IS INFORMATION ON SECURE HARD DISK DRIVE ONLY YOURS?

Jakub Arm
Doctoral Degree Programme (4), FEEC BUT
E-mail: xarmja00@stud.feec.vutbr.cz

Supervised by: Zdenek Bradac
E-mail: bradac@feec.vutbr.cz

Abstract: This paper focuses on security of information saved on hard disk drives using encryption. The posibilities of information protection are outlined. Security of using AES cipher algorithm is discussed and some possible attacks are described. Regarding these attacks, some of them are serious threat, for instance, side channel attacks. Some possibilities how to avoid these attacks are demonstrated. Cipher filesystem, as the file cipher tool, is also presented. Among them, EncFS is introduced in greater detail and its use on cloud server is pointed out.

Keywords: Security, hard disk drive, encryption, decryption, AES, cold boot attack, EncFS

1 INTRODUCTION

The present is sometimes called informational age. This is caused by rising value of good information. Some companies deal only with information. So they need to keep their valuable information secured. Almost every computer is connected to the internet to the global network, which the information can be got from or which the information can be stolen through. Information stored on hard disk drive can be stolen also locally by physical access to the computer. So user passwords, unique ideas or projects saved on user hard disk drives are in danger. To protect information on hard drives, the content of the drive can be encrypted. That means making information impossible to read. There are three approaches to do this. First, the entire hard disk drive or disk partition can be encrypted by specific software or by hardware coprocessor built in disk drive. Second, filesystem (files and directories) can be encrypted. Third, special cipher filesystem can be used [1]. Using cipher algorithm to make information unreadable promises us that potential attacker will break the cipher in very long time on current computers. But exist some other methods to get encrypted information ?

2 ENCRYPTION AND DECRYPTION

In this section, encryption approaches and methods will be described. By each method, pros and vulnerabilities will be discussed.

2.1 ENTIRE DRIVE ENCRYPTION

Using this method, entire content on hard drive is encrypted by special software even with operating system files. So it is necessary to login with disk password right after boot time. There is running small bootloader from special non-encrypted partition provided by special cipher software. This software then decrypts cipher key, which is encrypted on the drive, using entered password to the RAM memory. Then the software automatically encrypts and decrypts data when reading and writing is demanded [Fig 1].

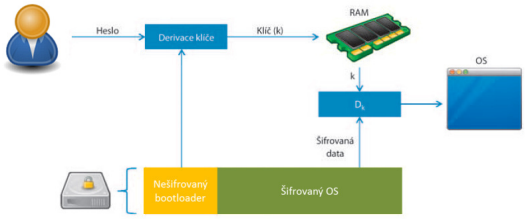

Figure 1: Full disk encryption [6]

This method is used with common disk drive when overall security is demand. Also special or even own software can be used. This software uses one of the block cipher. The most used cipher is AES in XTS mode for these purposes [2]. This cipher is used by software TrueCrypt. Another disk cipher software is BitLocker which uses AES cipher in CBC mode [Fig 2]. This mode is nowadays sufficiently considered as secure. AES cipher is also chosen thank to hardware acceleration support on newer processors [6]. AES cipher is described more later. Software is running on main processor, therefore there is a vulnerability. Software tools stores the cipher key in RAM memory. Using fast reboot attack or cold boot attack can be the password revealed [7]. This is described later.

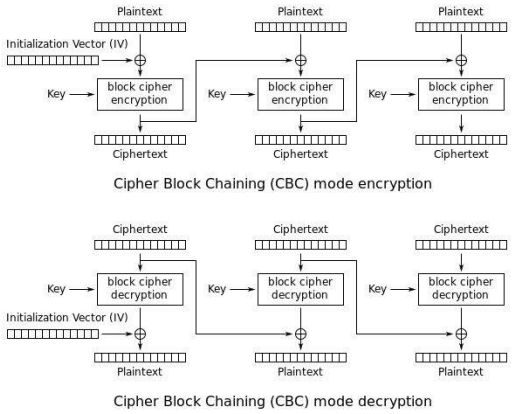

Figure 2: Full disk encryption [10]

Software encryption and decryption of information means a load for main processor and thus slower reading of these information. Hardware encryption and decryption is made to be faster because of optimization and external execution of cipher processes. Hardware encrypted drives called Self-encrypting Drives uses cipher subsystem built in chip which takes care about reading and writing data over SATA bus. Also reading and writing the data is faster thank to optimized cipher algorithms. This drive can run any operating system. Unlocking is done before boot phase of the OS [3].

2.2 FILESYSTEM ENCRYPTION

Some software can encrypt each file or folder separately. This approach is used when only some data are confidential. There are many software to do this, e.g. FileCryptor, X-Key or VeraCrypt. This software makes encrypted file from plain file using user key and then erase safely the plain file. For these purposes can be used any symmetrical block cipher. One of the used cipher is AES because it is efficient in comparison between speed and security [2]. Difficulty of decryption without the key is equal to difficulty of AES algorithm after crypt software performs encryption and closes. This is one

of the advantage to hard drive encryption. Also amount of data to be encrypted is smaller therefore the encrypt process is faster. On the other side, key is needed every time the file is accessed or modified and cipher operations has to be done.

2.3 CIPHER FILESYSTEM

Cipher filesystem is another approach how to encrypt files. It is possible to mount encrypted and decrypted version. Cipher filesystem is superstructure to common filesystem. This is often used in cloud services like Dropbox. It takes advantages of common file encryption that is cipher file looks and behaves like a file. Advantage of entire disk or partition encryption is that all cipher files behaves like mountable partition. Files in cipher filesystem are not encrypted by user cipher key but by generated random key which is then encrypted by user key and saved as a file. This makes changing user password operation shorter and easier [8]. On the other side, once the user key is lost, every data will be lost.

Examples of these filesystems are EFS on Windows [1] operating system and EncFS on Linux OS. These filesystems use AES cipher described later or Blowfish.

EncFS is Linux cipher filesystem but there is experimental Windows port called Encfs4Win. When EncFS is used on Dropbox, the files can not be read from webclient. Webclient only knows that there are some files. EncFS can even run on Android because Android is based on Linux [8]. Diagram of mounted points and file transfer channels is in [Fig 3].

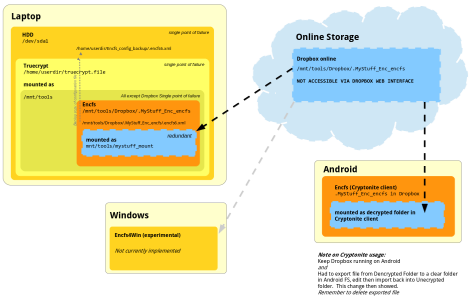

Figure 3: EncFS diagram [9]

3 AES

AES (Advanced Encryption Standard) is one of the block crypt algorithms. This algorithm is standardized. It encrypts defined block of data using cipher key. Using the same key, it decrypts the resulted cipher back to plain text. Therefore it is called symmetrical crypt algorithm. The key can be 128, 192 or 256 bits long. The cipher key is transformed to expanded key which is used in parts in each round. Firstly, the initial round is performed and then after some count of rounds the encryption ends performing final round. Decryption algorithm is different but can use some operations of encryption algorithm [11].

AES algorithm flow is drawn on Fig 4. Before the drawn algorithm is performed, the key has to be expanded.

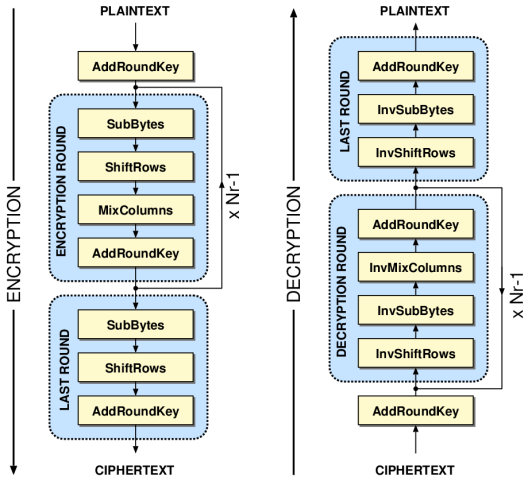

Figure 4: Full disk encryption [10]

3.1 AES CIPHER RESISTANCE

AES cipher is well described and it is believed it has no structural weakness. Like all other ciphers, this can be broken using brute force attack. So every possible key is tried to get plain data. Possible variants of the key is derived from its length. The complexity of this algorithm is $O(2^n)$. Nowadays 128bit key is considered to be secure for common user even when Grover algorithm running on the certain count of quantum computer is used. This system can reduce the cipher complexity to $O(2^{\frac{n}{2}})$. So the cipher key length has to be increased [12].

3.2 SIDE CHANNEL ATTACK

Generally, an attack uses some of the system vulnerabilities, e.g. software backdoors or drawbacks. In the system, even the user is involved because some types of attacks called *phishing* or *social engineering* use them. Suppose the direct access of an attacker to the system is not eliminated, some of the *evil maid attack* might be comitted, for instance, software or hardware keylogger, operation system modification, and bootkit. Another type of attacks are *side channel attacks* that uses weak points in the implementation of the system instead of weak points in cipher algorithm. One of the famous attacks to hard drive cipher software is boot attack.

This attack tries to reveal the cipher key from RAM memory where it is located. This can be achieved under certain conditions. Firstly, the data has to be retain in RAM memory for a certain time after power loss. This has been measured and proved on many RAM memories [5]. Secondly, a BIOS on the attacked computer must not fill the RAM memory at startup with random values which some new BIOS can do. This condition can be overcome moving the RAM memory physically into another computer where the BIOS does not do that.

There are two options: Cold Boot Attack and Fast Reboot Attack. In Cold Boot Attack, the cold nitrogen is used to lower the temperature of the RAM memory to postpone data loss after power loss. The RAM memory is read or moved into another computer and then it is read. Fast reboot attack relies only on retaining data for a couple of seconds in the RAM memory. The cipher key is then searched in the content of the RAM using special software developed at Princeton University [5]. This process is described in [7].

Other type of attack aims to debug software implementation of cipher algorithm. If attacker has access to debug cipher process and knows the algorithm, he can find weak point or even the key in

stack or registry. The defence against this is to link cipher binaries statically [10]. Other defence is to obfuscate cipher code implementation to make it difficult to debug it. The obfuscation can not be done completely because every program is translated into machine language so the program is readable. The point is to make it difficult to catch the meaning of instructions. There are some techniques to detect and then stop debugging.

Some types of self encrypted drives have backdoors or security bypasses. The drive can be controlled directly by SCSI commands so anyone has full access to disk even without the password. Other vulnerabilities comes from badly implementation. For example random generator has lesser random capabilities then expected. About this type of vulnerabilities, the research is presented in [4].

4 CONCLUSION

Every confident information needs to be encrypted. Especially when is uploaded to cloud server. There are many options how to encrypt files with information. All options use some kind of symmetrical block cipher, e.g. AES or Blowfish. AES is well described and considered to be secure for a certain time by using present computers. Therefore all possible attacks aim to some kind of vulnerability of the system, e.g. bad implementation. Majority of possible side channel attacks can be avoided using right hardware, good implemented software and some support mechanism in BIOS. On the other side, there are possibilities how to get data by professional using some side channel attack at certain conditions. Among file cipher options, there is cipher filesystem EncFS presented which is good option that benefits advantages of other options.

ACKNOWLEDGEMENT

This paper was made possible by the grant No. FEKT-S-17-4234 - “Industry 4.0 in automation and cybernetics” financially supported by the Internal science fund of Brno University of Technology.

REFERENCES

[1] BCV SOLUTIONS. Sifrovany filesystem v linuxu.

[2] BURDA, K. Aplikovana kryptografie.

[3] GENISOFT. Fakta a myty o hardwarovem sifrovani disku. *ICT Security* (2015).

[4] GENISOFT. Got hw crypto? on the (in)security of a self-encrypting drive series. *ICT Security* (2015).

[5] HALDERMAN, J., SCHOEN, S., HENINGER, N., CLARKSON, W., PAUL, W., CALANDRINO, J., FELDMAN, A., APPELBAUM, J., AND FELTEN, E. Cold boot attacks on encryption keys. *Proc. 17th USENIX Security Symposium* (2008).

[6] IT SYSTEMS. Sifrovani pevnych disku.

[7] KRCMAR, P. Jak prolomit sifrovani disku za 2 sekundy. *OpenAlt* (2010).

[8] KRCMAR, P. Encfs: sifrovani souboru jinak a bez problemu.

[9] LINUXLIST. Overview of shared online encrypted storage via dropbox using encfs.

[10] PARSIYA. Tales from the crypt(o) - leaking aes keys.

[11] SVENDA, P. Srovnani standardu aes s algoritmy 3des a idea.

[12] WIKI. Delka klice.