IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A NOVEL TECHNICAL APPROACH TO DRIVE ENCRYPTION TOOLS WITH THEIR WORKING AND COMPARATIVE ANALYSIS FOR IMPROVING SECURITY REQUIRED FOR DATA

1st Dr. Rishi Kumar Sharma,2nd Dr. Nitsh Kaushik,3rd Sunil Kushwaha

1st Associate Professor,CSE , 2nd,Professor. SCE, 3rd Assistant Professor. FCE

1st Quantum Univeristy, 2nd Anand International College of Engg, 3rd Poornima Univeristy

1st Roorkee (UK) India, 2nd India,Jaipur (Rajasthan), India , 3rd Jaipur (Rajasthan), India

Abstract—The research below describes how tools protect your holdings in information and data. The tools used in this document are VeraCrypt and BitLocker Drive Encryption, mostly used for drive encryption. These two open-source encryption tools, VeraCrypt and BitLocker Drive Encryption, support Microsoft Windows, Linux, and macOS. The tools use a different set of algorithms in the encryption and the decryption method. In this document, the tools are demonstrated that how they work. The comparative analysis between VeraCrypt and BitLocker Drive Encryption is shown, and which tool provides you enhanced security in the protection of your data.

***Index Terms*—VeraCrypt,Drive Encryption,Data Protection.**

I. INTRODUCTION

The protection of the digital data on the computer hard disk or in the storage devices is considered one of the most important aspects of today's digital world. Trusted computing is considered a better form of protection of system integrity. Many software or applications that store data can benefit from the mechanisms that protect data on a device from being tampered with. To end this type of issue, many software's are there, providing data security by using different encryption methods. Out of many tools available, the two tools opted in this document are VeraCrypt and BitLocker Drive Encryption, considered one of the most trusted and effective tools in the disk encryption processes. VeraCrypt and BitLocker Drive Encryption are open-source tools that support Windows, Linux and macOS. These tools are designed to protect your data using different encryption methods, and the user interface is simple to understand for the end-users. The research aims to demonstrate the VeraCrypt tool and the BitLocker Drive encryption tools and find which tool is more adequate for the end-users. So, they find a tool that provides confidentiality, integrity, and availability (CIA Trade) of the data and which tool provides satisfactory performance. A comparison of the tools is made based on the user interface, performance, and the level of security the tools provide after the encryption of the drives.

LITERATURE REVIEW

Eric Spero at.el demonstrated the tool VeraCrypt that en- crypts disk and partitions and researched issues faced by the user operating the tool during the encryption and the decryption processes, which decreases the product's usability. The solution provided by the authors in the paper is by improving the usability of the tool by better supporting the mental models by making some changes in the functionality description. They conclusion is that the mental model builder (MMB) can provide more accuracy in terms of short text [1]. Michal Kedzoria at.el researched about the security con- cerns related to the tool VeraCrypt on its hidden operating systems. This paper concludes that encryption of the outer vol- ume can contain the information that shows and compromises the hidden data of file. The technique, cross-drive analysis could be used to analyse the deniable file system and provide you with the hidden file or folder [2].

Gareth Knight at.el describes how the tool VeraCrypt drive encryption can be used to encrypt files and folders that stores your personal and sensitive files from the prying eyes, and told about the encryption and the decryption process of the tool and about the encryption it uses [3].

Jesse D. Kornblum at.el describe how BitLocker Drive Encryption can be operated. In particular, they described how the key management system of the tool, modes and algorithms used, and the metadata format. The attention is mainly given to forensic examiners' methods to access the protected data [4].

Stephen G. Lewis at.el demonstrate how BitLocker Drive Encryption can be proven cost-effective in a large institution where 2900 systems are used. The document describes how reliable and secures they found the tool. They also advised other institutions to use the BitLocker Drive Encryption for cost-effectiveness and a safer hand [5].

Chang Ten at.el demonstrates the security check of the BitLocker Drive Encryption and found a difficult time the Core Key in BitLocker is the decryption process of the encrypted VMK in terms of system and non-system partition encryption [6].

EXPERIMENT WORK

A. *BITLOCKER DRIVE ENCRYPTION:*

BitLocker Drive Encryption is a tool used for data pro- tection. In windows it is a preinstalled feature that makes a collaboration with the operating system and saves the system from data thieving or being stolen. In this document, the BitLocker is Demonstrated on the Windows Operating System. When using the tool BitLocker with Trusted Plat- form Module (TPM) version, 1.2 or later, BitLocker Drive Encryption provides the best protection for using the Windows operating system. Before protecting the system, BitLocker Drive Encryption first checks for all the system requirements with the BIOS, Boot Loader, Kernel, User Apps concerning the Trusted Platform Module (TPM). The encryption process in BitLocker uses three encryption keys the Full Volume Encryption Key (FVEK), Volume Master Key (VMK), and the Root Key after all the keys are matched correctly, and the data is encrypted/decrypted. The permission and decryption process of the BitLocker Drive Encryption is displayed in Figure 1 [8].

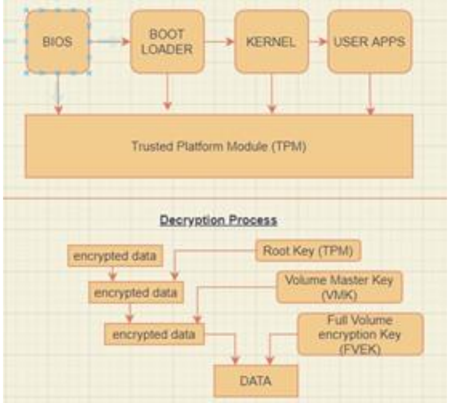
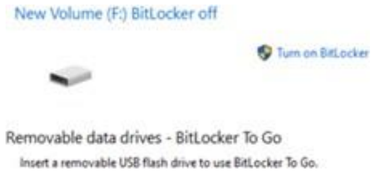


Fig. 1. BitLocker Permissions and Decryption

Processes-: Click on the start menu, go to the Control Panel, go to the System and Security, and then go to BitLocker Drive Encryption. After entering the BitLocker Drive Encryption go to the drive volume, you want to encrypt using the BitLocker. Click on Turn on BitLocker, and then the tool will appear demanding the password you need to set to unlock the drive. Then the tool will prompt you for the back up and recovery key in four formats Save to Microsoft account, save to USB flash drive, save to file, Print the recovery key. In the procedure Save to a file option is chosen


New Volume (F:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Fig. 2. BitLocker View in Windows

After clicking on the next, select the path for the BitLocker recovery key to be stored, then click on open.

Now, choose what space in your drive you want to encrypt. You have two options encrypt used disk space only and encrypt entire drive. In this option encrypt entire drive is chosen.

Now select encryption mode to use. In this, the compatible mode is chosen as the encryption mode.

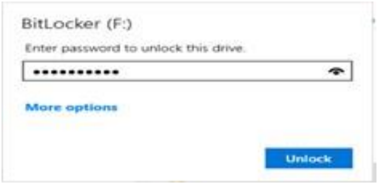
Then it will prompt you that are you ready to encrypt device?

Select the Start encrypting option, and encryption process will start. After the encryption process will complete, click on close.

Now, restart the device. As the device will start the drive that you have selected for the encryption, in our case, the F drive will be displayed with a lock on the drive depicting the drive is encrypted.

Fig. 3. Encrypted Drive

When you double click the drive, it will prompt you for the password.


BitLocker (F:)

Enter password to unlock this drive.

•••••••••••

Fig. 4. BitLocker Demanding Password

Click on unlock, and as the password matches correct, the drive will get unlocked.

New Volume (F:)

1.98 GB free of 1.99 GB

Fig. 5. Decrypted Drive

B. ***VeraCrypt :***

An open-source utility tool used for the virtual encryption of the drive. The VeraCrypt tool creates an encrypted virtual disk that function like a regular drive but stores itself within a file. The tool can encrypt the entire portion or the entire storage device. VeraCrypt is the updated version of the discon- tinued tool TrueCrypt project. The algorithms used to encrypt files in VeraCrypt are AES, Camellia, Kuznyechik, Serpent, etc. VeraCrypt also uses RIPEMD-160, SHA-256, SHA-512, Whirlpool, Streebog as their hash functions [9].

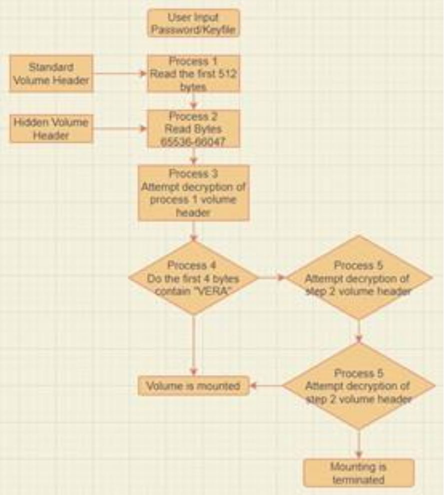

User Input Password/Keyfile
Standard Volume Header
Process 1 Read the first 512 bytes
Hidden Volume Header
Process 2 Read Bytes 65536-66047
Process 3 Attempt decryption of process 1 volume header
Process 4 Do the first 4 bytes contain "VERA"
Process 5 Attempt decryption of step 2 volume header
Volume is mounted
Process 5 Attempt decryption of step 2 volume header
Mounting is terminated

Fig. 6. Decrypting Processes of VeraCrypt

Processes-: Download and install the VeraCrypt Disk En- cryption tool and then open it [7].

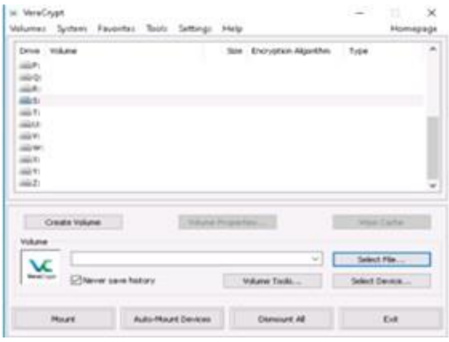


Fig. 7. First Look of VeraCrypt

When you open the VeraCrypt tool, it looks like fig 7. Then you have to click the option that displays Select File.

Then VeraCrypt Volume Creation page will display. Click on create an encrypted file container and click next.

Now select the volume type as Standard VeraCrypt volume and click next.

Now select the location where you want to keep the file. The file will work as a container to our virtual drive that we will access through VeraCrypt.

Now select the type of encryption you want. In this case, I have selected the AES encryption type and clicked next.

Now the VeraCrypt will prompt you for the Volume Pass- word. Set the password according to you, and then click Next.

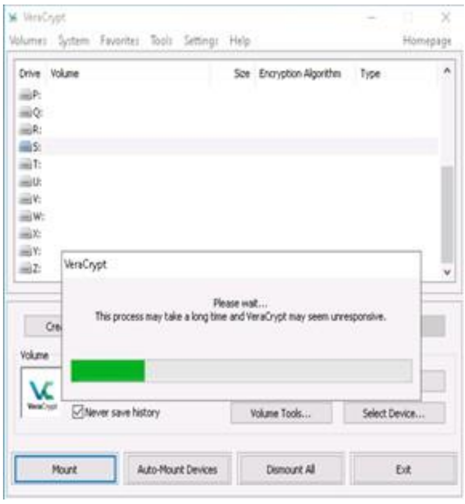
Now the tool will format the file. After formatting the file, it will make a full container for the virtual hard drive. Click on the format.

Now your volume is created, click on exit.

Now multiple drives with the drive names can be seen. Select any drive and click Select File.

Select the file container that has been made with our tool VeraCrypt and click on open.

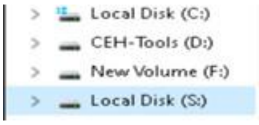
Now click on the Mount button. It will prompt you for the password you gave to the tool earlier at creating the file container and then click OK



VeraCrypt

Please wait...
This process may take a long time and VeraCrypt may seem unresponsive.

Fig. 8. Mounting the file

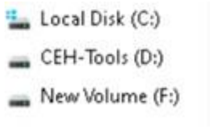


Local Disk (C:)
CEH-Tools (D:)
New Volume (F:)
Local Disk (S:)

Fig. 9. Virtual Drive (S:)

After completing the mounting process, it can be seen that our virtual drive (S:) can be seen in our This PC, now we can upload data into the drive.

After completely updating the data into the file container, we can now hide the data by clicking on the dismount. The data is hidden into the file, and the drive can no longer be seen.



Local Disk (C:)
CEH-Tools (D:)
New Volume (F:)

Fig. 10. Drive (S:) is hidden

RESULT:

In this document, it is noticed that both the tools work completely fine with the Windows Operating System. Both the tools BitLocker and VeraCrypt work on the encryption on the drive but processes completely differently. BitLocker Drive Encryption encrypts the drive and is a preinstalled feature of the Windows OS, whereas, in VeraCrypt, you have to download and install the tool. The tools have successfully encrypted the drive, and the encryption works completely fine even when you restart the device. The data’s confidentiality, integrity, and availability after the decryption process remain the same as when encrypting the data.

CONCLUSION:

In the research, the demonstration of both the tools is displayed. In the comparative analysis, both the tools are tested by performing the encryption and decryption process. BitLocker Drive Encryption and VeraCrypt use encryption techniques to encrypt the drive. BitLocker Drive Encryption uses the Advanced Encryption Standard algorithm to encrypt and decrypt the drive. The VeraCrypt, by default, provides you with various encryption algorithms like Serpent, Twofish, Camellia, Kuznyechik and the Advanced Encryption Algorithm. After the drive's encryption in the BitLocker Drive Encryption, the encrypted drive can be seen with a lock sign in This pc, as shown in fig.3. So, if an attacker somehow gains control of the device, it is purely visible that some important files are kept in the drive as it is locked. An attacker then can try using multiple techniques to decrypt a drive, such as John the Ripper tool, because an attacker gets a region to search for the important data as it is visible that the drive is locked. Whereas is VeraCrypt, the tool makes a file as the container that can be booted using a virtual drive and the password provided by the user. The data can be read by mounting the file container that the user creates, and as the user dismounts the file from the virtual hard drive, the drive is no longer visible to anyone until it is mounted again. So, the VeraCrypt tool adds an extra layer of protection to the data by making it disappear and storing it into a file. If an attacker attacks the device, the attacker does not have a particular region to search for as the data is hidden. After this research, the researchers concluded that the tool VeraCrypt provides an extra layer of protection to the encrypted data. After the encryption, it hides the encrypted data by mounting the container with a virtual hard drive.

REFERENCES

[1] Kornblum, J. (2009). Implementing BitLocker Drive Encryption for forensics analysis.Digital Investigation,5(3-4), 75-84.

[2] Kedziora, M., Chow, Y., Susilo, W. (2017). Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems.Applications And Techniques In Information Security.

[3] Knight, G. (2017). Encrypt data using VeraCrypt. Retrieved 21 February 2022, from https://www.researchgate.net/publication/316235032 Encrypt data using VeraCrypt

[4] Lewis, S., Palumbo, T. (2018). BitLocker Full-Disk Encryption. Pro- ceedings Of The 2018 ACM SIGUCCS Annual Conference.

[5] Spero, E., Stojmenovic´, M., Biddle, R. (2019). Helping Users Secure Their Data by Supporting Mental Models of VeraCrypt. Communications In Computer And Information Science, 211-218.

[6] HOFFMAN, C. (2019). Howtogeek.com. Retrieved 21 February 2022, from https://www.howtogeek.com/howto/6169/use-truecrypt-to- secure-your-data/: :text=Once

[7] Tan, C., Zhang, L., Bao, L. (2020). A Deep Exploration of BitLocker Encryption and Security Analysis. 2020 IEEE 20Th International Con- ference On Communication Technology (ICCT).

[8] Huculak, M. (2021). Setting up BitLocker Drive Encryption on Windows 10. Windows Central. Retrieved 21 February 2022, from https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10 .

[9] VeraCrypt - Wikipedia. En.wikipedia.org. (2022). Retrieved 21 February 2022, from https://en.wikipedia.org/wiki/VeraCrypt .