**ISSN** 1746-7659, England, UK
**Journal of Information and Computing Science**
Vol. 6, No. 3, 2011, *pp*. 163-172

# Full Disk Encryption based on Virtual Machine and Key Recovery Scheme

Min Liang [1, +], Chaowen Chang[1]

[1] Institute of Electronic Technology, Information Engineering University, Zhengzhou China

(*Received November 18, 2010, accepted December 20, 2010*)

**Abstract.** Full disk encryption is a good choice to solve the problem of information leakage. In this paper, a full disk encryption based on virtual machine is proposed for computers without TPM. The program to decrypt the operating system is stored in a USB device which is more secure than in hard disk together with confidential information. Its key recovery scheme is with the help of a smartcard which is used for enhancing security. The experiments, security analysis and comparison demonstrate the efficiency, security and advantage of the proposed scheme.

**Keywords:** Full Disk Encryption, Virtual Machine, Key Recovery, Smartcard

## 1. Introduction

Storage security is one of the important preconditions for information security and information leakage from the disk has been a serious problem. Encryption is often used in protecting information from modification and leakage, but it is not secure only encrypting the information itself. Full Disk Encryption (FDE) is an effective manner to protect the confidential information in the hard disk. It is widely used in governmental and military departments. FDE can encrypt all the data including the operating system files, temporary files and user's files. And Microsoft has provided Bitlocker Drive Encryption Technology but there are some limitations. FDE provides a comprehensive protection for the confidential information. However, there must be a program to decrypt the operating system files, if not, the system could not start. But it is not secure that the program and confidential data are stored together in hard disk. USB device is a good choice to store the program.

The security of cryptographic data is based on the key which is used to encrypt and decrypt data. The key should be stored in a safe place, but also should be convenient to use. The hardware token, such as smartcard, is a good solution. But there must be some methods to recover the key when the smartcard is lost or stolen, and maybe the key is damaged.

The secret is only accessed by limited users, who are based on the authorization, but not the position in organizations or something else. We call this private hierarchy. The key should be recovered by the authorized user, not by the system administrator or the administrative superior.

In this paper, we present full disk encryption based on virtual machine (VM) and its key recovery scheme based on Shamir's secret sharing scheme. In this scheme, we use smartcard to store user certificate and confidential information such as the privacy key. The program, XEN, is stored in a USB device instead of in the same place with confidential data. The key is stored nowhere and generated in the startup. The key can be recovered without the administrator knowing it, when the user lost his smartcard and USB device.

The roadmap of this paper is as follows. We present the related work in Section 2. A detailed review of Bitlocker is provided in Section 3. We present the full disk encryption based on XEN in Section 4 and the key recovery processes in Section 5. We make an evaluation in Section 6. We draw a conclusion in Section 7.

## 2. Related Work

Full disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a

[+] Corresponding author. Tel.: +86-0371-8163 8719.
*E-mail address*: lm7186345@163.com.

disk or disk volume. Full disk encryption prevents unauthorized access to data storage. There are multiple tools available in the market that allow for full disk encryption. They are divided into two main categories: hardware-based and software-based. The hardware-based full disk encryption solutions are considerably faster than the software-based solutions, but more expensive. Bitlocker is a software-based solution which is available in some editions of Windows.

Many kinds of key recovery scheme have been proposed in [1], [2], [3], [4], [5] and [6]. The main key recovery methods are key escrow, trusted third party, key backup and key encapsulation. Starting in 1993, the US government announced a new encryption technology call key escrow system [7]. Key escrow is an "all or nothing" proposition, with no mechanism to guarantee that the caretaker is doing the job honestly [8]. Most key recovery systems based on trusted third party aim to recover lost keys, support law enforcement for message investigation, and consider personal rights of privacy [9]. Key backup is a simple method which is used in Bitlocker. Key encapsulation is the only one in which the key is not known to the administrator [4, 6]. It is hard to confirm that the recovered key is the legitimate user's key. This means that the key can be recovered by a malicious user. The key with a certificate can resolve the problem, but the key would be known to the administrator in advance. Key recovery schemes using a smart card have been proposed in [10] and [11], but they are different from the one in this paper. Shamir secret sharing scheme is one of the key recovery solutions proposed by Shamir [12], also referred as (t, n)-threshold secret sharing scheme. In order to reconstruct the secret, one only obtains any t of the n shares. There is a scheme that integrates the (t, n)-threshold scheme into document archiving system to recover key [1].

There is a key recovery scheme which is used in FDE [11]. In that method the author uses a smartcard to store cryptographic object and makes use of a blind signature for both the generation of the disk encryption key and authentication. It can limit the recovered encryption key without informing the administrator. But the decryption program is stored together with the confidential data in hard disk, which is not secure.

## 3. Bitlocker

Bitlocker is a typical full volume encryption scheme. Bitlocker is available only in the Windows Server 2008, in the Enterprise and Ultimate editions of Windows Vista and in Windows 7. There are at least two NTFS-formatted volumes: one for the operating system and another called the system volume with a 1.5GB from which the operating system boots. Bitlocker requires the system volume to remain unencrypted. Bitlocker encrypts the entire Windows operating system volume on the hard disk [13]. Volumes other than the operating system volume and the system volume are called data volumes. Bitlocker encryption of data volumes is supported only in Windows Server 2008 [14]. So Bitlocker is not a strict sense of full disk encryption.

Bitlocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 which is installed in many newer computers by the computer manufacturers. The key used for disk encryption is sealed by TPM and will only be released to the OS loader code if the early boot files appear to be unmodified. But this mode is vulnerable to a cold boot attack, as it allows a powered-down machine to be booted by an attacker. In addition to the TPM, Bitlocker provides user authentication mode. This mode requires that the user provide some authentication to the pre-boot environment in the form of a pre-boot personal identification number (PIN) or inserting a USB flash drive that contains a startup key. This mode is vulnerable to a bootkit attack. However, there are still a large number of computer without TPM. On computers without TPM, Bitlocker encrypts the Windows operating system drive requiring the user to insert a USB startup key to start the computer or resume form hibernation, and it does not provide the pre-boot integrity verification offered by TPM. This mode is also vulnerable to a bootkit attack.

Furthermore, the key recovery of Bitlocker is simple and not secure. In Bitlocker, recovery consists of decrypting the volume master key using either a recovery key stored in the form of plaintext on a USB flash drive or a cryptographic key derived from a recovery password. The TPM is not involved in any recovery scenarios. The recovery password can be printed or saved to a file and the recovery key can be created and saved to a USB flash drive during Bitlocker setup. A domain administrator can generate recovery passwords automatically and transparently back them up to servers. There is not enough protection to the password and key which are plaintexts. The adversary can get access to the encrypted data as long as they get the password and key.

In short, the shortcomings of Bitlocker are as follows:

1) The scope of Bitlocker is limited. It is available in Windows Vista and Windows 7, but not supported