Blocking USB Drive from Virus Using Filtering Techniques

Mr. Ranjith M
Computer Science & Eng.
Jain University

Mr. Manjunath C R
Computer Science & Eng.
Jain University

Mr. Prasanna Kumar C
Electrical & Electronics Eng.
Jain University

Abstract*— USB disk are very useful portable storage devices which are very commonly used for transporting computer data from one computer to another. The USB flash disk may be a good choice for its convenience and low cost. However, it is also very difficult to guarantee that the USB flash disk is safe and clean absolutely. With the wide use of the flash memory, the USB flash disk has become a new carrier in the spread of computer viruses which may be a disaster to a computer. The percentage of the flash drive being infected by viruses has also increased. Once plug a virus-infected drive in any system, the system will be spreading virus. To overcome this problem, the filtering technique will be using while writing the files entering into the USB drive. The signature based detection is used to match the strings which are encrypted by MD5 algorithm. Based on this, the method is going to detect the infected files. Arduino UNO microcontroller is used to lock and unlock the USB flash disks which are written the in Arduino UNO IDE (Integrated Development Environment).By providing the enable or disable the read and write modes for the USB drive. An access control model for USB storage device. Hereby, this approach is an attempt is to tried with set of defined virus. The system can block, if observed virus is detected.
Keywords: filtering technique, read, write, block

I. INTRODUCTION

In recent days the USB drive has become the best device for storing the data, however the data stored in the drive has to be protected from viruses when connected to any computer system. Nowadays, most of the peripheral devices are connected to computers via USB. There are many software applications (anti-virus programs) to ensure the virus that being attack into the system. It has more effective depends on how effectively works and updates the program in the system. These preventing software applications (anti-virus programs) are works inside the system. It will help in killing (delete) and quarantine the virus without infecting the system. It will manage the virus files are entering into the system without affecting the current system. For this scenario, the process of virus is to affect the system and hard drives with their own manner by the attacker.

Currently, we are using the different antivirus programs to protect our PCs and laptops from virus. Attacker will spread virus in any format and in many ways, effectively through Internet and Internet applications that we used while browsing. Nowadays, USB drives are effectively used in the real world business and other purpose for storing and sharing the information (private) or any documents which need to be saved. In case that, USB drive is one the most dangerous in spreading of virus to other systems and network connected systems. Even though, the researchers are invented virus program to avoid in spreading of viruses through USB drives. But in case of vice-versa not applicable present now. So am planning to avoid the USB drives from the viruses using filter techniques. By providing read and write enable or disable options and checking the virus while entering (copying) data into the USB drives using filter techniques.

The scenario that the virus how it will affects.

The USB flash drive has become a new carrier in the spread of computer viruses which may be a disaster to a computer. If the computer is connected to the unknown system which is connected to the network, which is very difficult to guarantee the network is safe and clean absolutely. USB disk drives are usually named as Pen Drives are very useful portable storage disks which are commonly used for keeping the files to transfer computer data from one computer to another, whenever we want. But, as the storage devices are increased and the percentage of the flash drive being infected by viruses has also increased simultaneously. If pen drive connected unknowingly to the system which was already infected, thus the virus may enters into the pen drive without the user knowledge. In this case, the pen drive which is infected, it can then infect any other computer you might use with the drive. Once plug a virus-infected drive in any system, the system will be spreading virus. So, that there is a need of a system which blocks viruses entering into the pen drives.

VIRUS

The term "VIRUS" refers to the "vital information resource under siege". It defines that, segment of self-replicating code planted illegally in a computer program often damage to the entire system, like affect the files, converts files to other formats, hide the files, change the memory size, creating shortcuts, unauthorized access through the network, and etc. Viruses are categorized such as Boot virus, Program virus, Multipartite, Stealth, Polymorphic, Macro, Active X, Retro viruses and etc.

A. Purpose of the Project

There are many applications like anti-virus programs are available in the software market that will protects our system from virus. It should be installed in the computer

ISSN: 2278 – 1323

which to scan and detects the virus and keep the system safe. So, here, there are the applications that will protect the systems only. And its regularly scans and updates automatically when system connected to the network. So, here, we are mainly concentrating on USB drives, that are being affects and infects the other computers too when we connect to it. Currently, there is no methodology to blocks the USB drives from virus to be infected. Here, am trying to avoid the virus through the software and hardware method. The main purpose of the project is to prevent the USB drives from virus while entering into it ,by using filter techniques.

B. Motivation

As per survey on different papers regarding virus and an antivirus program, the viruses are being infected to our systems by the attacker in several ways. The main aim of the attacker to deny the access of users system by spreading the virus in many ways. Without users' knowledge only, viruses are spread in the system and infect the systems by the way it was programmed. It affects the storage disks which are used to store the data and to manipulate in the system by the user. In such a way, the storage devices like USB drives, which is portable and has increased in usage by the user to store and transfer the important files from one system to another system. Virus are easily spread via USB drives and its affects the files inside the drive and it will infect other systems also when we plug into the system for manipulate the files. There are many applications like anti-virus programs are available in the market that will protects the system if and only if, the anti-virus programs is installed in the system. In case that, USB drive is one the most dangerous in spreading of virus to other systems and network connected systems. Even though, the researchers are invented virus program to avoid in spreading of viruses through USB drives. But in case of vice-versa not applicable present now. So, there is a need of a system to prevent the files which are reside in the USB drive while virus entering into it.

C. Scope of the Project

As concentrate on the current problem, which arises in the most of the USB drives are infected through the virus. It corrupts and deletes the data that saved inside the flash drive. It leads to loss to a person who is having his personal information, project data of a business man, and etc. For these related problems, this kind of method is going to protects and blocks some type the viruses to be damage to the flash drive when we plug into an unknown system, which was already infected.

D Proposed System

The proposed method is going to block the virus while entering into the USB drives using filtering techniques. Though, it is a Component Based System Engineering (CBSE).So it is a combination of hardware and software system. The filters are used to block the virus, i.e. each time system going to check the files for checksum. The md5 algorithm is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length).It compress any large input files into small bits. It's nothing but 32-digit hexa- decimal number. So the storage of the virus signatures would be stored in less memory size. By default, the USB drive in the read mode. When enabling the write mode, the data need to be transfer. When it matches the checksum value to the entering file value it blocks and shows an error message in the window.

II. METHODOLOGY

The work started with literature survey for analysing the virus and how it will affects the USB drives when connected to the infected system. Then, started creating test virus and run in the system to check, how it works. Then got an idea to block or avoid the virus before affecting the work. Then, started implementing this idea through several methods and techniques. To work this method MD5 algorithm is used to store the virus signature by signature based detection. This will works through the microcontroller called Arduino UNO Atmega328.Connections through COM ports and USB cable for serial and data communication for data transfer and other data signals.

Method:

1. Connect the COM port and USB cable.
2. Select the LOCK mode for read operation.
3. In read operation: No write operation, if any data transfer, it displays a message as write protected.
4. Select the UNLOCK mode for write operation.
5. In write operation: Data need to be transfer , if any infected file found, it blocks and display error message.

III. SYSTEM DESIGN

The design of the system will integrate of each component using the bread board to design of a new interface to connect with the system. The Arduino Uno microcontroller is to fix using the analog, digital port pins, then Opto coupler, resistors and LED's are solder those using wires. After, fix the USB flash disk and interface it with Arduino Uno controller. Then test and connect the COM port to Arduino Uno and USB male to female cable to USB flash disk.

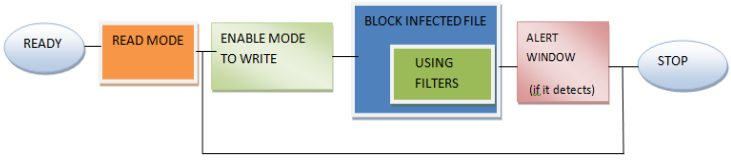

Fig 1. System Architecture

Block diagram of the system is shown in Fig 1. When the system is started, USB drive is in read mode by default. Then, selecting the write mode to enable the write operation for data transfer. When the data transfer , the method is going to block the infected file using the filters. The filters are nothing but a signature based detection to block the virus. After the detection, it displays in an error message window. Then returns to normal operation.

ISSN: 2278 – 1323

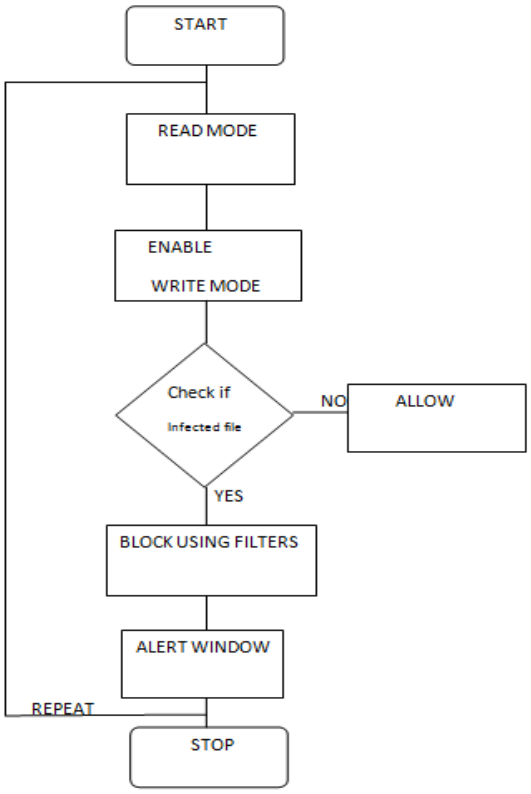

Fig 2. System flow

In the flow diagram in Fig 2 shows the system of the proposed method. By default the USB drive is in read mode. Then changing the read mode to write mode for write operation. Therefore, data need to be transfer to the USB disk drive. The filters will be added is used to detect the infected files while data transfer. If any infected file is found, its alerts an message window and then continues to its normal operation.

IV. IMPLEMENTATION

Signature based detection is a fixed examining method used on every antivirus product. This is also called a static analysis method. This decides whether the code is malicious or not by using its malware characterization. This technique is sometimes also called scan strings. In general every malware has one or more patterns of signature which has unique characters. Antivirus software searches through data stream bytes, when the program is executed. Database of antivirus software has thousands of signatures it scans through each signature comparing it with the program code which is executed. For comparing purposes searching algorithm is used, the comparison is usually between program code content with the signature database. The code which is converted by MD5 algorithm. Based on the code which is said as signature, the system is going to detects and blocks the defined virus. This technique at the beginning of the framework because of its effective detection of well-known viruses.

IV. CONCLUSION

USB disk drives are very useful portable storage disks which are commonly used for keeping the files to transfer computer data from one computer to another, whenever we want. But, as the storage devices are increased and the percentage of the flash drive being infected by viruses has also increased simultaneously. There are many devices that are in the present world using USB drives connecting to the computers. As there is no guarantee, to ensure USB drives being affected by virus. The proposed system is going to detect the set of defined virus and its blocks the one type of virus very effectively. A filtering technique is identified to study and analyze the virus and thus avoiding them from entering into the USB drives.

V. FURTHER WORK

The developed system can further extended and tested for more similar type of viruses. However developed method to enhance by adding new feature depending on the kinds of virus that can be considered to protection. Still finding the unique methods to ensure avoid the viruses are allowed to enter into the USB is an open problem.

REFERENCES

[1] Qiuting Jia, Guizhen Wang, Ruilian Hou, *A USB Flash Disk Viruses Preventing Technique Based on Filtering Access* , 978-1-4244-7237-6/$26.00 C 2010 IEEE.

[2] Gao Teng, *Research of Access Control of USB Storage Device with Information Security in Unauthorized Internet Access Monitoring System*, 978-1-4244-4507-3/09/$25.00 ©2009 IEEE.

[3] Sun-Ho Lee, *The Study on The Security Solutions of USB Memory*, 978-1-4244-5130-2/09/$26.00 © 2009 IEEE.

[4] Fuw-Yi Yang, Tzung-Da Wu, And Su-Hui Chiu, *A Secure Control Protocol for USB Mass Storage Devices*, IEEE Transactions on Consumer Electronics, Vol. 56, No. 4, November 2010.

[5] Debiao He, Neeraj Kumar, Jong-Hyouk Lee, *Senior Member*, IEEE, and R. Simon Sherratt, *Fellow*, IEEE *"Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices"* IEEE Transactions on Consumer Electronics, Vol. 60, No. 1, February 2014.

ISSN: 2278 – 1323