TrueCrypt LAB

LAB 10

Josiah Smythe

April 15, 2019

Dr. Lehrfeld -Information Security and Assurance

East Tennessee State University

1. Purpose

This exercise will develop an understanding of encrypting as is done on hard drives and directories. This process will exemplify the convenience and simplicity of encryption and allow

2. Materials

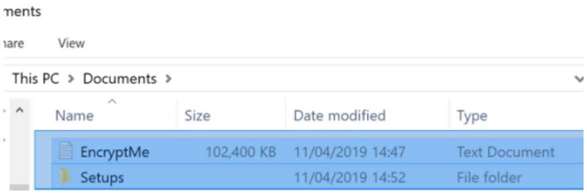
This lab was completed within the virtual machine environment Windows 10 Consumer. This system was running in the virtual machine hosting application VMware Fusion Professional, Version 11.0.2. VMware Fusion was being supported by Mac OS Mojave on a MacBook Pro 2015 15” with 16 GB of DDR3 Ram and an Intel i7-4770HQ running 2.2GHz. The procedures implemented in this project were completed according to the instructions in the document “TrueCrypt - Lab.dox” provided by Prof. Lehrfeld and was also supported by personal class notes.

3. Procedures and Results

This process of implementing the encryption software TrueCrypt was done within a Windows 10 system because of compatibility and performance. To initialize this evaluation the application TrueCrypt installer was downloaded from the internet via Google Chrome on the Windows 10 system. The application was installed with the default settings.

To begin practicing encrypting TrueCrypt was open and the Create Volume button was selected. An encrypted file container was created and the encryption was the standard TrueCrypt. The next step taken was to create a file to encrypt and it was named, “EncryptMe.txt” and it was stored in the document’s directory. This file was then selected to continue the volume creation steps taken earlier. The file size for the volume was set to one-hundred megabytes. A password was created for the file encryption and then it was formatted. To utilize the encryption of this file it must be mounted to the system to allow access to its files. When mounting the file, it will request the password set in the first step of creating the encrypted file to be entered. After successfully mounting the drive there is now another drive of label Z in the This PC directory.

With the file mounted a test was done two exemplify the encryption capability. This was done by copying a folder of desktop wallpapers into the file. After copying the files into the drive, it was dismounted. The encrypted file was examined, and it was discovered that the size of the file was 102MB. Then the file was again mounted, and all the wallpapers were removed and then it was dismounted again. After cleaning out the directory the discovery was made that the size of the file remained consistent regardless of files being added or removed from the directory. Image #1 shows the size of the file and provides an explanation for the files unchanging state.



Name	Size	Date modified	Type
EncryptMe	102,400 KB	11/04/2019 14:47	Text Document
Setups		11/04/2019 14:52	File folder

EncryptMe.txt size, Image #1

After completing this evaluation of the text file encryption another experiment was performed with a virtual hard drive. To do this an external hard drive was simulated using the VM software and the hard drive created was set to 1GB in size. This drive was stored in the same folder as the Windows 10 Virtual machine system. Then the application computer management was launched to view and initialize the unmounted hard drive. When formatting the hard drive, the drive letter was set to E and the format was NTFS.

With the new drive initialized and formatted it was time to implement the encryption. This was done by closing out of the computer management application and launching the TrueCrypt application. Within the application "Create Volume" button was selected and that opened the Volume Creation Wizard. The option of Encrypt a non-system partition/drive was selected from the first set of encryption choices. The standard TrueCrypt option was selected for encryption then the drive was created by encrypting and formatting it. The encryption algorithm selected was AES and the hash algorithm was RIPEMD-160. Then a password was set and the drive was formatted and encrypted according to all the previously configured settings. This drive was now able to be opened and files added to it and then dismounted via TrueCrypt to protect them.

4. Observations

This encryption tool supports three different types of encryption algorithms and they are AES, Serpent, and Twofish. AES (Advanced Encryption Standard) is based on a fixed block size of 128 bits and it operates on a four by four column table. This is a common encryption standard that the other two algorithms fall into. Extending from AES is Serpent which is similar in many respects but has several advantages one of which is the ability to run thirty-two processes of the same four by four table for the algorithm. And the last encryption type supported by TrueCrypt is Twofish. This protocol also extends from the AES protocol but differs from the other two cited because it uses pre-computed s-boxes along with a complex key schedule.

A hidden volume in TrueCrypt is a directory that is concealed by utilizing the empty space in a TrueCrypt drive. The reason that this is so hidden is because after mounting the other encrypted drive it is impossible to see whether the extra space is storing hidden data because when TrueCrypt encrypts a drive it randomizes the extra space, therefore making it impossible to view the hidden drive.

TrueCrypt offers the ability to encrypt a vast number of different media types. This is because it's encryption can be applied to a drive that is storing many different kinds of data. TrueCrypt can therefor encrypt many different media types via its drive encryption methods.

The TrueCrypt application does not provide any way of recovering a lost password. If a back door was installed into this software, it would be a vulnerability in the security of the data being encrypted because it would allow for hackers to infiltrate the data.

Although TrueCrypt is intuitive and simple to use for a computer competent individual it would not be for a non-computer savvy user. Dealing with mounting and dismounting hard drives along with formatting and understanding different encryption algorithms is too complex for an average individual. If TrueCrypt was able to be utilized like BitLocker it would be simple enough for anyone to use, but as of now, that is not the case.

The warning that TrueCrypt is insecure is coming from the concern that the open source software may have hacked and that a Trojan was inserted. Christopher White for Neowin.net considers this warning and considers the expressed concerns on the issue. He states "the tool is now considered insecure as it 'may contain unfixed security issues.'" (White 1) This clarifies that the perceived threat lies in the new discovery of possible security issues.

5. References

Wikipedia, TrueCrypt, Web January 9, 2019, accessed April 16, 2019.
https://en.wikipedia.org/wiki/TrueCrypt

Andrew Y, *Hidden Volume*, Web accessed April 16, 2019.
https://andryou.com/truecrypt/docs/hidden-volume.php

White, Christopher. TrueCrypt is saying it's insecure, recommends using BitLocker. Neowin, Web