http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (7): 1517-1520, 2010
ISSN 1812-5638

A Review of Encryption Storage

Chaowen Chang, Min Liang, Hongzhao Kou and Zhigang Si
Institute of Electronic and Technology, Information Engineering University,
450004, Zhengzhou, Henan, People's Republic of China

Abstract: Information leakage leads to very serious consequences. Encryption storage is an effective means of ensuring information security. We summarize several typical encryption storage methods: application layer encryption, filter driver encryption, virtual disk encryption and full disk encryption. At last this paper compares these methods in some respects and provides the references for design and research of encryption storage systems.

Key words: Encryption storage, filter driver encryption, virtual disk encryption, full disk encryption

INTRODUCTION

The computer is hugely popular and computer applications become more widespread. Corporate, government and individuals have a lot of sensitive information stored in the computer. As the vulnerability management or inappropriate use, the confidential information stored in the computer is likely leaked out and damaged, taking losses to businesses and individuals, even seriously harming to the social and national. Data storage security has been a serious problem. Encryption is an effective way to prevent information leakage. Encryption storage is widely used to improve data or system security. Gao *et al.* (2010) has proposed a computing platform based on embedded system for tolerating untrusted component and encryption storage technology can protect the information in the platform. Encryption storage is used to protect the mobile device such as a smart phone, which is proposed in Cai and Chang (2009) and He *et al.* (2009). Chen *et al.* (2007) proposed a secure database scheme which is based on encryption storage. Currently, technicians are constantly researching the encryption storage techniques. This study introduces and compares the existing main encryption storage techniques.

APPLICATION LAYER ENCRYPTION

The most simple and most common method is using applications to achieve encryption, selecting cryptographic algorithms according to the needs. Secret information is encrypted and saved to a specific format (Damgard and Dupont, 2005). The most famous is free software PGP which is produced by Network Associate Inc. (Atkins *et al.*, 1996). The encryption processes in most applications intercept file read and write operations and embed their encryption algorithms to achieve encryption function. The implementation of interception is usually with the help of HOOK technique. When the HOOK holds up the operation of open protected files, the copy of encrypted file is copied to the hidden location. Then the copy is decrypted, open and edited. Lastly, the copy is encrypted and covered the original file. All of these are implemented in the application layer.

Although, this method is easy to develop, it requires users to participate more and security is poor. And it has lower efficiency, bad compatibility and weak stability. The user should remember the password. If user forgets it, the file can not be restored. At the same time, the plaintext of secret with no protection, the illegal user can take the right to access the data. So it is only suitable for less demanding on the security and a small amount of sensitive data.

OPERATING SYSTEM KERNEL LEVEL ENCRYPTION

To address the user complicated operation steps and poor security of the application layer encryption, the technicians have proposed operating system kernel encryption. The so-called kernel level encryption is that the data encryption and decryption are implemented in the operating system kernel. There are two different technical methods: filter driver encryption and virtual disk encryption. 1. Filter drive encryption.

In the commonly operating systems, filter driver can be inserted between I/O manager and file system. There have been some schemes (Zhao *et al.*, 2009; Shen *et al.*,

Corresponding Author: Chaowen Chang, Institute of Electronic and Technology, Information Engineering University, 450004, Zhengzhou, Henan, People's Republic of China

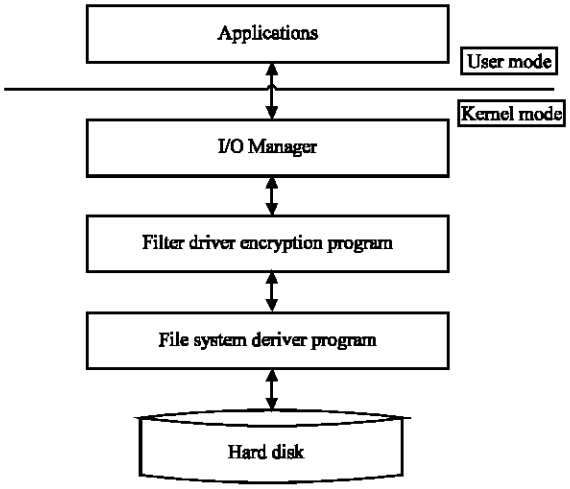

Fig. 1: Filter driver encryption model

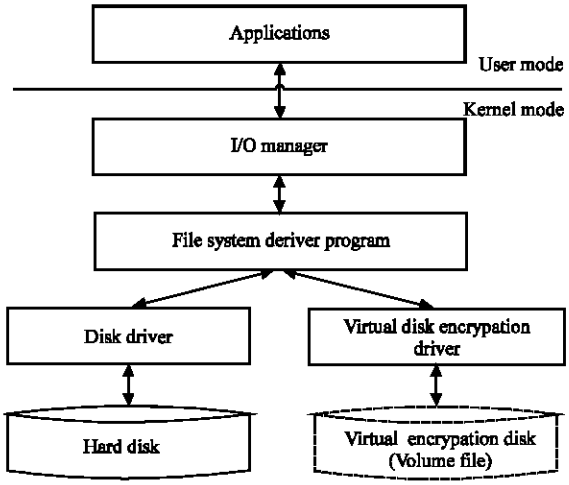

Fig. 2: Hierarchy of virtual disk encryption driver

2009; Gu and Huang, 2009). The operations on files, such as open, close, read and write, can be intercepted by filer driver. According to this feature, the specific files or folder are encrypted, decrypted or other processes to achieve the purpose of secure storage, which is shown in Fig. 1. Filter driver encryption in the kernel can avoid the shortcoming of application encryption. It improves the security of data encryption and decryption. The file operating size is also easy to control. Because the operation of encryption and decryption is transparent to the application layer, it can greatly simplify the user operations of encryption and decryption.

The meaning of developing filter driver encryption is that the underlying file system does not need to be made any changes. The file system is responsible for data management and operation, including data storage and file naming. Once the file system is designed and would not be made major changes. So it is not easy and appropriate to change the complicated and mature file system. The filter driver encryption is part of the operating system kernel, so the kernel mechanisms ensure the security of filter driver encryption.

Virtual disk encryption: Virtual disk encryption is another kernel level method, which is proposed by Li and Gan (2006), Ni *et al.* (2009) and Xiao-Wen *et al.* (2009). The virtual disk encryption driver is between the file system and disk driver, which is shown in Fig. 2. Virtual disk driver maps a storage area on a local disk as a virtual disk partition. The data which need to be encrypted is stored in virtual disk partition. The data is encrypted dynamically and stored on the disk by virtual disk encryption driver. When the data is read from the virtual disk partition, it is decrypted by virtual disk encryption driver and it is in plaintext to user. When the data is written to the virtual disk partition, it is encrypted and transmitted to the hard disk by virtual disk encryption driver. For users, the encryption and decryption operation is transparent with the help of virtual disk encryption driver.

Virtual disk encryption technology can be used to achieve higher-level security architecture than application encryption. It encrypts and decrypts data with stronger security, higher performance and better availability. The data in the virtual disk is meaningless to the operating system without virtual disk encryption software. Even if an attacker steals the virtual disk image file, he can not get the meaning of the structure of the virtual disk partition and file catalog. Also the authentication and encryption greatly protect the security of data. Another advantage is easy to use. User can load the virtual disk when using and uninstall when not. After uninstalling, virtual disk is shown as a normal file but in the form of ciphertext. It is easy to carry and preserve. The virtual disk image file can be transmitted in the network, without worrying about data loss and leakage.

Although, filter driver encryption and virtual disk encryption have many advantages, because they are kernel mode processes, its development is difficult. And it also has some limitations. For examples, they can not encrypt and protect system files and page files. Applications often have temporary files stored in an unknown location. When unpredictable things occur such as power outages or application fault, these temporary files may be missing, so that sensitive files are stored in plaintext on the hard disk. This is not secure.

FULL DISK ENCRYPTION

As the name suggests, Full Disk Encryption (FDE) means that all the data including operating system, temporary files and page files on the disk is carried out the encryption and decryption operations. There has been decades of development history of FDE. Many products based on FDE have been widely used, especially in high security needs such as government and military. There are two main ways of FDE.

Hardware-based: The FDE based on hardware means that FDE is implemented by a cipher chip which is embedded in the hard disk or in the card (Huang *et al*., 2008). The hard disk with FDE on its own function will no longer be achieved through installing the software. The mainstream hard drive manufacturers have supported FDE hard drive. The feature of hardware-based FDE is separated from operating system and it is also transparent to operating system (Hars, 2007). The data encryption and decryption operations are usually completed by a cipher chip and the whole do not need CPU support basically.

The security level of hardware-based FDE is much higher than software-based. Theoretically, it can prevent the brute force way, so more secure. However the limitations of hardware-based FDE are too reliable on the encryption card. If the encryption card is damaged, even the user can no longer access the data and the manufacturers have no way to get the key. In addition, the high cost of hardware-based FDE hampers its widespread application. The users with lower demanding on security prefer to use software-based FDE approach.

Software-based: The FDE technology carries on encryption and decryption to almost every byte on hard disk (Casey and Stellatos, 2008). In this way, an insurmountable random data isolation wall is established for malicious users who want to obtain the disk domination. The majority FDE products realize this kind of protection through setting an independent boot sector to bypass operating system normal startup procedure. Therefore, the system is even unable to start without the key. The FDE usually use symmetric crypto-algorithm to encrypt data because of its high speed. To further protect the data, the asymmetric algorithm is used to encrypt the symmetric key, which is mentioned by Liang and Chang (2010).

The main advantages of FDE are high encryption intensity, high security and comprehensive protection. It directly processes the physical disk sector, regardless of data logical structure and any data stored on the disk are ciphertext. The impact on system performance is only related to crypto-algorithms. FDE is limited to the influence of system performance, generally no more than 10%.

Because FDE has many advantages, the products based on FDE can protect confidential information. There are many products such as Windows Bitlocker (Ferguson, 2006; Ray and Schultz, 2007), Check Point (Check Point Software Technologies Ltd., 2009) and PGP Whole Disk Encryption (PGP Corporation, 2009). We make a brief introduction to Bitlocker which is representative. The Enterprise and Ultimate editions of Windows Vista contain a new feature called Bitlocker Driver Encryption which encrypts all the data on the system volume. Bitlocker requires at least two volumes: one volume used to store the boot loader, the other one used to store encrypted system files. There are three authentication methods: (1) to combine Trusted Computing Module (TPM) with personal identification number (PIN), (2) to create a removable USB drives with authorization data which is used in conjunction with PIN and (3) manual input PIN (more than 25 characters) which is allocated by operating system but input by user.

Technically, this software is very mature. There are two main problems. One is the key security. It is easy to find the key in the active directory. The key security is questionable. Another is authentication. Bitlocker startup procedure is: Power up-identity authentication-Windows start up-Bitlocker start up. The problem is the second part of authentication. Generally speaking, user authentication system is very easy to break. Once authentication has been cracked, the sensitive data is also easy to crack. There is also another problem. Bitlocker is developed by Microsoft and naturally it will not support operating systems other than Windows.

COMPARISON

These encryption storage ways are different in the working level and technology, so they have different characteristics and applications. We compared these ways in some respects, which is shown in Table 1. Application layer encryption is appropriate for the condition that the security requirement is low and the data quantity is small. The kernel level encryption is stable, high effective and relatively easy to develop, especially transparent to users. It applies to the general security requirements. FDE can encrypt all the data including operating system files and temporary files and have high security. The hardware-based FDE is fast and security, but difficult to develop, complex management and high cost.

Table 1: Comparison of encryption storage ways

Characteristics	Application layer encryption	Filter drive encryption	Virtual disk encryption	Software-based FDE	Hardware-base FDE
Working level	Application	Kernel	Kernel	Kernel	Hardware
Encryption method	File	File and folder	Volume	Full disk	Full disk
Security	Poor	Normal	Normal	Good	Very good
Encryption efficiency	Poor	Good	Good	Normal	Very good
Key management	Simple	Normal	Normal	Difficult	Difficult
Development difficulty	Simple	Normal	Normal	Difficult	Very difficult

CONCLUSION

This study summarizes kinds of methods and technologies of encryption storage, including application layer encryption, filter drive encryption, virtual disk encryption and full disk encryption and carried on the comparison of them in different aspects. This paper enables us to have a clearer and directviewing understanding to the method and technology of encryption storage and this is help for designing and researching encryption storage system. Also this paper is conducive to users to choose the right encryption storage scheme according to actual needs.

ACKNOWLEDGMENTS

This study was supported by the National High Technology Research and Development Program of China (863 Program) under grant No. 2007AA01Z479.

REFERENCES

Atkins, D., W. Stallings and P. Zimmermann, 1996. PGP message exchange formats. RFC-1991. http://www.rfc-archive.org/getrfc.php?rfc=1991.

Cai, L. and C. Chang, 2009. Research and implementation of smart phone secure storage system mobile-crypt. Network Security Technol. Appl., 4: 83-84.

Casey, E. and G.J. Stellatos, 2008. The impact of full disk encryption on digital forensics. Operating Syst. Rev., 42: 93-98.

Check Point Software Technologies Ltd., 2009. Check point full disk encryption. http://www.checkpoint.com/products/datasecurity/pc/index.html.

Chen, L., Y. Wang and C. Chang, 2007. The design of a secure database scheme. Microcomput. Inform., 23: 94-96.

Damgard, I. and K. Dupont, 2005. Universally composable disk encryption schemes. http://eprint.iacr.org/2005/333.pdf.

Ferguson, N., 2006. AES-CBC + Elephant diffuser: A disk encryption algorithm for windows vista. http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/BitLockerCipher200608.pdf.

Gao, L., X. Qin and C. Chang, 2010. A embedded system-based computing platform for tolerating untrusted component. Geomatics Inform. Sci. Wuhan Univ., 35: 626-629.

Gu, Z. and H. Huang, 2009. Research and implementation of new encrypting file system. Comput. Eng. Des., 30: 3272-3277.

Hars, L., 2007. Discryption: Internal hard-disk encryption for secure storage. Computer, 40: 103-105.

He, R., Z. Qin, F. Wang and C. Chang, 2009. Security strategy for mobile police information system using SMS. Wireless Personal Commun., 51: 349-364.

Huang, J., C. Chang and S. Ma, 2008. Design and implementation of PCMCIA-based encryption card. Network Security Technol. Appl., 8: 94-95.

Li, Q. and M. Gan, 2006. File encryption approach based on virtual disk. Comput. Eng. Des., 27: 2835-2838.

Liang, M. and C. Chang, 2010. Proceedings of 3rd IEEE international conference on computer science and information technology. Chengdu, China.

Ni, K.B., G.X. Yao and Q.L. Guan, 2009. Security enhanced virtual disk encryption system and technology. J. Comput. Appl., 29: 2987-2989.

PGP Corporation, 2009. PGP whole disk encryption. http://www.pgp.com/products/wholediskencryption/index.html.

Ray, E. and E. Eugene, 2007. An early look at windows vista security. Comput. Fraud Security, 2007: 4-7.

Shen, W., L. Wang and J. Chen, 2009. Design and implementation of encryption system based on file system filtering drive. Comput. Eng., 35: 157-162.

Xiao-Wen, K., Y. Ying-Jie and D.U. Xin, 2009. Transparent encryption mechanism of backup data for disaster tolerance. Comput. Eng., 35: 131-133.

Zhao, M., R. Mao and R. Jiang, 2009. Transparent encryption file system model based on filter driver. Comput. Eng., 35: 150-152.