Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review of USB Encryption Techniques & Algorithms for Data Confidentiality

Jasmin Jivani
Computer Science & Engineering,
Gujarat Technological University
Ahmedabad, Gujarat, India

Samuel Johnson
Computer Centre,
Physical Research Laboratory
Ahmedabad, Gujarat, India

Gayatri Pandi (Jain)
HOD, Computer Department,
LJIET
Ahmedabad, Gujarat, India

Abstract*— With rapid development and usage of technology among people, data migration has become an essential part of our life. Various removable devices like USB flash drives, hard drives, PDAs etc are used to move data. Removable media are widely used for transferring, storing or for backing up data. People often spend considerable amount of time generating data that are confidential even for the organization they work for. Maintaining confidentiality of data has become a great challenge. Any security threat can lead to organization's sensitive data being compromised. Due to this many organizations restricts the usage of removable devices, but restricting usage of these devices is not an optimal solution. In this paper we will review various cryptographic techniques, algorithms and tools available for securing data on major platforms that might help in solving this problem.

Keywords*— Data Confidentiality, Information security, USB, encryption, removable media.

I. INTRODUCTION

Data confidentiality means that the data stored in the system is protected against unintended access. Due to advances in computer science, removable devices are thus preferably used for data storage and transfer due to its convenience, ease of usage and higher transfer speeds. Hence maintaining confidentiality is essential as removable devices are widely used among people for data migration. Due to this, the usage of these devices are tremendously increased resulting in the exposure of confidential data as it is stored in plain text and possess huge risk of data being compromised and being misused. Thus, this has become a major issue in the field of information security.

Data theft has now become a growing problem as with the ease in technology like desktop computers, other hand-held devices all the sensitive data is been stored in them and if proper security is not provided or if someone is intercepting or attacking the data it can create huge problems in individual's personal or professional life. Therefore, despite their convenience and ease of usage, removable devices (USB) have been prohibited in most of the institutes/organizations as they are main source of transmitting computer viruses and other harmful software that harms and degrades the performance of machines, but preventing usage of these devices is not an optimal solution.

USB memories have become standard components to store data in enterprises and among individuals. However, crucial information can be obtained from these memories when USBs are lost, stolen or hacked because they usually store many different kinds of important data. The loss of this data can result in considerable security vulnerabilities and sometimes can also breach national security [1].

Besides, [4] claimed that a security breach exposing the data of over 2595 Michigan resident's personal information was compromised when a laptop and a flash drive was stolen from the employee of State Long Term Care (LTC) Ombudsman's Office on January 30,2014.

In this paper, Section II discusses background information and related work. Section III presents description about the existing data encryption techniques for removable media, Section IV presents the comparison between algorithms, Section V presents the performance analysis of encryption algorithm and Section VI presents our conclusion.

II. RELATED WORK

Various tools and software are available that helps us in our study. They are widely used tools or disk encryption software which is computer security software that maintains confidentiality of data that is stored within removable media (such as USB media, hard disks, floppy disk etc.) by using disk encryption. Several types of tools are reviewed, such as BitLocker, TrueCrypt, FileVault, AESCrypt, SecurStick which shows the current trend in disk encryption scenario.

- BitLocker (BitLocker Drive Encryption) initially released in 2006, is a security feature that provides protection to data and is available for Windows operating system users running Ultimate or Enterprise version of Windows 7 or the pro and Enterprise version of Windows 8. It is also available for server platforms like Windows server 2008. It is used to provide encryption to data of entire volumes and by default it uses AES encryption algorithm in CBC

mode with 256 bit key, combined with Elephant diffuser as it provides additional security which is not provided by AES. But the disadvantage of this is it works only on Windows Platform [10].

- TrueCrypt is a software for preserving and implementing an on the fly encryption (OTFE). On the fly encryption is a method which refers to data being automatically encrypted or decrypted as it is loaded or saved. It creates a virtual encrypted disk within a file, partition or the entire storage device where data cannot be decrypted (read) without using password or encryption keys. TrueCrypt was the only software which was used on Android platform. But on May 2014, TrueCrypt Website announced that the project was no longer available and recommended users to find an alternate solution [9].
- FileVault was introduced in Mac OS X Panther, which encrypted user's home directory but not the entire volume. Now FileVault is available for Mac OS X Lion or later and OS X Recovery installed on the start-up drive. FileVault uses XTS-AES 128 bit encryption for securing data. Only authorized users can lock or unlock the drives. This encrypts whole OS X start-up volumes and includes home directory as well. But the major disadvantage of this is it works only for the Mac OS platform [8].
- AESCrypt is open source file encryption software which runs on Windows, Mac, Linux and even Android devices. It uses 256-bit AES encryption algorithm which can safely secure the user's most sensitive information. On Windows the files are encrypted by only right clicking and choosing aescrypt. On Mac, user can drag a file and provide the required password into the aescrypt program. On Linux, using command line specific syntax is used i.e by using word "aescrypt" encryption or decryption of files can take place. Relies upon having /dev/urandom, This program was deliberately kept extremely simple. It is not intended to be a full encryption solution, it is intended to be used within scripts as part of a complete solution. Keychain management, public key signatures, etc. are all expected to be done external to this program [11].
- SecurStick is a portable drive encryption tool which is used to secure data of USB drives and removable media. It uses AES-256 bit encryption algorithm and works for Windows, Mac, Linux platforms. It consists of WEBDAV which caches the data and passwords so it is more important to remove the cache files before leaving the page. SecurStick does not guarantee data protection as anyone can delete the files but it can protect our data from being stolen. It is a German website but its English translation is also available [7].

Table I Comparison of data encryption tools

Tools	**Comparison of tools**			
	Algorithm used	**Open Source**	**Platforms**	**Limitations**
BitLocker	AES	No	Windows	Platform specific
TrueCrypt	AES, Serpant or Twofish	Yes	Windows, Mac, Linux	Project already closed
FileVault	AES	No	Mac	Platform specific
AESCrypt	AES	Yes	Windows, Mac, Linux	Max file size 2GB
SecurStick	AES	No	Windows	Max file size 47MB

III. EXISTING DATA ENCRYPTION TECHNIQUES FOR REMOVABLE MEDIA

Removable media has the advantage of usage from any system and without any installation it is widely preferred among people for data migration. But due to security breaches removable devices are restricted in many organizations as data can easily be stolen through USB devices hence to protect the sensitive data many techniques have been used which are as follows:

A. Smartphone as a second authentication factor:

In this technique, when the user inputs the USB storage device required credentials of user is been given to open the encrypted files. The two phase authentication is been carried out through smart phone as mutual authentication between PC and smart phone is been done and authentication token is been sent through PC. The smart phone responds with the equivalent authentication value and thus eligibility to decrypt files on storage device is been gained by the user. The main advantage of this technique is that the authentication process is been achieved offline, eliminating the need of Internet connection. This mechanism also prevents forgery attack as device id is also been registered. But there is a possibility that if the mass storage device gets damaged and so is the ID then user might lose all his/her confidential data as system won't provide any information unless the user passes its verification phase [1].

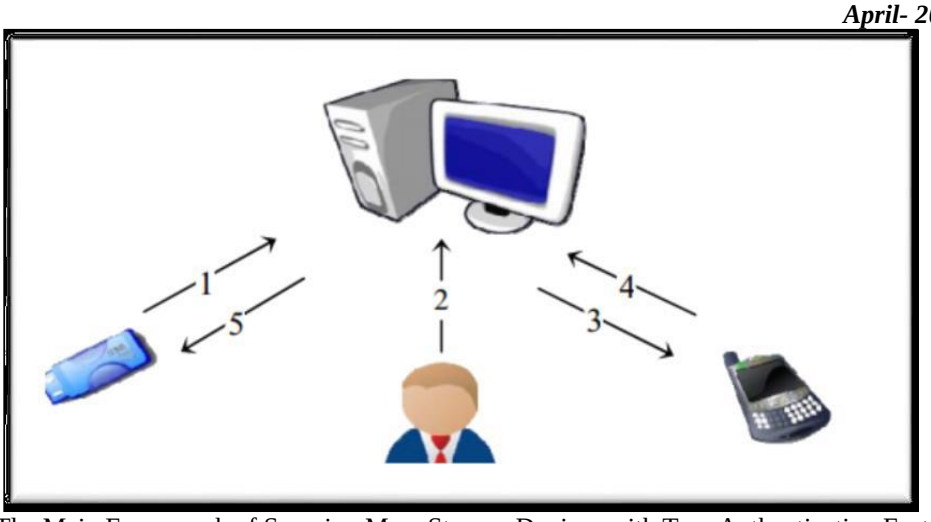

Fig 1 The Main Framework of Securing Mass Storage Devices with Two Authentication Factors [1]

B Providing authentication using Biometrics:

In this technique, the biometric keys are used which have the advantages like it cannot be lost or forgotten, very difficult to copy or share, extremely hard to forge or distribute and it cannot be guessed easily. Authentication Server (AS) is used to manage security for a USB device. AS restricts the data transfer over USB interface unless the user passes the AS's authentication. If the user wishes to transfer the data he/she is required to input their username, password and biometric characteristic to verify legitimacy [3].

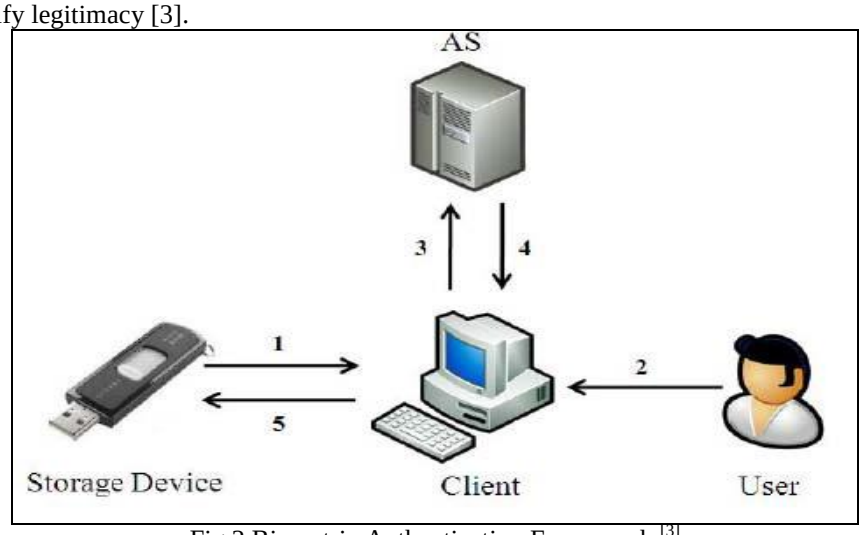

Fig 2 Biometric Authentication Framework [3]

When user wants to be the valid user of AS, he/she needs to input biometric characteristic, through a specified biometric device and provide password and identity. This input values are used for the authentication procedure. When user is successfully authenticated, a shared session key is generated between users and AS. Then, the session key will be used to encrypt the files transferred via the USB interface. When the user decrypts the files on the storage device user must follow the same procedure and generate the session key for the original file. The advantage of this is, it is robust against conceivable attacks but there is a still existing security vulnerability issue that is needed to be solved like the DoS attack and replay attack [3].

IV. COMPARISON OF ENCRYPTION ALGORITHMS

Cryptography is the art and science of protecting data. To convert the plain text data from readable format to non readable format using a key, it is known as encryption and when non-readable format is converted into readable using the corresponding key it is known as decryption. Different cryptographic algorithms are available to encrypt and decrypt data but they are broadly classified into two: symmetric key algorithms and asymmetric key algorithms. In symmetric key, also known as secret key encryption only one key is used to encrypt and decrypt the data. Asymmetric key algorithm consists of two keys viz public key and private key. Symmetric key algorithms are widely used for securing data than asymmetric key as it is 1000 times faster than asymmetric algorithms due to less computational processing power requirement. Asymmetric key algorithm is very slow due to the complexity of mathematical functions used by these algorithms, as well as the length of asymmetric keys.

Key length plays an important role in encryption. If weak keys are used then any one can try to brute force and decrypt the data. The strength of encryption depends on size of the key. Longer the size, more difficult it is to crack the encryption. Different symmetric key algorithms are as follows:

A. *Data Encryption Standard (DES):* DES is the first encryption standard recommended by NIST (National Institute of Standard and Technology). It became standard in 1974. It is symmetric with 64 bit block cipher and 56 bit key. It consists of a 16 round series of permutation and substitution. Multiple permutation, substitution, circular shift, swapping, XORing, a set of lookup tables is done in each round that are essential in DES algorithm. Due to its weak substitution tables and its vulnerabilities to differential and linear cryptanalysis, it is no longer cryptographically secure [2].

B. *Triple Data Encryption Standard (3DES):* 3DES is an enhancement of DES. This standard is similar to that of DES but is applied 3 times to each data block in order to increase the complexity. 3DES uses 3 different keys total size of 168 bits. All keys are identical or the first and last key may be the same. Thus, it is known fact that 3DES is the slowest among all other block cipher algorithms [2].

C. *Advanced Encryption Standard (AES):* AES is a new encryption standard recommended by NIST which replaced DES. AES is the combination of both substitution and permutation, and is fast in both hardware and software. It has a fixed block size of 128 bit and key size of 128, 192 or 256 bits with 10, 12 or 14 number of rounds respectively. Its encryption is faster and flexible hence can be implemented on various platforms especially in small devices [2].

D. *Blowfish:* Blowfish designed by Bruce Schneier in 1993, is a symmetric key block cipher that uses 64 bit block size and variable key length. It takes a variable key length from 32 bit to 448 bits. These variants have 16 processing rounds with 4 s-boxes. Two main functions are performed in this algorithm and they are key expansion and data encryption. In blowfish, s-boxes are key dependent [2].

TABLE II COMPARISON OF ENCRYPTION ALGORITHMS

Algorithms	**Comparison**		
	Key Length(in bits)	**Number of Rounds**	**Limitations**
DES	56	16	Linear cryptanalysis attack
3DES	128	16	Linear and differential attacks
AES	128,192 or 256	10,12,14	Haven't cracked and secure
BLOWFISH	32-448	16	Weak Key Attacks

V. PERFORMANCE ANALYSIS OF ENCRYPTION ALGORITHMS

A. Based on Scalability:

The performance of an algorithm can be calculated based on scalability which is based on the basis of memory usage and the performance of encryption (i.e. processing time). Hence, lesser the memory usage results in more efficiency whereas lesser the processing time results in more encryption rate. Encryption rate is defined as the processing time required by an encryption algorithm to encrypt data.

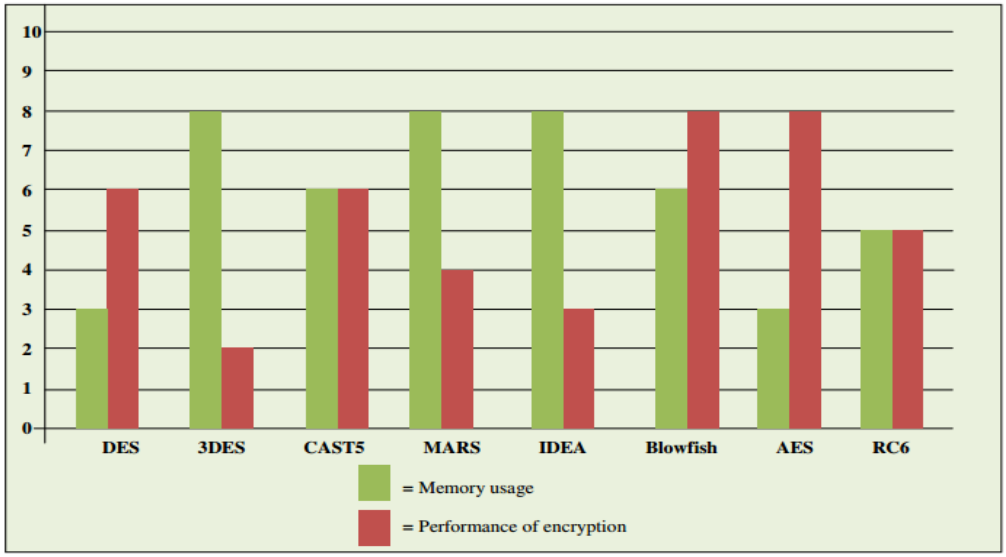

Fig 3 Comparison of algorithm based on scalability [2] (Memory Usage and Performance)

It is clear from the above figure that the performance of encryption is nearly equal in both AES and Blowfish algorithms but the memory usage of Blowfish is higher than that of AES, Hence AES is preferable over Blowfish.

B. Based on Security:

An encryption algorithm or any security system is considered better only if they cope well with the security aspects related with it. Security related features of symmetric encryption algorithms are discussed below.

1. **DES:** The key length of 56 bit is used with DES for the encryption. But today, it can be cracked by brute force attack using 256 combinations. Hence DES is not recommended for use in encryption [2].
2. **3DES:** In 3DES, DES process is performed three times using three different keys for improving the level of security. It uses key size three times larger than DES or simple DES. Hence it is preferred more than DES for encryption [2].
3. **AES:** AES uses variable length keys with key size of 128, 192 or 256 bits. Hence AES provides higher level of security for encryption. Different types of attacks like key attack, differential attack, square attacks were tried to crack this algorithm. But all of these attacks was not able to crack AES. Hence AES is classified as a best and more secured encryption technique [2].
4. **BLOWFISH:** Blowfish uses variable length key of 32-448 bits. In this algorithm each bit of the master key involves multiple round keys and hence independent of another. So we can say that blowfish is a secure algorithm for encryption [2].
5. **IDEA:** IDEA uses 128 bit key size for encryption. It is found that the vulnerabilities in IDEA are less in accordance with linear and differential attacks. It performs maximum operations for enhancing its security level and hence it provides a strong security against differential attacks [2].
6. **RC6:** RC6 provides security against differential attacks in a better way, RC6 possess the parameter of random series output that provides better protection against the attacks it can experience. In a Linear attack an adversary can apply for 16 rounds of RC6 but it would be impossible to succeed as an adversary has to at least perform 2119 combinations of plaintext [2].

After the comparison, it is analysed that AES is secure, fast, better and effective encryption algorithm among all these encryption algorithms with less storage space, high encryption performance currently without any weakness and limitations.

VI. CONCLUSION

In this paper, review of various existing USB encryption tools are discussed for maintaining confidentiality of data with their respective features and limitations which are highlighted. Different encryption techniques are also discussed like the two factor authentication using smart phone and the three factor based authentication using biometric which helps us to understand that different authentication factors can also be used to increase the security level in the removable media. Advantages and disadvantages of the same are also analysed.

Further, comparison between the encryption algorithms is given and the performance analysis of the same is also carried out. This concludes that both AES as well as the blowfish can be used for encryption of data but in terms of security AES is more secure and faster compared to the blowfish algorithm and as memory usage of blowfish is higher AES has more efficiency than blowfish. Blowfish also contains weak keys and thus the attack on data is possible and there is no such possibility in AES. Hence, AES is more preferable than Blowfish.

Hence, based on this review we can conclude that the existing tools are very complicated for everyday users to use. Therefore only the people who are technologically sound are using them where as other normal users are still facing issues with data loss, virus problems etc. So, better USB encryption tool is required which helps in protecting the confidentiality of data in removable devices which gives an optimal solution in terms of speed, security and performance which can also be used by normal users. The future work can also include the tool supporting various platforms as well large sized file like multimedia, images should also be encrypted with similar speed while maintaining confidentiality of data.

REFERENCES

[1] Mohamed Hamdy Eldefrawy, Muhammad Khurram Khan1 and Hassan Elkamchouchi, "The Use of Two Authentication Factors to Enhance the Security of Mass Storage Devices" IEEE 11th International Conference on Information Technology: New Generations, 2014.

[2] Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information Security" International Journal of Computer Sciences and Engineering IJCSE (ISSN: 2347-2693) Volume-2, Issue-4, April 2014.

[3] Debiao He, Neeraj Kumar, Jong-Hyouk Lee, *Senior Member*, IEEE, and R. Simon Sherratt, *Fellow*, IEEE, "Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices" IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

[4] Stolen Flash Drive Exposes 2,595 Michigan Residents' Data. Last accessed from http://www.esecurityplanet.com/network-security/stolen-flash-drive-exposes-2595-michigan-residents-data.html/ [3 November 2014].

[5] Information Security. Wikipedia. [Online] http://en.wikipedia.org/wiki/Information_security.

[6] Privacy and Confidentiality – current issues in research ethics. [Online] http://ccnmtl.columbia.edu/projects/cire/pac/foundation/
[7] SecurStick [Online] http://www.withopf.com/tools/securstick/
[8] FileVault [Online] http://en.wikipedia.org/wiki/FileVault
[9] TrueCrypt [Online] http://en.wikipedia.org/wiki/TrueCrypt
[10] BitLocker [Online] http://en.wikipedia.org/wiki/BitLocker
[11] AES Crypt. [Online] https://www.aescrypt.com/

