Mobile Encryption

by
Rick Smith rdsmith@mac.com
Rick Wanner rwanner@pobox.com

Group Discussion and Project
CDI East 2006

Table of Contents

List of Tables

Executive Summary

Due to the recently reported theft of a laptop containing sensitive data on 800,000 former employees' records, an encryption solution for all mobile devices is needed to protect the confidentiality of personally identifiable information and business sensitive data. Although the recent theft involved a laptop, consideration should be given to the fact that data mobility is not just a laptop problem, PDA's and smartphones and removable media must be considered as well.

Market research was performed evaluating technologies in the various encryption product classes including full-disk encryption, hardware-based disk encryption, virtual disk encryption, and file encryption. Based on this analysis it was determined a full-disk encryption solution is most appropriate.

Before performing a more in-depth review of the full-disk encryption technologies available, criteria were formulated with the critical criteria being industry standard encryption, minimal impact on users and operations staff, and strong key management and recovery capabilities as well as other criteria.

Based on those criteria two product suites are deemed to be the best fit. These suites of products are from SafeBoot Corporation and from PointSec Mobile Technology.

The next steps should be to perform a detailed technical evaluation of these two products including a limited trial to determine the suitability of these products in our environment. Further details are in the Project Planning section.

Background

Due to the recently reported theft of a laptop containing sensitive data on 800,000 former employees' records, an encryption solution for all mobile devices is needed to protect the confidentiality of personally identifiable information and business sensitive data. Although the recent theft involved a laptop, consideration should be given to the fact that data mobility is not just a laptop problem. Data is becoming increasingly mobile on handheld devices, such as PDA's and smartphones as well as removable media such as USB devices. Any solution should consider these aspects as well.

User and management considerations must also be considered. Of utmost importance is that the solution has minimal impact on users and not be overly burdensome on operational or helpdesk personnel. Also important is the ability to recover encrypted files in the case when an employee leaves the company, and to be able to reset the user's password when it is forgotten, preferably with minimal impact to help desk services.

In addition to the requirements above, records storage requirements dictate the data must be recoverable for at least five years. For most encryption schemes, this is a requirement for key management or key escrow and password recovery features.

Operating Environment

Our company standard operating environment is Microsoft Windows centric. The Windows Server 2003 Active Directory is the basis of the network authentication for both computers and users. Group Policy Objects are used to push software and updates to the domain. The exception is the Cisco firewalls and routers. The standard hardware and software for company computers are listed in Table 1.

Platform Type	Hardware	Operating System
Servers	Dell PowerEdge 2850	Windows Server 2003
Desktops	Dell Optiplex GX620	Windows XP SP2
Laptops	Dell Latitude 600 series	Windows XP SP2
Handhelds	Cingular 8125 Pocket PC	Windows Mobile 5.0

Table 1: Operating Environment

Encryption Technologies

Encryption technologies generally fall into the following categories:

- Full-disk encryption
- Hardware-based disk encryption
- Virtual Disk encryption
- File Encryption

Full-disk encryption is software based technology that encrypts and decrypts as required as the disk is read or written. This is a fairly mature technology which supports a number of authentication methods and provides mature capabilities for key management and recovery. The major disadvantage is that since this is a software based solution CPU cycles are required to perform the encryption and decryption. Some products in this space are SafeBoot[1], PointSec[2], Encryption Plus Hard Disk[3] and PGP Whole Disk Encryption[4]. Microsoft has also committed to support full disk encryption in BitLocker which is integrated into Windows Vista[5].

Hardware-based disk encryption is similar to full-disk encryption except the encryption is integrated directly into the disk hardware. The principal advantage of this is speed. CPU cycles are not required to encrypt and decrypt data as it is accessed. The main disadvantage is that this is a relatively young technology and does not have the maturity of the full-disk products. At this time only passwords are

[1] http://www.safeboot.com/products/devicesecurity.html
[2] http://www.pointsec.com/
[3] http://www.tryten.com/products/Wcc27dada7d81b.htm
[4] http://www.pgp.com/products/wholediskencryption/index.html
[5] http://technet.microsoft.com/en-us/windowsvista/aa906018.aspx

available as an authentication mechanism and the key management and key recovery capabilities of this technology are limited. At this point only SeaGate[6] has made a commitment to this technology although other drive manufacturers are likely to follow.

Virtual disk encryption and file encryption both utilize the concept of setting aside portions of the disk for encrypted files. For virtual disk encryption generally the encrypted area will appear as a drive letter on the system. For file encryption technologies it can be an individual file or a folder on the system. All data read from or written to these areas will be encrypted or decrypted as required. The advantages are that this is a mature technology which supports a number of authentication methods. The major disadvantage is that because only selected parts of the disk are encrypted this technology relies on the user to place sensitive data in the encrypted areas. Also, temporary files created by applications will not be encrypted if they are not placed in the encrypted areas. Products in virtual disk encryption space are PGP Virtual Disk[7] and TrueCrypt[8]. The major player in the file encryption space is Microsoft's Encrypting File System (EFS) which is built into Windows XP and Windows Server 2000 and 2003.

Due to the limitations of some of these technologies, it is felt that the only viable solution at this point in time is a full-disk encryption product.

Product Assessment

The goal of the assessment is to find a pair of best-in-class full-disk encryption products for further evaluation. The following criteria were used to compare the products:

- Operating systems supported – supports all operating systems in the operating environment.
- Ease of Deployment – easy to install, minimal training required.
- Transparent to User – minimal user training required.
- Centralized Management – management from a central console.
- Ease of Management – intuitive interface, easy to use.
- Strength of Encryption – industry accepted encryption standard.
- Key Management and Recovery – easy to recover encrypted files and change password if required.
- Audit logging – detailed logging of success and failure.
- Cost – price point

The critical criteria being support for strong encryption and the ability to manage the keys easily and easily recover files when required.

[6] http://www.seagate.com/cda/newsinfo/newsroom/releases/article/0,1539,3347,00.html
[7] http://www.pgp.com/products/desktop_home/index.html
[8] http://www.truecrypt.org/

Preliminary research was performed utilizing the Gartner Magic Quadrant for Mobile Data Protection, and reviews of mobile encryption products in Network Computing and SC Magazine.

A number of products met the basic requirements, but in the areas of key management/recovery and centralized management two products rose to the top.

The first is SafeBoot Device Encryption from SafeBoot Corporation. The second is two related tools PointSec for PC and PointSec for PocketPC from PointSec Mobile Technologies. Both solutions are a centrally managed suite of tools that provide encryption for mobile devices including the Windows-based laptops, Windows Mobile-based handhelds, and removable media.

Safeboot

SafeBoot Device Encryption is a suite of software tools for securing mobile data. In this case the required products are *SafeBoot Device Encryption for PC / Laptop*[9] and *SafeBoot Device Encryption for Windows Mobile*[10] and *SafeBoot for USB*[11].

Also required is the SafeBoot Management Appliance which deploys the *SafeBoot Management Centre*[12] software. This solution provides centralized management and administration of all deployed solutions.

The SafeBoot Management Centre integrates the individual products permitting seamless management of all aspects of the deployment including centralized policy creation and enforcement, identity management, asset management, remote upgrades, credential revocation, and auditing and logging.

SafeBoot supports a number of user authentication methods including Active Directory, LDAP, and Entrust PKI.

The SafeBoot Management Centre also provides a web based administration interface to enable helpdesk personnel to perform password recovery or password resets via a challenge/response procedure. This same web-based administration interface permits user self-service, permitting the user to recover or reset their password via a standard web-browser.

PointSec

[9] http://www.safeboot.com/products/device-encryption/pc/
[10] http://www.safeboot.com/products/device-encryption/windows/
[11] http://www.safeboot.com/products/usb/
[12] http://www.safeboot.com/products/management.html

Similar in architecture to SafeBoot, the PointSec Mobile Technology solutions are a suite of products including *PointSec for PC*[13] and *PointSec for PocketPC*[14] and *PointSec Media Encryption*[15].

For management PointSec utilizes PointSec MI (Management Infrastructure) and webRH (web Remote Help)[16].

PointSec MI provides integration of the individual products permitting management of all aspects of the deployment including centralized policy creation and enforcement, identity management, remote upgrades, credential revocation, and auditing and logging.

PointSec supports a number of user authentication methods including Active Directory, LDAP, and dual-factor authentication tokens.

The PointSec webRH provides a web based administration interface to enable helpdesk personnel to perform password recovery or password resets via a challenge/response procedure.

Other Considerations

There is no reason why deployment of an encryption technology need be limited to only mobile devices. Both recommended technologies can also be extended to deployment on desktops and servers thus reducing the risk of theft of these devices.

Project Plan

The following is a proposed Software Development Lifecycle for this solution.

1. Project planning:
    a. Determine the need for an encryption scheme for mobile devices.
        i. What problem are we solving with this solution?
            1. Protecting the confidentiality for data at rest on mobile devices.
            2. Mitigate the possible legal implications of losing personally identifiable information.
            3. Mitigate the impact of loss of devices business sensitive data.
        ii. What mobile devices are you concerned about protecting the data on?
            1. Mobile devices:
                a. Laptops

[13] http://www.pointsec.com/products/pc/
[14] http://www.pointsec.com/products/smartphonepda/
[15] http://www.pointsec.com/_file/Removable_Media_Data_Sheet.pdf
[16] http://www.pointsec.com/products/managementtools/

b. Handhelds: Smartphones, Pocket PCs, PDAs

2. Removable media (CDs/DVDs, flash drives, external hard drives, etc.)

3. Plan for some degree of excess capacity, both in software licenses and in management server hardware. As you demonstrate the value of the solution you can expect to receive additional tasking to take logs from additional devices not on today’s roadmap.

iii. Should deployment include desktops and servers?

iv. Which business areas are you going to protect the data from?

1. Initially, Human Resources and Financial, then move to all company laptops, then removable media and, potentially, all desktop hard drives.

2. Plan for some excess capacity or the ability to add capacity easily, you can expect to gain additional users you have not planned for in the initial design.

b. Determine the financial viability of a data encryption solution

i. Software or appliance costs

1. Central management server or appliance

2. Per-seat license costs for each type (hard drive, handhelds, removable media, virtual disk, etc.) of encryption (if licensed per-seat)

3. Database Server software (if required)

4. Software needed to manage the systems (if required)

ii. Hardware costs

1. Servers to run the management console (unless deploying an appliance solution)

2. Storage (Local Disk, SAN, or NAS) (if required)

3. BCP hardware or hardware for a high-availability configuration (if required)

4. System management hardware (i.e., tape backup, monitoring, hardware management, etc., if required)

5. Any local costs relating to Data Center space

iii. Customization costs

1. Discuss with the encryption software vendors the feasibility and any costs associated with changes you may require to be made to the product.

2. Determine the complexity, cost and lead times for any customization of user installation packages required.

iv. Maintenance costs

1. Hardware annual maintenance

2. Software annual maintenance costs

v. Staffing costs

1. Sysadmins’ salary

a. Who will do the system administration for your management console systems?

2. Database Administrator

a. Do you require a DBA (on a full or part time basis)?

b. Can you split the salary cost between internal groups/projects?

3. SAN Administrator
   a. Do you require the services of a Storage Area Network admin (on a full or part time basis)?
   b. Can you split the salary cost between internal groups/projects?
4. Help Desk Support
   a. Will the help desk personnel need training on assisting user with the encryption product?
   b. Will additional help desk staff be required?

c. If an enterprise asset inventory system does not exist already, start the effort to build that infrastructure 6 months prior to starting the encryption scheme implementation. You will want accurate asset information to maximize the coverage.

d. Determine if an enterprise Identity management solution exists and if you can leverage this for mapping user identities, both for mapping IDs to users and keys/password during deployment and later when key recovery/password reset issues arise.

e. NTP – if you are not using it, start! Accurate system times may have an impact on the ability to recover keys/reset passwords.

f. Evaluate the encryption products; try hard to talk with actual users of the products you are considering, preferably without the vendor present.

i. Determine the anticipated usage scenarios (laptop, handheld, and removable for an encryption solution.

ii. Determine hardware devices supported

iii. Determine types of encryption supported from encryption vendors, e.g., whole disk and virtual disk.

iv. Ease of installation of management software

v. Ease of use of management software

vi. Ease of installation of the encryption software on the mobile devices

vii. End user experience

1. Effects on device performance
2. Effects on device start-up/user logon
3. User Interface issues

viii. Complexity of recovering from lost or forgotten passwords or keys

1. Remote password/key recovery

ix. Ability to integrate into existing authentication or identity management solutions, e.g., Active Directory, SSO, tokens

x. Responsiveness of vendor in addressing problems reported

2. Systems analysis:

a. Determine the number of and type of volume of devices you need to be able to accommodate.

i. Laptops

1. Manufacturer and model
2. OS
3. Hard drive capacity, speed, age
4. Processor speed
5. Memory capacity

ii. Handhelds

1. Manufacturer and model
2. OS
3. Processor speed
4. Memory capacity
5. Memory card slot capability

iii. Removable media

1. External hard drives
2. Flash drives

b. Determine the key recovery/password retention requirements (how long do you need to be able to decrypt the data for)?

i. Does there exist for your organization, any regulatory mandate to store or destroy data?

ii. How long do you need to have online and

iii. How long in offline (restorable) log data.

iv. Do you need to replicate database data

v. Do you need to store raw unmodified log data? If so for how long?

c. Determine how many users the system will need to support

i. How many users will need to author content

ii. How many users will be consumers of content only

d. Determine BCP/DR requirements for the encryption software.

e. Does the encryption solution allow use of external user authentication (via Active Directory, SSO, or Token) ?

i. What mechanisms are supported?

ii. What needs to be done for the authentication system to work with the encryption solution?

3. Systems design:

a. Hardware Requirements (unless an appliance solution is being deployed)

i. Determine the hardware requirements for encryption suite manager servers

b. Design the encryption suite management architecture

i. Determine the number of management servers required to support the volume of logs

ii. Determine the number of management servers required to support any organizational separation of functions (Line of Business or geographical region)

iii. Try to architect the encryption suite management environment in tiers to enhance overall scalability.

iv. Validate the encryption suite management server hardware and architecture design with the vendor to avoid any problems later relating to scalability or performance. Ask the vendor to provide a capacity plan that you can use as a scalability roadmap.

c. Design encryption suite management server network connectivity

d. Train the IT support staff team to deploy the encryption suite on the mobile devices product

4. Implementation:

a. Order, Receive, and Rack server hardware

b. Install selected Operating System

i. Configure to local standards.
ii. Patch OS to current levels.
c. Connect and configure network
i. Assign IP addresses
ii. Connect network
iii. Test connectivity
iv. Test any network related high availability features
v. Configure any SAN connectivity (if required)
d. Install encryption suite management software or deploy the appliance
i. Load DB (unless installed by management software setup)
1. Load any DB high availability solution (DataGuard, RAC, etc.)
2. Test any database high availability features
ii. Load encryption suite management software
iii. Basic management software configuration
e. Design and Implement access controls on user groups to restrict the users’ right in the encryption suite
f. Draft and issue policy documenting the requirements for data encryption scheme including all types of mobile devices

5. Integration and testing:
a. Install and configure the encryption suite products on the appropriate devices
i. Create the appropriate installation packages (if required)
b. Validate the packages install with the correct configuration
c. Validate the data is encrypted
d. Measure the encryption software impact on device performance by comparing against non-encrypted device
e. Test key recovery/password reset functionality for all different encryption suite products
f. Test the to transfer information between devices
g. Test auditing functionality

6. Acceptance, Deployment:
a. Provide access to test user community
b. Build production accounts for user community
i. Build accounts with appropriate rights
ii. Disseminate user accounts and software
c. Training of End Users, help desk, IT support and SOC personnel in the encryption suite operation for their position
d. Perform a staged installation of the encryption suite components on mobile devices to the various business areas
e. Integrate into the CSIRT/Incident Handling process
f. Integrate into the IT support processes
i. Help Desk support
ii. User device build and configuration
g. Educate internal groups on capabilities and limitations of the encryption suite, this can include Audit, Management, and especially Legal.

7. Maintenance:
a. Design a process for patching the OS on the encryption suite management servers
b. Design a process for patching the encryption suite application

c. Design a process for patching the encryption suite database software
d. Design a process to archive or escrow the encryption suite administrator keys/passwords
e. Design and document a process to recover archived encrypted data for later analysis or legal requirements.
f. Design a process for managing user accounts in the encryption suite if not integrated with existing authentication methods, including creation, deletion, and password reset/unlock
g. Ongoing training efforts for Administrative and Operations staff
h. Create a "lessons learned" feedback loop to allow processes involving the encryption suite to be improved based on help desk support calls and, if applicable, the incident handling process.
i. Anticipate the need for new data encryption requirements, or upgrades to current ones, as additional hardware devices are introduced into the environment.

References

PGP Corporation, PGP Whole Disk Encryption Data Sheet. Retrieved December 8, 2006, from PGP Whole Disk Encryption Web site: http://www.pgp.com/products/wholediskencryption/index.html

Loh, V (2006, October 30). Step Up Hard Drive Protection. Retrieved December 8, 2006, from eweek.com Web site: http://www.eweek.com/article2/0,1895,2047965,00.asp

Wabiszczewicz , T (2006, November 9). Full-Disk Encryption Suites - Security. Retrieved December 9, 2006, from Network Computing Web site: http://www.networkcomputing.com/article/printFullArticle.jhtml?articleID=193500189

Clarke, R (2006, August 7). Missing laptop, missing policy. Retrieved December 9, 2006, from SC Magazine Web site: http://www.scmagazine.com/us/news/article/576108/missing-laptop-missing-policy/

Brandt, A (2006, November 6). Review: Disc Encryption Products for your laptop. Retrieved December 9, 2006, from Computerworld Web site: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004881

Tullet, J (2005). Mobile Data Encryption. Retrieved December 9, 2006, from SC Magazine Web site: http://www.scmagazine.com/us/grouptest/details/3a035d3b-d088-412b-89f6-44f6a63892fe/mobile-data-encryption-2005/

Stephenson, P (2005). Mobile Encryption, Part II. Retrieved December 9, 2006, from SC Magazine Web site: http://www.scmagazine.com/us/grouptest/details/0d550b6c-c738-db7b-9537-a2d51006e8ef/mobile-encryption-part-ii-2005

Girard, J Wagner, R Wheatman, V (2006, Aug 29). Magic Quadrant for Mobile Data Protection. Retrieved December 9, 2006, from Pointsec Mobile security Web site: http://www.pointsec.com/downloads/resources/index.cfm

Allen, M How to kick start a mobile security project. Retrieved December 9, 2006, from Pointsec Mobile security Web site: http://www.pointsec.com/_file/How-to-kick-start-a-mobile-security-project.pdf

PointSec Mobile Security, PointSec for PC Data Sheet. Retrieved December 9, 2006, from PointSec Mobile security Web site: http://www.pointsec.com/_file/Pointsec_for_PC_LTR_ENG_Nov9-06.pdf

PointSec Mobile Security, PointSec webRH Data Sheet. Retrieved December 9, 2006, from PointSec Mobile security Web site: http://www.pointsec.com/_file/Pointsec_webRH_MP_LTR_ENG_72dpi.pdf

Safeboot Corporation, Safeboot - Join millions on the road to hassle free data encryption. Retrieved December 9, 2006, from SafeBoot Corporation Web site: http://www.safeboot.com/products/device-encryption/