January 2014

A STUDY OF ADVANCED ENCRYPTION TOOLS FOR DATA SECURITY

SHRIKANT G. JADHAV

Department of computer science, Yeshwant Mahavidyalaya, Nanded, Maharashtra, India,
SHRIKANT@gmail.com

GURUPRASAD B. CHOUNSTE

Department of computer science, Yeshwant Mahavidyalaya, Nanded, Maharashtra, India,
chounste@gmail.com

Follow this and additional works at: <https://www.interscience.in/ijcns>

Part of the [Computer Engineering Commons](#), and the [Systems and Communications Commons](#)

Recommended Citation

JADHAV, SHRIKANT G. and CHOUNSTE, GURUPRASAD B. (2014) "A STUDY OF ADVANCED ENCRYPTION TOOLS FOR DATA SECURITY," *International Journal of Communication Networks and Security*: Vol. 2 : Iss. 3 , Article 6.

DOI: 10.47893/IJCNS.2014.1092

Available at: <https://www.interscience.in/ijcns/vol2/iss3/6>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Communication Networks and Security by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

A STUDY OF ADVANCED ENCRYPTION TOOLS FOR DATA SECURITY

SHRIKANT G. JADHAV¹, GURUPRASAD B. CHOUNSTE²

^{1,2}Department of computer science, Yeshwant Mahavidyalaya, Nanded, Maharashtra, India
E-mail: chounste@gmail.com

Abstract- With the rapid growth and uses of internet, the task of protection of data and information is become a key challenge to the user as well as security experts. In the era of e-commerce, online shopping, online banking information security is a vital issue. Information may be hacked, stolen and misused. To overcome these issues, encryption tools can be useful. Wide range for encryption tools are available that provide the facilities to the user to secure the information. This paper highlights some of these tools with their features.

Keywords- e-security, encryption, encryption tools, AES.

I. INTRODUCTION

In last few years a rapid growth in internet browsing & surfing has taken place in all over world. Internet is great source of information but viruses & hacker are main problems on internet. The task of protection of the data and information stored in the computers and passing over the internet has become a challenge to the security experts.

Nowadays most of business deals, transactions, information sharing is done with the help of internet as it saves the time and less expensive. E-commerce, online shopping is raising trends. While there are benefits associated with the ever-increasing growth such trends there is a down side too. The technology provides great opportunities for business to reach new markets and more customers than ever before, but these opportunities comes some e-security risks. These risks can cause loss and misuse of sensitive information of user like information related with credit card or financial transactions.

II. ENCRYPTION & ITS NEED

Encryption is a method of coding information. In encryption method, the information is coded in such a way that a third party cannot access to the data or cannot reconstruct, decrypt the original information. Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it. For example, if a user purchases something from a website, the information for the transaction such as address, phone number, and credit card number is usually encrypted to help keep it safe [1].

The encryption methods apply a certain routine to information so that it's no longer identifiable as its original. With the decrepitated right key, that was determined before encrypting the data and the

accompanying routine for decrypting the information, the original information can be recovered [2].

Nowadays information is the key concern for the users on computers and internet. The privacy & security of information is highly expected from its users. So encryption methods and tools are beneficial for the same purpose. Encryption tools are found to be very useful in the basis of data integrity and privacy which is necessary for any type of transactions over the internet.

III ENCRYPTION TOOLS

Outfitting a PC with a firewall and antivirus tool may keep out most hackers but it doesn't assure security. If someone gets physical access to users system then the best internet security suite will not be useful and there is only one way to ensure protection is – encryption[3].

Encryption is important because it allows user to securely protect data that user don't want anyone else to have access to. Businesses use it to protect corporate secrets, governments use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

Widespread encryption tools are available today some of them are discussed below

A) Ax Crypt

AxCrypt is free and easy to use open source strong file encryption software for Windows, integrated with Windows Explorer. Encrypt, compress, decrypt, wipe, view and edit with a few mouse clicks. Encrypted files have a ".axx" extension added to their names [4].

AxCrypt is encryption tool that helps user to protect the documents from unauthorized access, encrypting files using an AES (Advanced Encryption Standard)

Algorithm with 128bit Keys. It combines a powerful symmetric encryption with compression and the ability to open/edit a file just with a simple double click. AxCrypt doesn't require any configuration at all, it integrates with the Windows Shell making the task of encrypting a file as easy as Right Clicking it and selecting "AxCrypt | Encrypt".

1) Features of AxCrypt:

AxCrypt encryption software comes with following key features [4].

1. Easy to install & use.
2. No need to configure just install and can use
3. Open source under GNU General Public License.
4. User can open or modify our encrypted files with our favorite application just by double clicking on them.
5. After saving & closing the file AxCrypt automatically re-encrypts it.
6. For programmers and system administrators, there is also a command line interface callable from batch files, scripts and other programming languages.
7. It use 128bit Key AES (Advanced Encryption Standard) Encryption. User can cache user pass phrase so user itself only have to enter it once per login. It uses Verification of data integrity so no file change goes undetected.
8. AxCrypt is compatible with almost all versions of Windows.

B) Truecrypt

Truecrypt is an open source application which is helpful for anyone who needs the privacy. Due to the sudden occurrence of bits, keeping confidential data under cover is becoming a difficult task, because you have risk to losing it. Data is insecure if we leave it as it is in any medium, which is a potentially dangerous situation. It means that for the need of programs which are capable of protecting our privacy.

TrueCrypt is software for establishing and maintaining an on-the-fly-encrypted volume. On-the-fly encryption means that data is automatically encrypted right before it is saved and decrypted right after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc) [5].

1) Features of Truecrypt :

The program protects the encrypted file using keys that are protected by a separate TrueCrypt passphrase. This encryption is transparent to the user and is done locally at the user's computer. This means user can

store a TrueCrypt file on a server and TrueCrypt will encrypt data before it is transmitted over the network.

Following are the main features of true crypt software. [5]

1. Creates a virtual encrypted disk within a file and mounts it as a real disk.
2. Encrypts an entire partition or storage device such as USB flash drive or hard drive.
3. Encrypts a partition or drive where Windows is installed
4. Encryption is automatic, real-time (on-the-fly) and transparent.
5. Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
6. Encryption can be hardware-accelerated on modern processors.

C) Comodo Disk Encryption

Comodo Disk Encryption allows user to create a virtual encrypted drive that will hold most confidential files but also lets users encrypt an entire partition of their hard drive. Comodo Disk Encryption then won't even let system start until user have entered the password, and you can optionally require authentication with a USB memory key as well.

It is a free software to secure files, folders, partitions or the entire computer hard disk by applying strong encryption. This stops preying eyes if share a computer with someone else and protects your data if you laptop or external hard disk gets lost or stolen.

1) Features of Comodo Disk Encryption:

It is a free software to secure files, folders, partitions or the entire computer hard disk by applying strong encryption. This stops preying eyes if share a computer with someone else and protects your data if you laptop or external hard disk gets lost or stolen.

Following are the key features of this software. [6]

1. Comodo Disk Encryption is absolutely free.
2. It can be installed on almost all versions of windows.
3. Its interface is logically organized and easy to use.
4. It allows user to encrypt entire partition or drives with a right-click on the item in the Drives view.
5. User can create virtual drives. Size of drive can be specified by user
6. Uses MD5, AES and Twofist algorithms.
7. The CDE Drives tab lets user to secure hard drives and partitions using encryption including the C:/ partition where Windows is installed.

D) Symantec Drive Encryption

Symantec Drive Encryption provides organizations with comprehensive, high performance full disk

encryption for all data (user files, swap files, system files, hidden files, etc.) on desktops, laptops, and removable media. This full disk encryption software protects data from unauthorized access, providing strong security for intellectual property, customer, and partner data. Protected systems can be centrally managed by Symantec Encryption Management Server simplifying deployment, policy creation, distribution, and reporting. [7]

1)Key Features Symantec Drive Encryption:

1. Easy Passphrase and Machine Recovery.
2. User-Friendly.
3. Comprehensive Multi-Platform Coverage.
4. Optional Silent Deployment.
5. High Performance .
6. Part of a Long-Term Enterprise Security Strategy.

E) Cryptomathic File2File

File2file offers an encryption solution where security is a common concern when data is to be sent over an insecure connection. This program enables to transfer data between colleagues, customers etc in a secure manner. It offers one password for the file, which is to be shared by the two parties.

The file can be retrieved only if the password is known. The application converts the file or directories into a simple distributable execution file that would ask for the password when the data is to be retrieved. The files are encrypted and decrypted on the AES algorithm base that is too strong to be broken through. The application deletes the original content in the hard disk and disk cache after encrypting the files [8].

1)Features of file2file:

1. It support sensitive and simple password protection.
2. Strong encryption and decryption of files and directory.
3. It based on AES encryption algorithm

4. Secure transfer of files.
5. Simple distribution with executables for decryption
6. Deletes the originals from hard disk and disk Cache after encryption
7. Send secured files via e-mail
8. Can be used on a standalone drive, a shared network,

IV. CONCLUSION

In the world of electronic communication, security has become as crucial as ever, and still more people realize that privacy and confidentiality can no longer be taken for granted and information can be misused at any moments. If someone gets the physical access of the system then risk of information theft become high. To avoid the risk , use of encryption tools can be very useful. Wide range of encryption tools are available today. Tools like Truecrypt, AxCrypt, etc are available freely for the user which helps user to secure his data on the system. It is on the user to select one of best suitable tool for data security as per requirements.

REFERENCES

- [1] (2013) The Microsoft website. [Online]. Available: <http://windows.microsoft.com/en-us/windows7/what-is-encryption>
- [2] (2013) Axantum Website. "Introduction to AxCrypt", [Online]. Available: <http://www.axantum.com/AxCrypt/Introduction.html>
- [5] (2013) TrueCrypt Website , "Introduction to Truecrypt" [Online]. Available: <http://www.truecrypt.org/docs/>
- [6] Mark Muller, (2011), "State-of-the-art Disk Encryption with Comodo" [Online]. Available: <http://www.brighthub.com/computing/ /reviews/53760.aspx>
- [7] (2013), Symantec Website, [Online]. Available: <http://www.symantec.com/drive-encryption/trialware>
- [8] (2013), Cryptomathic File2File website [Online]. Available: <http://cryptomathic-file2file.apponic.com/>