ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Survey on Bitlocker Techniques

Deepika Goyal
Computer Department
National College Bhikhi
Deepika.bhikhi@gmail.com

Abstract— *Bitlocker technology is one of the most popular system used in safety measure of Microsoft Window Operating system. Bitlocker is used to encrypt the Hard Drive of the computer or laptop. Bitlocker is a security mechanism that will protect the sensitive corporate data from attacker with bad intensions. The primary aim of this paper is to discuss the brief overview of Bitlocker technology and its impact on security measure. It also discusses the issues and drawbacks related to using Bitlocker*

Keywords— *Bitlocker, TPM, encrypt, FVEK, VMK, data security*.

I. INTRODUCTION

In present world, Data security and protection is an inevitable aspect. People who works in environments with sensitive corporate data want to protect their data from threats with physical access to the device or disk. Bitlocker is a new security strategy full name of Bitlocker is Bitlocker Driver Encryption release by Microsoft for Windows 7 and subsequent windows platform. Bitlocker is a technique that allow user to encrypt the system drive of the computer[7]. Encrypting data is one of the most effective ways to help keep it secure. Once a system Hard drive is encrypt with a Bitlocker . It secure the computer with a PIN code that require to be given every time the system is started Hard drive data is secure with this PIN and cannot be accessed without this PIN code. In this case if intruder or attacker success in stolen the system cannot read the drive data because without the PIN code data is in unrecognizable form no one can access the data without the decrypt code. Bitlocker stores the data encryption key in a trusted platform module (TPM)

II. BITLOCKER WITH TPM

Bitlocker is designed to make the encrypted drive unrecoverable without the required authentication windows vista Microsoft introduced a new defensive protective feature called Bitlocker Drive Encryption[10] .Windows 7 introduced the Bitlocker to Go for portable storage devices. For windows 10, need to be running the enterprise edition for a best secure result bitlocker must not be setup without TPM. TPM is the standard for a hardware device capable of various cryptographic operations such as secure key generation and random number generation[6]. TPM is a microchip that is located on a motherboard TPM is used to encrypt the hard drive so it is essential to follow some specific TPM operations before start to encrypt the hard drive by using bitlocker.

There are three conditions before starting the encryption operations TPM must be enabled, activated and owned[9]. TPM can be initializing by following the step-wise procedure. User must be logged on to a TPM equipped computer as a super user and follow the steps:

Step1: Turn on the TPM.
Step2: Set the ownership of TPM.

When this process is completed, choose one from two types of bitlocker here:

1. Bitlocker Drive Encryption:-This is a entire disk volume encryption. Bitlocker can encrypt and decrypt disk with a protection key(password)
2. Bitlocker To Go:-This can be used to encrypt the removable drives like USB flash drives or external hard drive.

A. Decryption process with TPM

If computer meets a window TPM requirement, the process for enabling bitlocker is followed. After following the enabling procedure enter a PIN minimum 8 to maximum 48 characters long[7]. Print this PIN or save it on another system. This PIN code must be entered every time when user start the system.

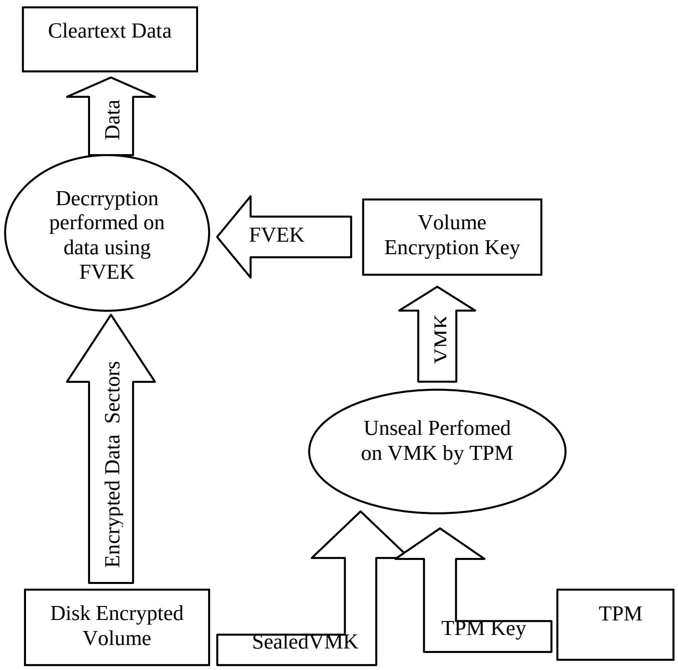

Figure1.Bitlocker enabled volume with TPM [11]

Procedure to enable and disable Bitlocker with TPM

1 step: Enable Bitlocker
2 step: Disk volume is encrypted with FVEK
3 step: FVEK is sealed by VMK
4 step:VMK is sealed by TPM key protecter
5 step:Turn off Bitlocker
6 step:TPM will Unsealed the VMK
7 step:VMK will decrypt the FVEK
8 step:FVEK will decrypt the Disk volume 9step:ClearKey will clear text data

B. Decryption process without TPM

By default Bitlocker security mechanism is configured with TPM. Bitlocker Drive Encryption can be set up with out a TPM but must have a USB Flash Drive with a Startup Key. Bitlocker To Go is use to protect data drive. To enable Bitlocker with out TPM require few settings in Group Editor Policy:-

1.Click start
2.In start search type gpedit.msc
3.Click on Computer Configration/Administrative Templates/Windows Components/Bitlocker Drive Configration
4.click Control Panel/Enable advanced startup options/properties
5.check the box for Allow Bitlocker without compatible TPM.
6.click apply and ok
7.close Local Group Policy Editor
Go back to hard drive and turn on Bitlocker
6.Restart the computer
After restart enter the startup key on Flash Drive.

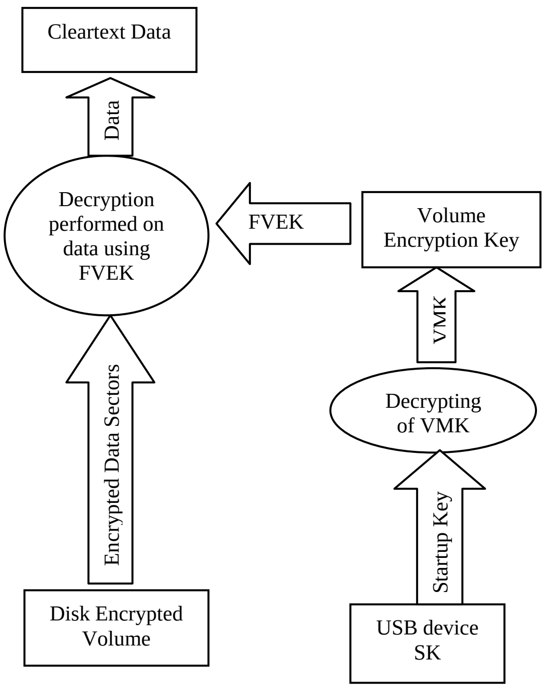

Figure2.Bitlocker enabled volume without TPM [11]

III. Review of literature

1. The author **Hou Rui and Jin Zhi Gang [2014][1]** has discussed about the security of data using Bitlocker on window 7. This paper also discussed the improvement of bitlocker in terms of system security startup but it takes huge time. Further, it can be improved by applying trusted computing method to secure the data which results in minimizing the time and increases the accuracy.
2. The auther **Andrew Woodward [2006]**[2] has discussed about to secure the hard drive of window vista focused to use EFS Encryption File System .User can choose the data file to encrypt on a hard drive. This method saves the time. This support only the two version of window.
3. The author **George Ou [2007][3]** has described the improved EFS and Bitlocker on Window Vista to secure the system drive. EFS are a hig h level security and work after system boot up process. Bitlocker is a low level security and work before the system boot. Combination of EFS with Bitlocker is perfect secure mechnisam
4. The author **Jesse D.Kornblum[2009][4]** described how Bitlocker technique can be used to protect the forensic data. Forensics deal with legal system.According to his research Bitlocker can be used to decrypt the keys protecting the FVEK(Full Volume Encryption Key)

5. The author **Lan Haken[2015][5]** described an attack which defeat the system security in the presence of Bitlocker. Attacker can access the hard drive of system. In following condition if system using Bitlocker without preboot authentication and user has previously logged into the machine. Attacker will set the mock domain and by-pass the system security.

IV. CONCLUSION

Bitlocker is designed to make the encrypted drive unrecoverable without the required authentication. Bitlocker protect the data in case the computer is stolen or lost. Bitlocker stores the encryption key in TPM that performs cryptographic operations. An attacker will not be able to boot the bitlocker enabled system from an alternate system to steal the data. In window 7 to window 10 there are lots of improvement in bitlocker. With fewer drawbacks like time consuming process, risk of forget the recovery key. No data protection against Network attacks and no security when system is on and leave unattended. There is a scope of lots of improvement in using bitlocker. Rather bitlocker might be the best option for average window user to rely on who want to encrypt their disks.

REFERENCES

[1]http://jocpr.com/vol6-iss7-2014/JCPR-2014-6-7-491-497.pdf

[2]https://www.researchgate.net/publication/49281276_BitLocker_-_the_end_of_digital_forensics

[3]http://www.techrepublic.com/article/prevent-data-theft-with-windows-vistas-encrypted-file-system-efs-and-bitlocker/

[4]http://jessekornblum.com/publications/di09.pdf

[5]https://www.researchgate.net/publication/49281276_BitLocker_-_the_end_of_digital_forensics

[6]http://www.eyeonwindows.com/2012/11/11/using-bitlocker-to-protect-your-data-in-windows-8/

[7]http://www.techworld.com/review/encryption/bitlocker-review-3212400/

[8] http://www2.le.ac.uk/offices/ias/topics/computer

[9]http://computer.howstuffworks.com/encryption.h

[10]https://technet.microsoft.com/enus/library/dd548341(v=ws.10).aspx

[11]http://www.microsoft.com/whdc/system/platform/hwsecurity/BitlockerFlow.mspx