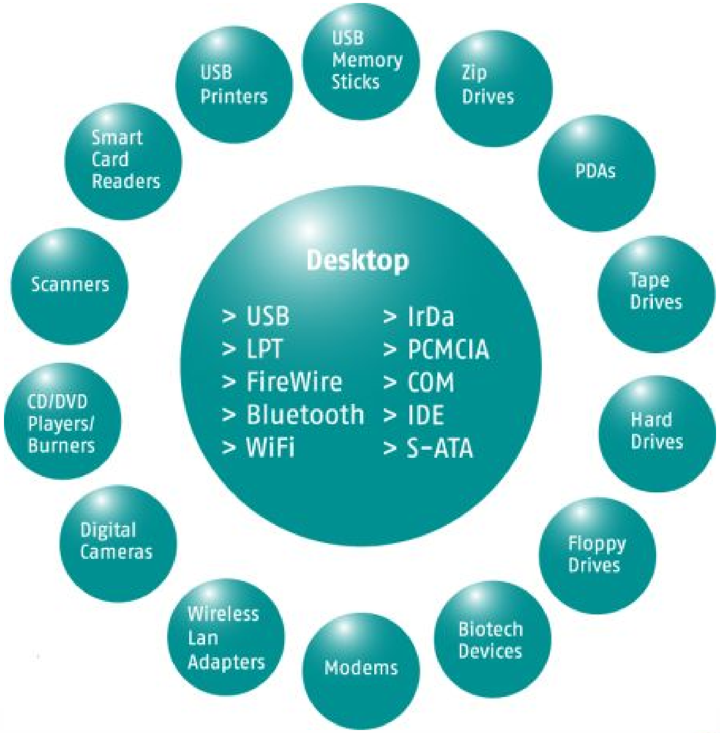
http://www.pointsec.com/products/removablemedia/

SecureWave Sanctuary Device Control

- Lock out all plug-n-play devices by default
  - White list authorization available
  - Uses Access Control Lists (ACLs) for authorization
- Provides an audit log
  - Allowed or attempted access with removable media
  - Assists with proof of compliance
- Maps to Active Directory and eDirectory objects

SecureWave Sanctuary Device Control

- Sanctuary controls the use of a huge range of devices that are key sources of security breaches
- Managed according to their type
  - – not on how they are connected



http://www.securewave.com/sanctuary_DC.jsp

Reflex Magnetics' Disknet Pro

- London-based company
- On the market since 1991
- Commercially available in the United States in 1994
  - James Shaeffer & Associates vendor in Ann Arbor
- Enforces encryption of data on removable media
  - Helpful if an employee wants to take sensitive data home to work on
  - If they lose the removable media, the data is safe because of the AES encryption

Reflex Magnetics' Disknet Pro Software

- Allows the system administrator to:
  - set permissions for each individual or user group
  - using its profile driven approach
- These profile templates
  - integrate seamlessly with existing domain users and group structure
  - management overhead is kept to a minimum.
- Whenever an employee plugs in a USB flash drive into a company computer before access is granted:
  - the device must first be authorized – content checked and digitally tagged

Reflex Magnetics' Disknet Pro

- **Once authorized, any files copied to the device are fully audited and stored centrally in a MYSQL database**
  - This filtered approach to auditing
    - Cuts down on unwanted traffic
    - Ensures that administrators can query the logs that have been obtained
    - Alerts are sent to IT administrators
- **These audit logs include**
  - What document was copied
  - Date
  - Time
  - Username

Program Security Guard (PSG)

- Disknet Pro feature
  - Allows the administrator to block the importing, deletion, or creation of certain file types
  - Capacity to create a customized exemption list so that company specified *trusted applications* are allowed access

Reflex Magnetics' Disknet Pro

- Writes an authorization tag for removable media devices to only work in organization's environment
- Digital tag will stay authorized until taken outside of the Disknet Pro environment
  - Checks for offline revisions
  - Will have to reauthorize the file when it comes back into network from home
- Have a way to revoke authorization of the whole corporation to get a number of memory sticks reauthorized
  - Important when terminating an employee

True Crypt

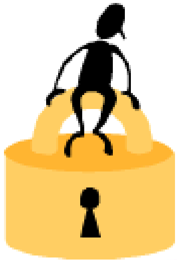
- Free ware
- Open-Source disk encryption
- Allows a duress partition with false information encrypted
- Windows and Linux
- On-the-fly encryption of USB flash drives
- Personal-class encryption tool
- Does not have enterprise class features
  - Auditing
  - Alerts

	AUDIT LOGS	ALERTS	AUTHORIZATION/ AUTHENTICATION OF DEVICE	ENCRYPTION OF DATA	ENFORCE STRONG PASSWORDS
DeviceLock®	√	Unknown	√ Set permissions at device type level, port level and individual device level	√	Unknown
PointSec® Media Encryption	Unknown	Unknown	Unknown	√	√
Reflex Magnetics Disknet Pro	√ Fully configurable filters and audit analysis reports; stored in an MS SQL database;	√ Configurable email alerts	√ Set permissions by type, brand, or model - Supports both blacklists and whitelists	√ Enforceable device encryption utilizing AES 128/256 bit algorithm EPM Explorer enables secure offline access of encrypted devices without the need to install software	√
SecureWave Sanctuary Device Control	√ Shadowing option to copy files or just filenames	Unknown	√ By default access denied. Must be authorized using ACLs	√	Unknown
True Crypt	None	None	√	√	√

	SYSTEM REQUIREMENTS	GROUP POLICY	SUPPORTS LOCKING
DeviceLock®	Windows NT/ 2000/XP or Windows Server 2003	Microsoft Active Directory Microsoft Management Console (MMC)	Floppies, CD-ROMs/DVDs, Any removable storage, Hard drives, Tape drives, WiFi Adapters, and Bluetooth adapters
PointSec® Media Encryption	Windows 2000/XP	Unknown	USB/USB2/PCCARD, Firewire memory cards, Storage media, and Floppies
Reflex Magnetics Disknet Pro	- Microsoft SQL Server or MSDE - Microsoft Windows 2000/XP Professional/ Server 2003 - Novell - Linux	Microsoft Active Directory Microsoft Management Console (MMC) Novell e-Directory Linux	Apple Ipods, Floppies, CD-ROMs/DVDs, Any removable storage Hard drives, Tape drives, WiFi Adapters, and Bluetooth adapters
SecureWave Sanctuary Device Control	- Microsoft SQL Server or MSDE - Microsoft Windows 2000/XP Professional/ Server 2003 - Novell	Microsoft Active Directory Novell e-Directory	USB Memory Sticks, Tape/Hard/Zip Drives, Floppies, PDAs, CD/DVDs, and Smart Card Readers
True Crypt	- Windows XP/ 2000/2003/Vista - Linux	Unknown	USB hard disks, floppy disks, USB memory sticks, and other types of storage devices.

Security Policies/Training

- How many people have:
  - – Security policies for portable and/or removable computing devices?
    - Is encryption required?
  - – Training on how to use and safeguard removable and/or portable media?



ePHI Security Policy Example

- **To ensure access to ePHI data is limited to only authorized users, the following policies shall be adopted:**
  - All mobile computer devices shall have the capability to encrypt sensitive hospital related files.
  - No ePHI files may be loaded onto mobile computers or removable media devices without the data being encrypted.
  - All laptop computers shall have encryption software that will authenticate and authorize users to allow access to the computer’s hard drive.
  - No ePHI data may be removed from the hospital without formal application to do so.
  - A mobile data information form must be filed with the IS security office before the data is taken out of the hospital.
  - Data on mobile systems may not be copied onto other media for any purpose.

Conclusion

- As more employees embrace removable media devices:
  - it is critical that employers guard against the removal of
    - company trade secrets
    - intellectual property
    - personally identifiable information
    - sensitive data from walking out the door.
- There are also legitimate business purposes for taking files home or on the road.
- Therefore, there must be a balance between
  - allowing employees to do their job successfully
  - preventing the theft or unintentional loss of data.

Next Steps

look, plan, act, repeat

Questions?

Thank You!

Contact Information

Faith M. Heikkila

Information Security Consultant

Pivot Group - **look**, **plan**, **act**, **repeat**

O: 269-353-7537

C: 616-430-8056

E: fheikkila@pivotgroup.net

W: www.pivotgroup.net

References

- Centers for Medicare & Medicaid Services – CMS. (2003, February 20). HIPAA administrative simplification – security: Final rule. *Federal Register, 68*(34), 8334-8381.
- Herold, R. (2006, March). Lexus laptop lockers. *Computer Security Institute Alert*, 5-6.
- Milas, B. (2004, October). ID mapping: The compliance key. *SC Magazine,* 74.
- Millman, R. (2004, October). Product reviews: DiskNet Pro 4. *SC Magazine*, 52.
- The HIPAA Academy. (2003). HIPAA penalties. *HIPAAAcademy.net.* Retrieved November 25, 2004, from http://www.hipaaacademy.net/hipaaPenalties.html.
- Yu, Y. & Chiueh, T-C. (2004, October 25). Display-only file server: A solution against information theft due to insider attack. *Proceedings of the 4th ACM Workshop on Digital Rights Management, Washington, D.C.,* 31-39.