Full Disk Encryption

Protection for Your System

February, 2010

Prepared by:
Farhan Badshah

Electrosoft

11417 Sunset Hills Road, Suite 228
Reston, VA – 20190
Tel: (703)-437-9451 Fax: (703) 437 -9452
http://www.electrosoft-inc.com

Introduction

On June 23, 2006, the Office of Management and Budget (OMB) released a memorandum on the Protection of Sensitive Agency Information as guidance to provide safeguards to protect remote information systems. Clay Johnson, the Deputy Director of OMB, made a recommendation on the protection of these systems, stating:

"Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."

Today, mobile devices are becoming an integral part of many organizations' daily operations. These devices sometimes hold sensitive data and are usually insufficiently secured from unauthorized access.

This brings us to the main question: What technology is available today to protect the information stored on mobile devices?

The answer lies in Full Disk Encryption (FDE).

Full Disk Encryption

FDE, also known as "Whole Disk Encryption" utilizes hardware and/or software components to encrypt stored data.

FDE provides the following benefits:

- Potential to encrypt every bit of data – this includes paging files and temporary data files
- Easy to use – does not require user's discretion on what files need to be encrypted
- Support for pre-boot authentication – provides access control and prevents unauthorized users from gaining access to encrypted data
- Data can be wiped instantly – system is cleansed of data when the latter is no longer needed

There are also concerns that arise when dealing with FDE solutions because it encrypts the hard drive as a whole. A problem that may arise with this solution is if an attacker can gain access at run-time, then he has access to the entire hard drive.

To combat this issue, FDE has software with features capable of encrypting not only at the hard drive level, but at the file level. This is known as providing encryption through *Layering*.

Layering

FDE can provide encryption at various levels, either separately or simultaneously. Layering can occur at the following levels:

- Disk partitions can be encrypted – an example of this is would be the C Drive in the Windows Operating System.
- Specific files can be encrypted – If the hard drive is encrypted, and an attacker gains access at the hard

drive level, the attacker will have to go through another layer to access specific files that are encrypted.

- Page files can be encrypted – page files (also known as swap space in Linux) reside on the hard drive and function as additional Random Access Memory (RAM).
- The hibernation file can also be encrypted – hibernation mode skips the initial start up process and resumes back to the state of the system it was last in. With this file encrypted, users will receive a login prompt before they can access the system.

Trusted Platform Module

Some FDE solutions leverage the use of a Trusted Platform Module (TPM). A TPM is a processing chip embedded on the motherboard of mobile devices that can perform cryptographic functions.

It also provides capabilities such as remote attestation. Remote attestation creates a hash key summary for software configuration. The hash summary key is decided by the program encrypting the data. Doing this allows third party vendors and other FDE solutions to verify that the software has not been changed.

Additionally, TPM is capable of performing platform authentication (e.g. Microsoft Windows Bit Locker) and can be used to store the encryption and decryption keys in the hardware.

Below is an example of how TPM performs platform authentication:

A laptop contains an internal hard drive which is encrypted using Microsoft Windows Bit Locker and the hard drive becomes unique to that particular machine. Since TPM contains cryptographic keys, it also stores the decryption key, thus tying the hard drive to the chip.
TPM can verify that the hard drive in the laptop seeking access is the expected system. Therefore, if the hard drive was removed from the laptop and swapped into another machine, the hard drive would be unable to decrypt because the TPM is not present to authenticate that device.

A major concern with TPM is that it can potentially be a single point of failure. Damage to the TPM can prevent recovery of the encrypted data on the hard drive, especially if the decryption key is stored in the TPM.

Hardware and Software Tools

FDE can come in the form of a hardware solution, a software solution, or a combination of hardware and software.

Since 2006, many of the new laptop machines have shipped with a built-in TPM chip on the motherboard. In future, there are plans to deploy built-in TPM chips in other mobile

devices, such as cell-phones and PDA's.

The hardware tools are significantly faster and produce no overhead for the CPU and hard drive. These types of tools contain pre-boot authentication and a BIOS password for basic access control.

Other examples of hardware FDE tools include external hard drives and flash drives with built-in encryption mechanisms. Hardware based FDE solutions are more appropriate for smaller organizations. For example, implementing password recovery mechanisms is easier with smaller companies because of fewer costs associated with help desk operatives. In these types of environments, the user is responsible for protecting their own data and not having to rely on support.

Software-based FDE solutions are more commonly used than hardware based tools. Enterprises and major corporations tend to leverage the use of software-based solutions since they can be centrally-managed, provide more features, and offer flexibility with network integration.

Recovery Mechanisms

Encrypting your hard drive data with the use of cryptographic keys is an essential security safeguard. But what if the decryption key is corrupted or lost? Password recovery mechanisms play a critical role in these types of situations. For example, a user may have forgotten his or her recovery password or may have left the company. How can the data be recovered?

When deploying FDE solutions on a large scale, the solution must provide an easy and secure way to recover encrypted data. For example, there may be times when an employee leaves the company without notice or forgets his or her password. In this case, a challenge/response password recovery mechanism allows the password to be recovered in a secure manner. There are a few FDE solutions that have this capability and using this recovery mechanism can provide the following benefits:

- Encryption keys are centrally managed – does not require the user to carry a disc with the encryption key
- Protection against disclosure of sensitive data – during the recovery process, sensitive data is not revealed to help desk personnel
- Offline flexibility – a network connection is not required for recovery, as long as the user can contact support via phone

Security Issues

FDE solutions provide greater security for your data, but there are some known issues to be aware of.

Most FDE solutions are vulnerable to a cold boot attack. This type of

attack occurs when encryption keys are stolen prior to booting into the operating system. From an attacker's perspective, here is how a cold boot attack would work:

1. The attacker would perform a soft-reboot of the system.
2. The attacker would reconfigure the boot device priority from the BIOS settings.
3. As the system is starting up, the attacker would insert a boot disk that runs an executable file to capture the decryption key.
4. After the executable file is finished running from the boot disk, the attacker would then analyze the data and identify the decryption key.
5. Once identified, the attacker would boot the system normally and use the decryption key to gain access to the system.

The counter-measure to this attack is to password protect the access to the BIOS settings of the system. This will prevent the attacker from changing the boot priority device, and more importantly, will decrease the chance of a cold boot attack from occurring.

GSA Approved Products

The following are examples of encryption products that provide FDE solutions that are approved by the GSA:

- Bit Armor Solutions
- GuardianEdge
- CheckPoint (PointSec)
- PGP

Success

It is important for enterprises to place an emphasis on security in order to protect their work and intellectual property, and FDE solutions can help. Whether it is hardware or a software solution, enterprises and small organizations must determine what the right solution is for them and implement it effectively to protect the data on their systems. With FDE, companies can easily manage and protect data. In addition, FDE is capable of securing data on the hard drive as well as the file system level. Other FDE solutions include pre-boot authentication and provides the capability of wiping out data instantly without having to go through the troubles of physically destroying the hard drive. Finally, FDE also provides an easy way to manage password and data recovery

What steps are you taking to protect your data? Does your organization implement FDE?

References

[1]http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

[2]https://www.gsaadvantage.gov/advgsa/advantage/main/start_page.do

[3]http://www.reuters.com/article/pressRelease/idUS123915+14-Oct-2009+BW20091014

[4]http://var.immixgroup.com/contracts/gsa70_pricing.cfm?client_id=110&contract=GS-35F-0330J

[5]http://en.wikipedia.org/wiki/Full_disk_encryption

[6]http://en.wikipedia.org/wiki/Trusted_Platform_Module

[7] http://www.microsoft.com/windows/windows-vista/features/bitlocker.aspx

[8] http://www.guardianedge.com/

[9] http://www.pgp.com/

[10] http://www.checkpoint.com/products/datasecurity/pc/