Forensic Recovery of Fully Encrypted Volume

Saravanan M
PG Scholar
Information Security and Computer Forensics
SRM University, India

Mukesh Krishnan M B
Assistant Professor
Department of Information Technology
SRM University, India

ABSTRACT

This paper is aimed at analyzing the efficiency of decrypting the bit locked volumes in PIN only mode. Based on the findings this paper considers the issue of decrypting the bit locked volumes in PIN only mode. The main drawback of the full volume encryption application is that it leaves several copies of the key used for encrypting the drive in the physical memory. This paper deals with the recovery of encryption key from the physical memory in case of live system. It also suggests offline methods for collecting the cryptographic keys required for decrypting the volume.

General Terms

Disk security, Memory forensics, Full volume encryption

Keywords

Bit locker, Physical memory forensics, Password, Meta data, Brute Force.

1. INTRODUCTION

A volume or a drive which is secured against theft of data is generally called a fully encrypted volume. Although numerous applications are available to perform full volume encryption, their effectiveness is at stake. Bit locker, a product of windows aimed at securing the drive proved to be a fitting solution. It gives an equal opportunity for perpetrators to commit crimes and leave the scene by encrypting the volume giving a tough task for the investigator to examine the drive to confirm the incident. Bit locker, available in the latest versions of windows operating system enables the user to encrypt any volume in the computer [1]. There are three possible modes using which bit locker can be configured.

1. TPM (Trusted Platform Module) mode of the bit locker allows it to encrypt the drive and to store a token like key file inside the TPM chip. Each time when the system boots, it decrypts the drive by accessing the token from the TPM chip. It mainly protects the drive from network based attacks. Any changes in the computer's environment, moves the system to recovery mode where the user needs to enter the bit locker recovery key to decrypt the drive and boot the system. This mode is not widely used since it requires TPM chip to be attached to the motherboard of the system. Only few computer manufacturers produce systems with inbuilt TPM chip in it.

2. USB mode of bit locker needs an empty USB drive to be inserted at the time of configuration. Bit locker generates file, which resembles a token to the USB drive and the user needs to click this token file to access the data present in the bit locked volume. Although this mode is efficient, it requires a dedicated USB drive for configuration and most computers in organizations and educational institutions protect systems from using USB flash drives. Also, it is a time consuming mode of bit locker since the user needs to insert the USB drive to access the encrypted volume.

3. PIN only mode helps the user to configure bit locker on a drive either by using a password or by using a smart card provided with a smart card reader attached to the computer or by using both. Most users prefer to use bit locker with password to protect their drives from theft of data.

Bit locker encrypts the drive at the file system level. Whenever a drive is encrypted using bit locker, it changes the underlying file system to Full Volume Encryption File system irrespective of the file system. Bit locker encrypts all the user data, slack space, system files and unallocated spaces. It is even possible to encrypt the drive on which the operating system is installed. It encrypts almost everything on the operating systems drive except the files which are required for the system start-up. Bit locker uses Advanced Encryption Standard [3] in cipher block chaining (CBC) mode with elephant diffuser algorithm for encryption and decryption of the drives. 128 bit diffuser algorithm is used to protect the system from chosen cipher text attacks. Since bit locker uses AES encryption it is a real challenge for the forensic investigator to examine the suspect's system if it is protected with bit locker. To unlock the drive, investigator has to ask the user to reveal the password. In case, if the user is the real criminal then the only way to recover the information present in the drive is to forensically retrieve the encryption key. By default bit locker uses 128-bit AES with elephant diffuser algorithm. It also allows the user to select the key size through bit locker management. When a file is sent to the bit locked volume, it automatically encrypts the file and when it is sent out of the drive, it decrypts the file automatically.

2. RELATED WORK

Bit locking a removable file in windows7 generates a text file [6] for recovery purpose, in case if the user forgets the password. The recovery text file can be saved to any other drive in the computer or it can be printed. This text file contains a recovery key identification and the 48-digit recovery key. The key identification is used to identify the 48-digit recovery key. This key can be used to unlock the drive in case of forgotten password or when the removable drive is used in other than the bit locker configured computer. When the removable drive is used in other system, it shows the first part of the recovery key identification and asks the user to type the corresponding 48-digit recovery key. Past researches on bit locked showed the methods to unlock the bit locked drive when it is configured using USB-only mode. Once a removable media is encrypted using bit locker with a password, investigator can look for three things mentioned below to unlock the drive:

1. Password
2. Recovery key
3. .BEK file/.txt file

.BEK represents bit locker external key file. Bit locker encryption creates a hidden read only .BEK/txt file in the physical memory of the system. Sometimes it creates a hidden read only text file which contains bit locker recovery key. Both BEK file and text files are used to unlock the bit locked volume. Using command line commands bit locked volume can be unlocked and using GUI operation, the drive can be decrypted.

3. METHODOLOGY

Forensic analysis of a bit locked drive depends on the status of the system. Investigator can choose any one of the following methods based on the system status, to unlock the bit locked volume.

1. Live analysis
2. Offline analysis
3. Brute force attack

Hardware

- Desktop PC- forensic workstation
- USB Flash Drive

Software

- Microsoft Windows 7 Ultimate version
- Dump It
- Win Hex
- HxD Analysis of forensic images

3.1 Live Analysis

Live analysis involves acquisition of physical memory dump to look for the evidence. If the system is in the live state after bit locker configuration, investigator can dump the physical memory and analyze it. When the bit locker is turned on using the password, operating system writes encrypted copies of VMK (Volume Master Key) and FVEK (Full Volume Encryption Key). VMK can decrypt the FVEK and FVEK in turn can decrypt the entire drive. BEK file contains GUID and the last 32 bytes in the BEK file contains recovery key which can decrypt the FVEK. Sometimes the operating system writes the clear key and sometimes the encrypted key. Physical memory of a windows machine can be dumped using tools like dump it, win32, dd etc. Once the memory is dumped, hex viewer is used to view the byte codes, Unicode strings, and file identifiers from the RAM image. Existence of bit locker traces can be identified by searching the keyword ‘External Key’ in the raw image. This keyword search gives the location of the BEK file inside the memory dump. The exact name of .BEK file may exist below the keyword ‘External Key’ in the file identifier section of the hex viewer. The current research has shown the following name,

0DAFC714-B799-4B2F-A356C56FA5FEE58D

The above name with .BEK/txt extension can be used to unlock the bit locked drive using the below command in the command prompt:

```
Manage-bde –unlock f: -RecoveryKey filename.BEK
```

Eg: Manage-bde –unlock f: -3F800DA0-0B7F-4095-BC41-F3248DA0E90C.bek

If the BEK file is not available readily, proper grouping of bytes can be done to find the exact name of the file. Location of Meta data of the bit locked drive inside the memory dump [7] can be found by using string search with the signature ‘-fve-fs’. Search for .BEK or, txt file with the key inside the Meta data and at the file identifier section. Extract the .BEK or .txt file from the memory image using software like Volatility (Memory Analyzer) to know more about the size and structure of BEK file and the recovery key. It is commonly believed that the windows operating system erases all the contents from physical memory once the power is switched off. But the contents stored in the registers disappear only when the temperature increases. If the room temperature is maintained below the actual temperature, the RAM contents like cryptographic keys will exist for hours even after the device is switched off.

3.2 Offline Analysis

Traditional offline analysis involves collection of evidence from the storage media [2]. Since bit locker changes the file system to Full Volume Encryption file system, it is essential to use a software application that supports FVE file system. Currently there are no software applications for full volume encryption file system. If the live forensic method does not reveal any forensically sound evidence then the investigator has to create software to read and mount the disk image to other drive for analysis. Mounted disk image is analyzed to find the traces of bit locker key file. Another method is to use disk decryptor which is capable of mounting the bit locked volume to forensic workstation. Mounted disk image is viewed using hex viewers to view the sector wise storage of files inside the storage media. True back is a tool using which bit locked drive can be mounted and the Meta data can be viewed which gives the logical structure of files and storage areas. Sometimes executing the below command [5] may reveal the exact name of the .BEK/txt file in the command prompt:

```
Manage-bde –protectors –get f:
```

If the exact name of the BEK file is found it can be used to unlock the volume by using the command mentioned in the section 1.1

Extract BEK/txt file from the Meta data of bit locked drive can be extracted using memory analyzer tools. Once it is unlocked, the drive can be decrypted using windows GUI options in the control panel.

3.3 Brute Force Attack

If both the live and offline analysis fails i.e. if they do not reveal any information about the bit locker recovery key then the only way to unlock the drive is done by using brute force attack. Bit locker allows user to make several number of wrong attempts while typing the recovery key. As discussed in the previous sections, bit locker recovery key is actually a 48-digit number [4] which is divided into 8 groups of 6 digit numbers. Also it is observed that each 6 digit number is divisible by 11. Each 6 digit number must be less than 720,896, or (2 ^ 16) * 11. Using this information all the 6 digit numbers which are divisible by 11 and less than 720,896 are identified.

E.g.: 176660-669900-117491-029909-201256-610588-533753-623271

The 6 digit numbers which satisfies the above conditions are fed as input to an array. Using combinations, below mentioned algorithm generates the possible bit locker recovery keys. Though there are millions of possible keys are generated by this algorithm for brute force attack, it is the only way to unlock the bit locked drive since it is not possible to break the AES encryption used by bit locker. Time consumption in testing each possible key manually may be reduced by automating the key checking process using super computers. Super computers can test each key by automatically typing the key in the corresponding recovery key box. Any one of the recovery keys generated by this algorithm will definitely unlock the bit locker and thereby allows the investigator to access the disk data.

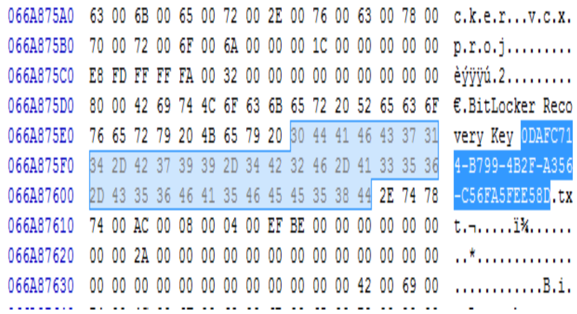
```
Start
Initialize arr[] -> i/p array
      data[] -> temp array
       start  -> starting index
       end    -> ending index
       index -> current index in temp array
       r       ->size of combination
  for(i=start;i<=end;i++)
      data[index]=arr[index]
      repeat
            if (index==r)
                  print current combination
                  replace index with all possible elements
                  print combinations by changing one element
                  at a time till the end of loop
end
```

Fig 1 Algorithm

This algorithm helps in identifying the possible combinations of strings which can be used to decrypt the bit locked volumes. Essentially the input to this module should be drafted from an another procedure which generates the possible strings of size 6 which are divisible by 11 as it is the pattern found during internal analysis of bit locker recovery keys.

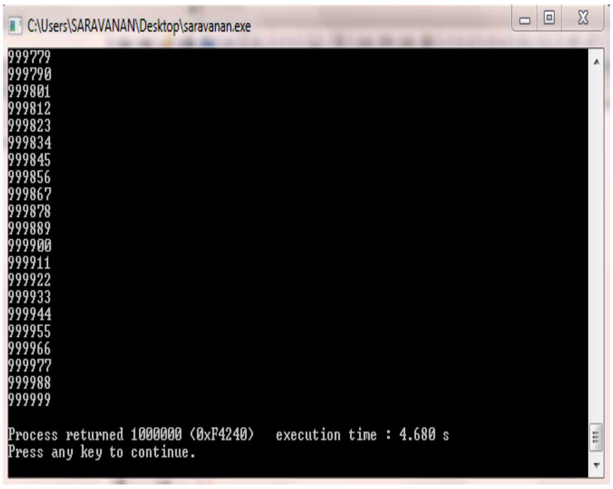
4. RESULTS

After thorough analysis of bit locked volumes in all the two modes it has been observed that recovering the drive information is accurate in live system analysis. Though analyzing the drive in offline mode is essential, it poses quite a big challenge for the forensic examiners. However, the performing a brute force attack using the above mentioned methodologies this paper addresses the issue of recovering the key in PIN-only mode.



```
066A875A0  63 00 6B 00 65 00 72 00 2E 00 76 00 63 00 78 00  c.k.e.r...v.c.x.
066A875B0  70 00 72 00 6F 00 6A 00 00 00 1C 00 00 00 00 00  p.r.o.j.........
066A875C0  E8 FD FF FF FA 00 32 00 00 00 00 00 00 00 00 00  èýÿÿú.2.........
066A875D0  80 00 42 69 74 4C 6F 63 6B 65 72 20 52 65 63 6F  €.BitLocker Reco
066A875E0  76 65 72 79 20 4B 65 79 20 30 44 41 46 43 37 31  very Key 0DAFC71
066A875F0  34 2D 42 37 39 39 2D 34 42 32 46 2D 41 33 35 36  4-B799-4B2F-A356
066A87600  2D 43 35 36 46 41 35 46 45 45 35 38 44 2E 74 78  -C56FA5FEE58D.tx
066A87610  74 00 AC 00 08 00 04 00 EF BE 00 00 00 00 00 00  t.¬.....ï¾......
066A87620  00 00 2A 00 00 00 00 00 00 00 00 00 00 00 00 00  ..*.............
066A87630  00 00 00 00 00 00 00 00 00 00 00 00 42 00 69 00  ............B.i.
```

Fig 2: Recovered text files from image

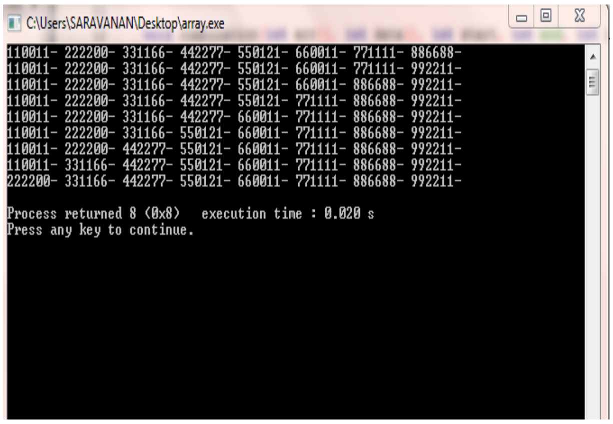


C:\Users\SARAVANAN\Desktop\saravanan.exe

```
999779
999790
999801
999812
999823
999834
999845
999856
999867
999878
999889
999900
999911
999922
999933
999944
999955
999966
999977
999988
999999

Process returned 1000000 (0xF4240)   execution time : 4.680 s
Press any key to continue.
```

Fig 3 Generating strings



C:\Users\SARAVANAN\Desktop\array.exe

```
110011- 222200- 331166- 442277- 550121- 660011- 771111- 886688-
110011- 222200- 331166- 442277- 550121- 660011- 771111- 992211-
110011- 222200- 331166- 442277- 550121- 660011- 886688- 992211-
110011- 222200- 331166- 442277- 550121- 771111- 886688- 992211-
110011- 222200- 331166- 442277- 660011- 771111- 886688- 992211-
110011- 222200- 331166- 550121- 660011- 771111- 886688- 992211-
110011- 222200- 442277- 550121- 660011- 771111- 886688- 992211-
110011- 331166- 442277- 550121- 660011- 771111- 886688- 992211-
222200- 331166- 442277- 550121- 660011- 771111- 886688- 992211-

Process returned 8 (0x8)   execution time : 0.020 s
Press any key to continue.
```

Fig 4 Brute Force attack

5. FUTURE WORKS

Bit locker provides multi factor authentication by combining the different modes:

- TPM + PIN
- TPM + PIN + USB Key
- TPM + USB Key

Microsoft has announced that this multi factor authentication improves the security of the application and it is impossible to break the bit locker security by any means [8]. Future work can focus on unlocking the bit locked volume configured with multi factors. Even though it gives multi factor authentication, there may be some traces found inside the RAM and storage Medias which shows the traces of bit locker. It is must for the investigator to formulate new methodologies in order to conduct the investigation.

6. CONCLUSION

Physical memory is the important source for the forensic investigator to collect evidences from the live system and it is considered as the heart of the investigation. Although RAM is a volatile memory, from the detailed study conducted, it is observed that RAM content can be preserved by maintaining the room temperature below the normal. Cold boot attacks are possible by this method which would give forensically sound evidence like cryptographic keys to the investigator. It is also observed that whatever the mode bit locker uses, it is possible to decrypt the drive without knowing the password or key. Though the image of the physical media can be obtained easily, it holds only the encrypted data and it is of no use. If the investigator is not able to get access to the system in the live response scenario then he must realize that it is tough to recover the cryptographic keys from the storage media. Also it is understood that bit locker cannot encrypt the boot volume of the system. The investigator should start with live analysis followed by offline and brute force methods since the criticality and the time consumption increases in this fashion. Brute force method is a time consuming process but when the other two methods fails, investigator has to implement this attack.

7. ACKNOWLEDGMENT

We thank every person who helped us in finishing this work perfectly.

8. REFERENCE

[1] Microsoft Corporation. Bit locker drive encryption technical overview. Technical report, Microsoft Corporation, May 2008. http://technet2microsoft.com/WindowsVista/en/library/ce4d5a2e-59a5-4742-89cc-ef9f5908b4731033. mspx?mfr=true.

[2] Microsoft Corporation. Protect Key with Numerical Password Method of the Win32 Encryptable Volume Class, February 2008. http://msdn.microsoft.com/enus/library/aa376467(VS.85).aspx.

[3] Niels Ferguson. AES-CBC + Elephant diffuser A Disk Encryption Algorithm for Windows Vista. Technical report, Microsoft Corporation, Septem-ber 2006. [4]. J.H. Choi, K.G. Lee, J. Park, C. Lee, and S. Lee, "Analysis framework to detect artifacts of portable web browser," *Center for Information Security Technologies*, 2012.

[4] Microsoft System Integrity Team. Bit locker recovery password details, August 2006. http://blogs.msdn.com/siteam/archive/2006

[5] Microsoft System Integrity Team. De-tecting bit locker, October 2006. http: //blogs.msdn.com/siteam/archive/2006/10/26/detecting-bitlocker.aspx.

[6] Nitin Kumar and Vipin Kumar. Bit locker and Windows Vista, May 2008. http://www.nvlabs. In/node/9.

[7] ManTech International Corporation. ManTech Memory DD, 1.3 editions, August 2008. http: //mdd.sf.net/.

[8] Microsoft Corporation. Bit Locker FIPS Security Policy, 2007.http://csrc.nist.gov/groups/14 STM/cmvp/documents/140-1/140sp/140p947.pdf.