USB SECURITY AND MECHANISM TO ENSURE IT

[1]Mavlonov Alisher Bagbekovich, [2]Mavlanov Azizbek Bagbekovich, [3]Mavlonova Shodmonoy Bogbek qizi

[1]PhD student of Urgench State University, mavlonosher@gmail.com

[2]Master student of Urgench Branch of Tashkent university of Information Technologies Named after Muhammad al-Khwarizm

[3]Master student of Urgench Branch of Tashkent university of Information Technologies Named after Muhammad al-Khwarizm

https://doi.org/10.5281/zenodo.7857074

Abstract. *The paper considers aspects of the top risks of using USB devices, practice to protect ourselves from flash drive threats. There are some tips to help using USB device safely.*

Key words: *USB Security, USB drives, Malware, Password, BitLocker, Risk, e-Mail, Information*

INTRODUCTION

Many organizations connect flash drives to critical networks and information systems to transfer and store large amounts of critical information. Also, employees use USB devices to carry sensitive work information when working remotely. Unfortunately, there are numerous USB security risks you should be aware of to prevent flash drives from becoming a danger to your organization.

Many companies expose themselves to many security threats since their USB security programs lack adequate measures to ensure data security. In a recent survey, approximately 58% of organizations lack safe listing and USB port control software for managing flash drive usage. The same survey found that only 47% of businesses require their employees to encrypt data stored in USB drives. Furthermore, 53% of companies lack appropriate controls for detecting and preventing users from downloading sensitive data onto unauthorized USB devices[4].

MATERIALS AND METHODS

While at least 90% of employees worldwide use USB devices for work-related reasons, it is worrying that more than half of companies don't allowlist flash drives or use USB port controls to manage USB connections or encrypt data stored in flash drives[3]. The following are the top risks of using USB devices[1]:

1. Data Loss from Misplaced USB Drives
2. Malware Attacks
3. Risk of Non-Compliance
4. Lack of Acceptable Use Policies
5. Lack of Employee Awareness

In order to stay away from these troubles, it is necessary to make the following habits:

- Always scan USB with latest Antivirus before accessing.
- Protect your USB device with password.
- Encrypt the files on the device.
- Monitor what data is being copied.
- Never keep sensitive information like username/passwords in USB.
- Do not plug-in unknown USB into your computer.

- Maintain separate USB for office and personal use.

RESULTS AND DISCUSSION

The security risks of using flash drives are growing every day, while 79% of USB-based security threats can cause widespread disruption to critical business operations and destruction to operational technology. Therefore, we should adhere to the following recommended practice to protect ourselves from flash drive risks[1].

Setting Password on USB by BitLocker

- Right Click on USB Drive. (Figure 1)
- Click on Turn On BitLocker.
- On the Next Screen it ask the option to unlock USB.
- Select any of the option either Password or smart card.(Figure 3)
- Then ask to encrypt for Used disk or Entire disk and finally click on Start Encrypting.

(Figure 7)

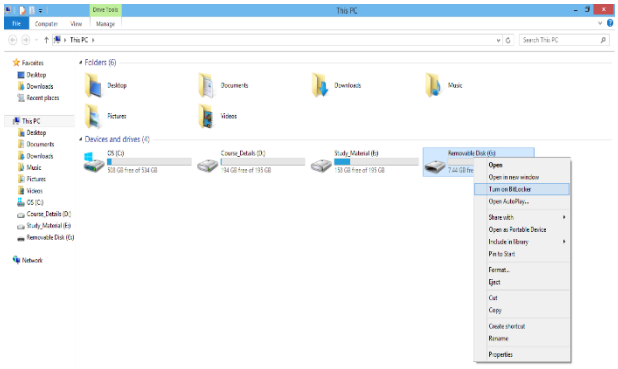

Figure 1

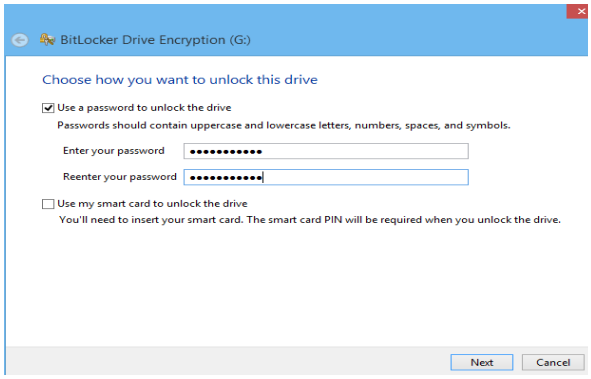

Figure 2

Figure 3

Figure 4

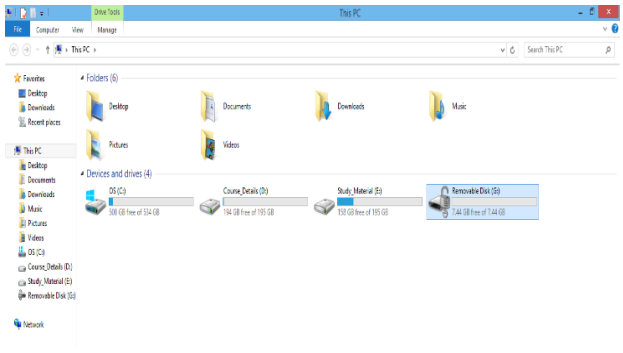

Figure 5

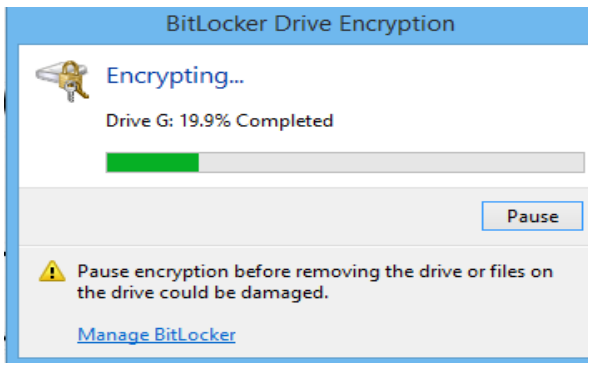

Figure 7

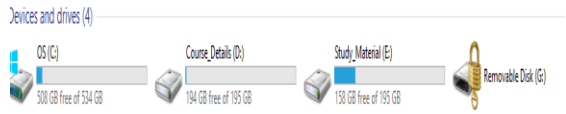

Figure 8

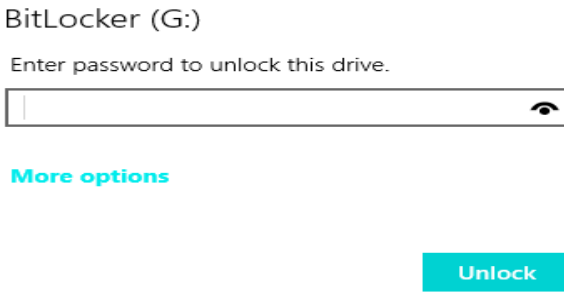

Figure 9

CONCLUSION

The USB flash drive is currently the most popular mobile storage unit because of its many strengths including fast data transfer speed, high portability, and free transfer and deletion. However, serious problems have arisen, such as the inability to protect the internally stored data after the loss of a USB drive, leading to demands for the development of a secure USB flash drive featuring improved security functions. For that reason, new and more secure USB flash drives protect the internally stored data using such security technologies as data encryption/decryption and user authentication and identification. However, the problems of access to the inside of a drive and the leakage of data have been identified in secure USB flash drives installed with the latest security technologies due to such vulnerabilities as implementation and environmental vulnerabilities, unlock command, and reverse engineering. To solve such problems, this paper proposes a safe secure USB flash drive mechanism that does not expose the authentication data. The mechanism overcomes the existing vulnerabilities to protect the data more safely, since it does not store the data needed for user authentication and disk decryption inside the flash drive data and has no routine for comparing the authentication. To analyze the security of the proposed mechanism, the security requirements which the secure USB flash drive must satisfy and an attack technology scenario were deduced. The results of the security assessment confirmed that the proposed mechanism satisfies the confidentiality, integrity, authentication, and access control requirements and safely protects the data from impersonation, man-in-the-middle, resending, and eavesdropping attacks[2].

The following conclusions are also very important to us[1]:

- Since the e-Mail messages are transferred in clear text, it is advisable to use some encryption software like PGP (pretty good privacy) to encrypt email messages before sending, so that it can be decrypted only by the specified recipient only.
- Use Email filtering software to avoid Spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.
- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.

- Avoid sending personal information through e-Mails.
- Avoid filling forms that come via e-Mail asking for your personal information and do not click on links that come via e-Mail.
- Do not click on the e-Mails that you receive from un trusted users as clicking itself may execute some malicious code and spread into your system.

REFERENCES

1. CDAC Noida, "SPECIALISED PROGRAMME ON REDUCING CYBER CRIME THROUGH KNOWLEDGE EXCHANGE AND CAPACITY BUILDING" course materials 13.02-24.03, 2023.
2. O. Insu, Y. Lee, H. Lee, K. Lee, and K. Yim, "Study on secure USB mechanism without exposure of the authentication information," in Proceedings of the International Symposium on Mobile Internet Security (MobiSec), Jeju Island, South Korea, October 2017.
3. A.N. Magdum and Y. M. Patil, "A secure data transfer algorithm for USB mass storage devices to protect documents," International Journal of Emerging Engineering Research and Technology, vol. 2, no. 4, pp. 113–119, 2014.
4. https://blog.pulsarsecurity.com/