Securing of Data on USB Storage

Manasa Yenuga[1], G.Sujatha2, A.Vijay Kumar[3]
[1]M.Tech. Scholar, [2]Assistant Professor
Department of Information Technology, SRM University, Chennai, India
[3]Scientist,ANURAG Laboratory.
[1]manasa21yenuga@gmail.com

***Abstract*— Information security has become an important issue in the field of security. There are various kinds of securities features that are provided to the data. There are also many security risks that are related to the Universal Serial Bus(USB).As USB has become an important media for transferring and storing the data. The USB is very small in size so it is easy carry. But there are many risks that are involved in the USB device. The risks such as data leakage, unauthorized access, tampering of data.The current scope of effort is to mediate access of data present in the USB storage device by implementing a mediating module that facilitates secure access of the data stored in it.When ever user inserts USB drive in the system, automatically this software module will be invoked, gets complete access of the USB drive contents and regulates its access through authentication according to need of specific application. The code which is responsible for accessing the data will be part of the USB drive.**

***Keywords*—USB Memory,USB Bus,Driver,Windows Kernel.**

I. INTRODUCTION

Removable storage media has become an important feature for transferring the data. There are many removable devices such as Pendrive,memory stick, external hard disk,CD,Floppy disk. These devices are mainly used for information exchange. So there is a need to protect the data from malicious attacks and unauthorized access. Now the concentration goes mainly on the USB devices. There are many advantages and disadvantages that are related to the USB.As increasing in the technology the demand of security provided to the data is also increasing. Protecting the sensitive information has become an challenging task.USB memories should be protected. The leakage of personal information and confidential matters leads to many problems. Accordingly, this paper suggests a technique for Securing of USB devices; this can be done by providing authentication to the device, So that whenever user wants to access the device it asks permission[5]. Only the authorized users can only access the data. If the device is lost, the unauthorized user cannot access to device.

This paper is divided into chapters. Chapter 2 shows the approach to solve the security issue related to the USB devices. Chapter 3 describes about the architecture of the proposed method. Finally, Chapter 4 presents the conclusion and future work.

II. APPROACH

For secure access of the USB device, writing a user-mode driver (.dll) that interacts with the system using WinUsb. The system has WinUsb.sys Kernel-mode driver which is used for the interaction of USB devices. For writing the driver Microsoft has provided windows driver tool kit.

When the USB drive is inserted into the system, the system automatically identifies the device and makes the contents available to the user, thus it is serving our purpose. Sometimes the data is modified/altered so the user is worried of the data lost. When the device is inserted the operating system is responsible for handling the data and giving the control to the user[3].

The code that is responsible for handling the data is called as Codebase and it is part of the environment, as the code is part of the operating environment and it is difficult to analyse the code and identify or trace the threat. As operating system handles multiple events at the same time identifying the piece of code that is handling the USB devices is difficult to identify.
So we are making the code as a part of the thumb drive thus it is easy for the analysis and identify the threat.

The objective is to regulate the access by implementing a software module that regulates the USB access. When the drive is inserted the device[4] prints the details of the device. Then sensitize the data access by categorizing data into critical and non-critical on the USB thumb drive.

- critical data (assuming to be less voluminous)
- Non-critical data (assuming to be more voluminous)

For handling or accessing the critical partition, the code will be part of the thumb drive access with authentication[2]. So, for this we are writing a driver which is understandable by the OS and communicates with the device. In windows the communication of the USB device is done using WinUsb function.
Make data access routines as part of the thumb drive itself to regulate the access,Based on authentication more critical and less critical data can be made visible/accessible to the application with controlled operations like read-only. So USB access through authentication with reduced code base offers better security.

Flow of Operations – USB

The typical flow of operations while using USB device is brought out below.

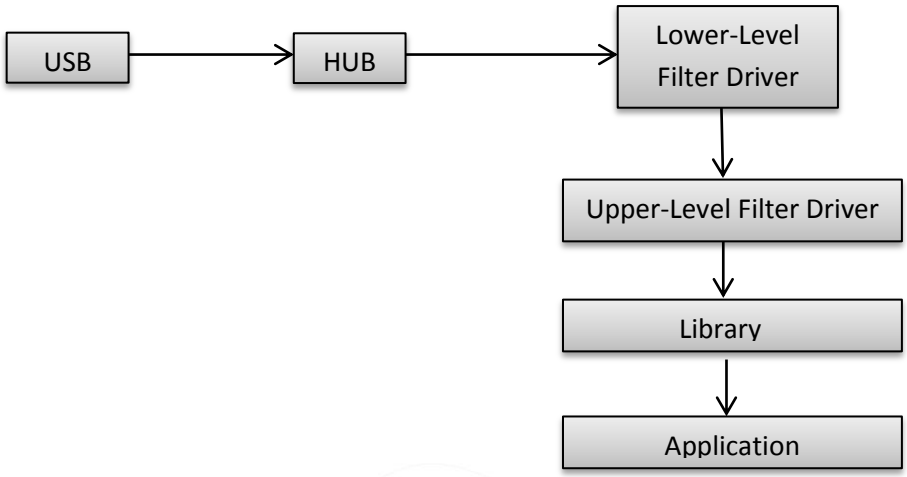

Figure 1.Flow of operation

III.ARCITECTURE OF THE PROPOSED METHOD

USB Control & Communication (User & Kernel Mode)

In windows, when USB device is inserted the device interacts with the hub and identifies the lower level device driver which is nothing but user mode driver. The client driver interacts with the kernel mode driver and the data flow starts.Now in our case we are writing a client driver which is a dll called as Usbsec.dll.This dll interacts with the[2] kernel mode driver and to the application as shown in Fig. 2.This dll will be inside the critical partition or secured data and can access only through authentication. A KMDF or UMDF driver is the software installed on the computer that communicates with the hardware to make the device function. If the device belongs to a device class supported by Microsoft, Windows loads one of the in-box class drivers for the device. Otherwise, a custom driver must be provided by the hardware manufacturer or a third party vendor. The user installs the driver for the device when the device is first detected by Windows. After successful installation, Windows loads the client driver every time the device is attached and unloads the driver when the device is detached from the host computer. Thus our user mode driver will be invoked. The code that is responsible for handling the data in critical partition will be very less so it is easy to evaluate and reduces the code evaluation process so we can provide better security.

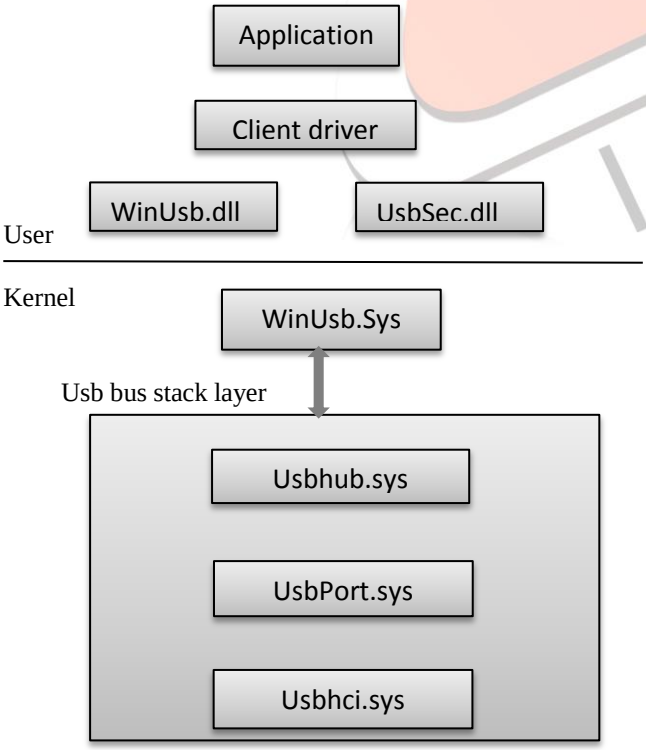

Figure 2. USB Control & Communication

The Fig. 3 describes about the technique that is used for the USB device. Whenever user inserts the device into the system, the software module will be invoked and gets complete access of the device.

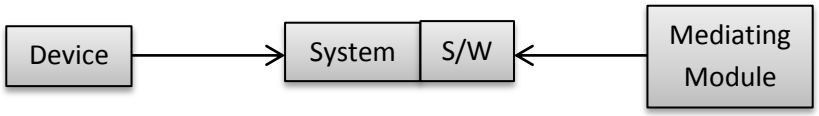

Figure 3.Module invoking mechanism.

How the Module is developed

The step by step process includes:

1. Writing an application that prints details of USB device or device detection.
2. DLL creation for the application that prints details of USB device or detection.
3. Access the partition holding the critical data with password authentication.
4. Encrypt the critical partition with strong encryption algorithm.
5. Integrate the availability of encrypted data with password authentication.
6. The entire code that is responsible for handling this thumb drive is mapped to registry.
7. The code that is to be kept in the thumb drive such as location in windows so that this routine will be invoked.
8. Invoking the code seamlessly with windows 7 systems.

IV.CONCLUSION

The USB Storage device monitoring method was proposed which is based on the driver layer that meets the requirements of majority enterprises, and for the control of USB storage access. The mediating module is developed that facilitates or regulates the USB access and make the contents available to the user.

The study aimed to prevent personal information leakage to attacker when USB memory is lost or stolen to prevent such accidents, a secure USB solution has been released which provides only authenticated users with a security area i.e. Unauthorised users are restricted to access the data. In future, the entire code that is responsible for handling the critical data can be isolated from environment using the virtualization method and this is developed in windows environment the same can be extended to other environment.

REFERENCES

[1] Microsoft Corporation. Microsoft Windows XP Driver Development Kit [EB/ OL]. 2010. http :/ / www. msdn.microsoft.
[2] Anhe Wu, Ming Tai, Hongtao Yu, "Device Driver Development in Windows2000/XP/7 WDM [M], and Version 2" Beijing: Publishing House of Electronics Industry, 2005.
[3] Kaiyuan Fan. “Research on the Data Encryption 0f USB Interface Based on Filter Driver [J]". Information Security, 2009, 04(3): 0102-02.
[4] Hanjae Jeong, Younsung Choi, Woongryel Jeon, Fei Yang, Yunho Lee, Seungjoo Kim, and Dongho Won, "Vulnerability Analysis of Secure USB Flash Drives".
[5] Trusted Computing Group (TCG), “TPM main specification,” Trusted Computing Group, Main Specification, May 2009.