PORTABLE ANTI-VIRUS SYSTEM

Mr. Akshay S. Chavan

(Third year Computer Technology)

K. K. Wagh Polytechnic, Nashik

Mr. Akshay S. Jamdhade

(Third year Computer Technology)

K. K. Wagh Polytechnic, Nashik

Guided By- Prof. G. B. Katkade

(H.O.D. Computer Technology Dept.)

K .K. Wagh Polytechnic, Nashik

**Abstract:**

Any external drive can be infected by malicious programs. This malicious programs may enter in your external drive. Once your external drive has been infected, all the data on it might get corrupted or deleted. Also it will infect every computer system where it is connected. This can be avoided by keeping an antivirus program on external drive itself which will protect it from various viruses. This paper describes an inbuilt anti-virus protection system which will kept in an external drive and which will protect that external drive from various viruses and malicious programs.

**Keywords:**

Signature based virus detection, Heuristic Analysis, Portable Antivirus, Virus blocker ,Exception.

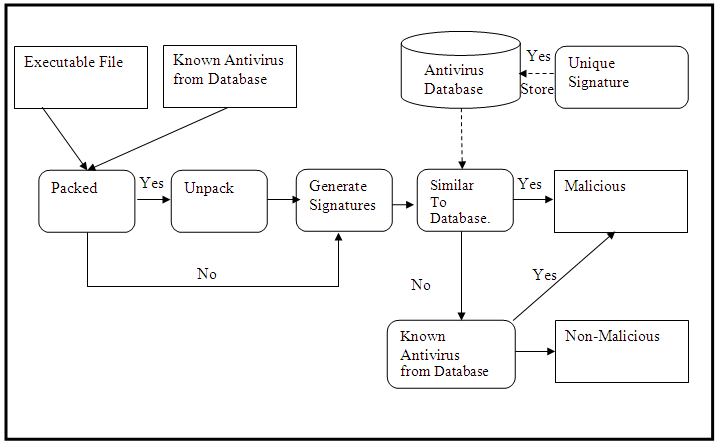
**Introduction:**

Viruses and other malicious programs are an ever increasing threats to current external drive and computer system. They can cause damage and consume countless hours and system administration time to struggles. People use external drives for all kind of storing activities: music, video, software’s,

documents, etc. At the same time, the risk of infection by malicious programs in these external drives is rising many viruses could enter into external drive. These malicious program may corrupt or alter the data on the external drive and also the computer systems where the external drive is connected. The main issue is that general users don't understand what a virus is and how external drives get infected. General users don't understand that how a virus may corrupt the data. A virus-infected drive can then infect any other computer where you might use the drive. Once plug a virus-infected drive in any system, the system will be filled with many viruses

The purpose of this software utility project is to protect external drives from malicious program on their own. The external drive will contain it’s own antivirus which will defend the external drive from various malicious program ensuring the security of it’s own. This software utility will help general users to protect their data from various malicious programs. Also many viruses enters computer system through internet or external devices connected, this utility will reduce the risk of malicious programs which enters computer system through external devices.

**Working:**

****

***Fig. (a) Working of Anti-virus System***

When the user will connect his/her External Device( Pen-Drive) to the Computer system, first the System(Anti-Virus System) will check whether the incoming file is Packed or Unpacked shown in Figure (a). If the incoming file is packed then it will first unpack that file and then it will generate the signature for the file.

After that it will compare the generated signatures with the System Database. If the generated signature is matched with the stored database then, the Anti-virus system will delete that file.

Otherwise it will keep the file as it is and allow it to be entering in the External drive.

**Detection Techniques:**

**A. Signature based detection technique**

Signature based detection technique is a traditional, simple and efficient method for detecting viruses. This technique scans files for virus’s signatures. Signature resembles the instruction pattern or a specific string of byte from virus’s program code. Signatures can be extracted by examining disassembled code of malware. Antivirus developer must look virus program code carefully to extract virus signature pattern.

****

***Fig. (b) Diagrammatic review of Signature based detection technique***

If there’s new virus comes, whose signature pattern is not available then developer must analyze infected file to find its signature. After collecting signatures of viruses, a signature database is created which facilities in virus detection. During detection process, whole computer system including executable files, boot records, document files etc. are checked for viruses. Matching of database’s signatures with any file’s signature resembles virus’s presence .After identifying virus, signature based detection procedure raises alarm for files immediate remedy.

Figure (b) describes diagrammatic review of Signature based detection technique.

Signature based detection technique is used for the detection of known viruses, which has been identified earlier i.e. their pattern or signatures are already captured in database. The technique requires signature database to be regularly updated for better results. Higher the signatures present in database, more will be the virus detection rate. This technique produces fast and accurate results. That’s why, this technique is used in almost every antivirus system .

But problem come when it is required to detect a new virus, which become next to impossible for signature based detection technique as its database does not have any signature for a new virus. As a solution, other methods can be used, tools like dissemblers and debuggers are available in market which can help in extracting signatures from program code. The code gets disassembled, analyzed and then signature extraction is performed .

**Advantage of Signature based virus detection:**

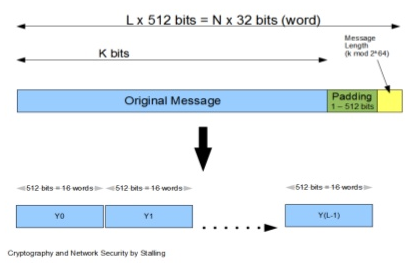
* This type of method is simple to implement.
* Give accurate result.

**Heuristic scanning**

Heuristic scanning is used to detect new/unknown viruses. It examines application program code and looks for particular commands to relate it with malicious programs. The process scans various programs i.e. boot record, macro files, executable files for virus-like instructions. Virus-like instructions could be malicious program’s payload, worm propagation routine, virus replication routine, etc. If scanning detects virus-like instructions, then heuristic scanner informs users about it. Heuristic scanning can be of two forms: Static scanning and Dynamic scanning. The former includes the scanning of program code and later includes the execution of program code on emulators to locate virus’s presence. Heuristic scanning can be done by three techniques which are:

1. Code Anomaly Detection
2. Protocol Anomaly Detection
3. Mixed Heuristic Detection

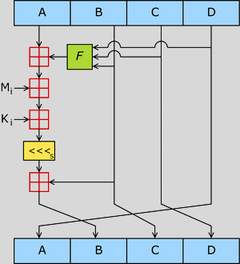
**Message Digest 5 (MD5) Algorithm**



***Fig(c). MD5 Algorithm***

MD5 is a message digest algorithm developed by Ron Rivest at MIT. It is basically a secure version of his previous algorithm, MD4 which is a little faster than MD5. This has been the most widely used secure hash algorithm particularly in Internet-standard message authentication. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit message digest of the input. This is mainly intended for digital signature applications where a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public key cryptosystem. Assume we have an arbitrarily large message as input and that we wish to find its message digest. The processing involves the following steps:

1. Padding of Bits
2. Append Length
3. Divide input into 512-bit Blocks
4. Initialize chaining variables
5. Implement Final Process Steps



***Fig.(d) Final Process Steps***

**Advantages of Anti-Virus System:**

1. **No prerequisites:-**

The prerequisite is already installed in windows

1. **Low Memory:-**

It take less space 50mb in USB Drive.

1. **Enhance Scanning:-**

It will scan USB drive as well as System drives also.

1. **Saves system space:-**

Saves Memory of computer system to installed Antivirus software.

1. **Less chances to conflict:-**

Less chances to conflict the utility with system antivirus.

1. **Virus Exception**

Exception of a virus can be added this will exclude the file and not scan the it

**Limitations of Portable Anti-Virus System:**

* **Update offline**

The virus database should be updated without internet connection

* **Limited Detection Techniques**

There's more than one way to detect a virus, but one big disadvantage to some antivirus programs is that they may not employ all detection techniques

* **Compressed File are not scanned**

Files within the compressed file will not be scanned

* **File is completely deleted**

When a file is detected as virus, it is removed directly. The file is not repaired.

**Applications:**

* **Antivirus protection**

As soon as the memory medium is connected to a given computer the resident protection is activated. This prevents the storing of harmful codes on the given medium. So you never have to worry that while using a computer with an unknown level of security, for example in an internet cafe, that your USB flash disk or memory card will be infected.

* **Secure transmission of data**

As we are not allowing any virus infected file to be entering into the external drive so obviously our data is protected at the time of transmission.

* **Scanning on demand**

According to your needs you can also launch a scan of the computer on which you are working on easily with your portable memory media. In the event of a harmful code being found, the file will be renamed, moved to quarantine or deleted depending on the settings.

* **Universal use**

The program is not installed on the computer’s hard drive but on a separate memory medium. This medium for example can be a USB flash disk or a memory card in any format.

**Future Enhancement:-**

* At present the utility has to be started manually. we will try to make it to start automatically when USB devices plugged in.
* Currently our database is updated offine. In future,we will try to update our database online.
* We will try to scan all the computers connected in a network
* Currently the viruses found are directly deleted,in future enhancement instead deletion we will try to repair the file.

**Conclusion:**

This project has dropped a small stone in water, by designing an application that provides a generic antivirus approach that is used to scan the files efficiently. ‘External drive protection system being developed by restricting to the present technology available in our college meets the desired needs of the requirements completely.

Our system can be extended further to an extent at which it can provide more facilities and flexibility than it provides at present..

**References:**

**Books**

1. Peter Zsor, The art of computer virus research and defense, Addison-Wesley, Maryland, USA, 2005.
2. Michael Erbschloe., Trojams, Worms, and Spyware, Butterworth-Heinemann publications. Oxford, UK, 2005
3. John Aycock, Computer Virus and Malware, Springer Science+Business Media, LLC. Calgary,Canada, 2006.
4. Cameron H. Malin, Eoghan Casey, James M. Aquilina, Malware Forensics: Investigating and Analyzing Malicious Code, Spi Publishing Services, Burlington, USA, 2008.
5. Mark A Ludwig, The Giant Black Book of Computer Viruses, American Eagle Publication, Arizona, USA, 1995.
6. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Inc., New Jersey, USA, 1999.

**Web Reference:**

http://www.ijarcsse.com/docs/papers/Volume\_4/3\_March2014/V4I3-0180.pdf

<http://www.anti-virus-softwarereview.com/>

[http://www.antivirus-software.com/](http://www.antivirus-software.com/ )

[http://www.buzzle.com/articles/ different-types-of-computerviruses.html](http://www.buzzle.com/articles/%20different-types-of-computerviruses.html )

[http://www.spamlaws.com/ virus-types.html](http://www.spamlaws.com/%20virus-types.html )

[http://www.ehow.com/list-7258284- computer-virus-detectiontechniques.html](http://www.ehow.com/list-7258284-%20computer-virus-detectiontechniques.html )

http://www.security.iitk.ac.in/contents/events/workshops/iitkhack09/papers/vinod.pdf