Security System using Full Disk Encryption (FDE)

Polasi Sudhakar[1], Kondaveti Venkatesh[2]
[1, 2] Department of CSE
[1, 2] Ramachandra College of Engineering, A.P., India

Abstract- *Full Disk Encryption (FDE) system for analyzing the Security of the system is presented in this paper. Recent advances in FDE have enabled the use of hardware-based encryption, eliminating the need to use valuable CPU time for encryption, increasing performance, and maximizing security. This paper also comprises the implementation of the FDE, comparison of Full disk encryption vs. file system-level encryption and Boot key problem.*

Keywords- Full disk Encryption (FDE), Information Security, Authentication, File system-level encryption.

I. INTRODUCTION

Full disk encryption is a kind of disk encryption software or hardware which encrypts every bit of data that goes onto a disk or disk volume. The term "full disk encryption" is often used to signify that everything on a disk is encrypted, including the programs that can encrypt bootable operating system partitions. Full-disk encrypt is in contrast to file system-level encryption, which is a form of disk encryption where individual files or directories are encrypted by the file system itself.

The most effective approach for improving disk access performance is enhancing data locality. This is because the method could increase the hit ratio of disk cache and reduce the seek time and rotational latency. Data moves the frequently from the magnetic disk to the flash memory. Due to the data migration, most of the data accesses can be satisfied with the flash memory, which extends the idle period of the disk drive and enables the disk drive to stay in a low power state for an extended period of time. Data confidentiality on a computer can be achieved using encryption. However, encryption is ineffective under a forensic investigation mainly because the presence of encrypted data on a disk can be easily detected and disk owners can subsequently be forced (by law or other means) to release decryption keys. To evade forensic investigation, intelligent information hiding techniques that support plausible deniability have been proposed as an alternative to encryption; plausible deniability allows an evader to hide data in a manner such that can deny the very existence of the data. Security of information is an issue that has been taken into consideration from many years ago and by computer systems, this concept has gained further importance.

Lot of research was carried out in this area some of the useful works are Ming Xu et al [1] presented a method to identify the disk cluster size based on data content for various file systems. The main idea is using the difference between the entropy difference distributions of the non-cluster boundaries and the cluster boundaries to identify the cluster size. Hassan Khan et al [2] presented a new, plausible deniability approach to store sensitive information on a cluster-based file system.

Yuhui Deng et al [3] proposed an Energy Efficient Disk (EED) drive architecture which integrates a relatively small-sized NAND flash memory into a traditional disk drive to explore the impact of the flash memory on the performance and energy consumption of the disk. Lirong Dai and Kendra Cooper [4] presented the Modeling and performance analysis for security. Jesse D. Kornblum [5] reported the BitLocker Drive Encryption system included with some versions of Microsoft's Windows Vista. Yuhui Deng [6] investigated some important characteristics of modern disk drives. Based on the characteristics and the observation that data access on disk drives is highly skewed, the frequently accessed data blocks and the correlated data blocks are clustered into objects and moved to the outer zones of a modern disk drive. The performance.

Gains are analyzed by breaking down the disk access time into seek time, rotational latency, data transfer time, and hit ratio of the disk cache.

II. FULL DISK ENCRYPTION (FDE)

Full disk encryption is shown in figure 1. The main advantage of full disk encryption (encrypting all byte data on the disk) is that everything, including the swap space and the temporary files, is encrypted and the decision of which files to encrypt is not left to users. Our scheme uses a symmetric-key encryption algorithm such as AES because it is a high security algorithm and can encrypt/decrypt a disk quickly. In a full disk encryption, the OS is encrypted in a hard disk. So some program would start up the OS by decrypting the hard disk data.

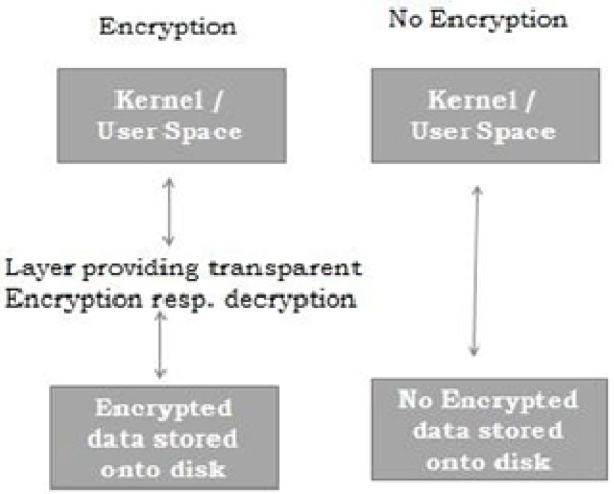
Encryption
No Encryption
Kernel / User Space
Kernel / User Space
Layer providing transparent Encryption resp. decryption
Encrypted data stored onto disk
No Encrypted data stored onto disk

Figure 1. Full Disk Encryption (FDE)

III. BENEFITS OF FDE

Full disk encryption has several benefits compared to regular file or folder encryption, or encrypted vaults. The following are some benefits of full disk encryption:

1. Nearly everything including the swap space and the temporary files is encrypted. Encrypting these files is important, as they can reveal important confidential data. With a software implementation, the bootstrapping code cannot be encrypted however. (For example, Bitlocker leaves an unencrypted volume to boot from, while the volume containing the operating system is fully encrypted.)
2. The decision of which individual files to encrypt is not left up to users' discretion. This is important for situations in which users might not want or might forget to encrypt sensitive files.
3. Support for pre-boot authentication. Immediate data destruction, as simply destroying the cryptography keys renders the contained data useless. However, if security towards future attacks is a concern, purging or physical destruction is advised

1) Implementation of FDE

Full disk encryption (or whole disk encryption) uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Full Disk Encryption prevents unauthorized access to data storage. The term "full disk encryption" is often used to signify that everything on a disk is encrypted, including the programs that can encrypt bootable operating system partitions. But they must still leave the master boot record (MBR), and thus part of the disk, unencrypted. There are, however, hardware-based full disk encryption and hybrid full disk encryption systems that can truly encrypt the entire boot disk, including the MBR.

Full Disk Encryption (FDE) prevents unauthorized access to data storage. Booting a system from a different media (e.g., a CD or a USB stick).

There are more than one way exists to achieve Full Disk Encryption. The fastest way is by implementing a pure software-based solution. Still greater security and performance are achieved with by combining this with special encryption hardware. Hardware-based Full Disk Encryption, without some form of user authentication, provides absolutely no protection of data. Currently, there are two solutions providing Pre-Boot Authentication for Hardware-based Full Disk Encryption.

Organizations considering full disk encryption should evaluate solutions based on five key enterprise requirements:

[1] End-user productivity: The solution should remain transparent at all times and not interfere with end-user productivity.

[2] Enhanced data security: Beyond full disk encryption, the solution should provide options for protecting USB flash drives, files stored on shared systems, and files and directory archives shared with others.

[3] Centralized management: The solution should allow for central management that enables administrators and help desk staff to easily support remote users.

[4] Business continuity: Encrypted data needs be accessible not only today, but for years to come.

[5] Enterprise systems integration: The solution should leverage the organization's existing infrastructure (such as directories and systems management tools) to expedite deployment and automate management and should also deploy as a single system that can be expanded later to multi-application encryption.

IV. FULL DISK ENCRYPTION VS. FILE SYSTEM-LEVEL

encryption

Full disk encryption does not replace file or directory encryption in all situations. Disk encryption is sometimes used in conjunction with file system level encryption with the intention of providing a more secure implementation. Since disk encryption generally uses the same key for encrypting the whole volume, some FDE solutions use multiple keys for encrypting different partitions. Conventional file and folder encryption instead allows different keys for different portions of the disk. Thus an attacker cannot extract information from still-encrypted files and folders.

FDE data is encrypted automatically when it's stored on the hard disk. This is different from file or folder encryption systems, FDE's biggest advantage is that there's no room for error if users don't abide by or don't understand encryption policies. The shortcoming of FDE, Lambert points out, is that it does not protect data in transit, such as information shared between devices, stored on a portable hard drive or USB or E-mail.

V. THE BOOT KEY PROBLEM

Boot is an issue to address in full disk encryption is that the blocks where the operating system is stored must be decrypted, meaning that the key has to be available before there is a user interface to ask for a password. Most Full Disk Encryption solutions utilize Pre-Boot Authentication. Some implementations such as BitLocker Drive Encryption can make use of hardware such as a Trusted Platform Module to ensure the integrity of the boot environment, and thereby frustrate attacks that target the boot loader by replacing it with a modified version. This ensures that authentication can take place in a controlled environment without the possibility of a boot kit being used to subvert the pre-boot decryption. With a Pre-Boot Authentication environment, the key used to encrypt the data is not decrypted until an external key is input into the system. All these possibilities have varying degrees of security, however most are better than an unencrypted disk.

VI. CONCLUSION

Full Disk Encryption (FDE) system for analyzing the Security of the system is presented in this paper. Recent advances in FDE have enabled the use of hardware-based encryption, eliminating the need to use valuable CPU time for encryption, increasing performance, and maximizing security. This paper also comprises the implementation of the FDE, comparison of Full disk encryption vs. file system-level encryption and Boot key problem.

REFERENCES

[1] Ming Xu., Hong-Rong Yang., Jian Xu., Ye Xu and Ning Zheng “An adaptive method to identify disk cluster size based on block content” Digital Investigation, Vol. 7, Issues 1-2, Oct 2010, pp 48-55.

[2] Hassan Khan. , Mobin Javed., Syed Ali Khayam and Fauzan Mirza “Designing a cluster-based covert channel to evade disk investigation and forensics” Computers & Security, Vol. 30, Issue 1, Jan 2011, pp 35-49.

[3] Yuhui Deng., Frank Wang and Na Helian “EED: Energy Efficient Disk drive architecture” Information Sciences, Vol. 178, Issue 22, Nov 2008, pp 4403-4417.

[4] Lirong Dai and Kendra Cooper “Modeling and performance analysis for security aspects” Science of Computer Programming, Vol. 61, Issue 1,2006,pp 58-71

[5] Jesse D. Kornblum “Implementing Bit Locker Drive Encryption for forensic analysis” Digital Investigation, Vol. 5, Issues 3-4, March 2009, pp 75-84.

[6] Yuhui Deng “Exploiting the performance gains of modern disk drives by enhancing data locality” Information Sciences, Vol.179, Issue 14, 27 June 2009, pp 2494-2511.

AUTHORS PROFILE

P.Sudhakar working as a Assoc. Professor, Department of Computer Sciences and Engineering at Ramachandra College of Engineering, Permanent Affiliated to JNTK, Kakinada, A.P., India. My researches Interests are data warehousing, Computer Network. He is life member of ISTE

K. Venkatesh working as a Asst.Professor, Department of Computer Sciences and Engineering at Ramachandra College of Engineering, Permanent Affiliated to JNTK, Kakinada, A.P., India. My researches Interests are data warehousing, Computer Network. He is life member of ISTE