Malware Detection and Protection using External Devices

K.S.Charumathi, Y.I.Jinesh Melvin, K.S.Suresh Babu
Pillai Institute Of Information Technology,Engineering,
Media Studies And Research

Abstract— Virus Security Protection play a vital role while sharing files from PC to other external devices, normally to secure the file in PC some antivirus applications are used. This paper mainly focuses on to detect and protect malware from PC to other external devices using MDP (Malware Detection and Protection) method which is inbuilt in a microchip with external devices.

Index Terms— Microchip, Malware Detector, Protector, External Devices.

1 INTRODUCTION

In our day-to-day life everyone using PC's and other devices for communication, in which unwanted programs and files were copied and corrupted the data in the PC which is not aware to the users. Suppose the data is shared with any other external devices, that device is also vulnerable to those unwanted programs.

Now-a-days many antivirus software's are provided to overcome this problem. In this proposed paper malware is detected and protected [10][8] using MDP method and hence, MDP is inbuilt in a microchip which can be integrated with any external devices.

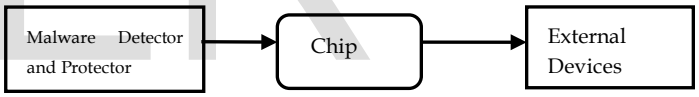
2 RELATED WORK

Malware is very huge threat and it corrupts the files easily. While downloading data from internet, some malwares are also downloaded along with data and hence the data is corrupted. Malware will spread to any external devices while someone trying to connect with malware PC. It classifies into virus, spyware, worms, Trojan etc... , after some related survey to satisfy for securing the external device from infected PC choosing Malware Detector and Protector. During fast scanning some small infected programs will missed to detect [9] and also it has low efficiency need of matching against more signature. In fast pattern matching it covers only the emergency virus [7]. By using Antivirus shielding software there is absence of accurate performance [6]. MD is to detect the infected code and encrypt the original data [10].

3 PROPOSED SCHEME

In this scheme inbuilt microchip which will be implemented by MDP application with any external devices. Suppose to connect external devices in any PC infected by virus, MDP will secure the device and if trying to share any files from PC to eternal device then MDP will scan the whole folder and detect the virus and protect it. After removing the detection of infected files, actual file will be transmitted to external device which the user connected with PC.

3.1 Module



The proposed scheme consists of the following three modules.

1. Malware Detection and Protection
2. Chip
3. External Device

3.2 Malware Detection and Protection

Consider D is detector and p is the set of executable program D (p). D detector scans the program and test to identify false positive, false negative and hit ratio. Signature referred as binary pattern of a suitable virus of the machine code. The database of virus signature is included in antivirus programs that compares with files on the hard disk and removable disk.

3.2.1 False Positive. It occurs when an antivirus program detect a virus by mistake in a non-infected files.

3.2.2 False Negative. An antivirus program fails to detect a virus in infected files.

3.2.3 Hit Ratio. Detector will detects the malware and the signature of malware will match with the signature in there database. Malware mechanism will manually protect the malware with malicious self-protection [8].

3.3 MDP Chip

In MDP chip to detect malware, anomaly-based detect and signature based detection are used. Specification based detection is a type of detector in anomaly-based detection. Three kind of malware were used they are Basic, polymorphic malware and metamorphic malware [10].

3.3.1 Basic Malware Detector. Basic malware controls the entry program and to compare the signature to found malware code.

3.3.2 Polymorphic Malware Detector. To enable the polymorphic virus the virus got polymorphic engine. It create a new evolve while it execute in each time, also API sequencing used to delete polymorphic virus [4], using certain Obfuscation technique [5] metamorphic malware can reprogram with itself.

3.3.3 Metamorphic Malware Detector. Malware detection will detect a malware code, it generate a new variant, and it have different signature. Metamorphic engine implement with some disassembler to the entry code and will produce new code with retain its functionality until gets different code.

3.3.4 Specification Based Detector. Specification-Based Detection trained the valid behavior of a program to inspected using panorama tool which capture the information under inspection and check behavior against valid set of rule to detect malicious activity. Obfuscation will hide the information others cannot find the true meaning.

3.4 External Device

MDP Chip is inbuilt in any external device, when user trying to connect the external devices with any PC then it will protect those devices. Implemented methods will process in that same time. Here we focuses external device such as pendrive, harddisk, cardreader etc.After sharing the folder MDP method will scan and variant the infected files and the original files. Then remove the infected file and sent original files. Now these external devices is secured and connected to other PC again it protect and safely send the files from external device to PC. So this makes the total security between external devices and the PC.

4 Working of Proposed Seheme

1. Connect external device to PC(secure)
2. Copy any folder
3. Automatically scan
4. Detect the virus file in display box
5. Protect the original files and send to External device

4.1 MDP Application

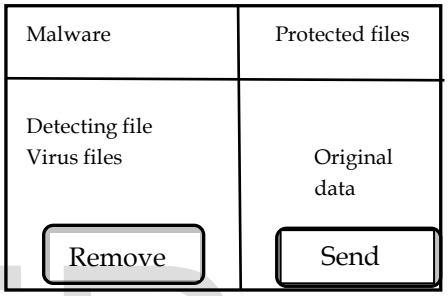
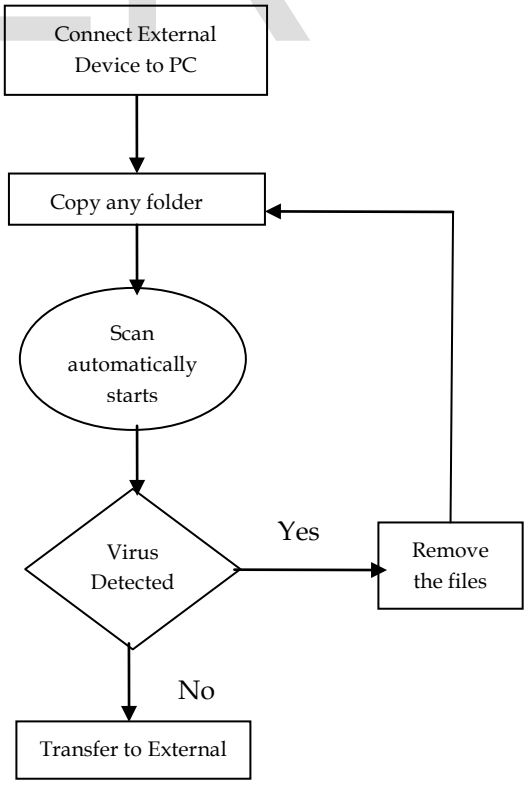


Fig. 4.1. MDP Application in Proposed

4.2 Flow Chart



- *K.S.Charumathi is currently Assisient Professor in Information Technology in Mumbai University, India,. E-mail: kscharumathi@mes.ac.in*
- *Y.I.Jinesh Melvin is currently Assisient Professor in Computer Engineering in Mumbai University, India,. E-mail yijmelvin@mes.ac.in*
- *K.S.Suresh Babu is currently Assisient Professor in Computer Engineering in Mumbai University, India, E-mail: sureshbabu@mes.ac.in*

Fig. 4.2. Flow Chart using Proposed Scheme

The Flow chart of proposed scheme describes, any user can connect their external device to viral PC, for copying files from that PC, it will scan automatically. While scanning the folder suppose there is any virus affected files, then it will detect the files into the application box. After detected the virus files, then remove those files and transfer the original data to connected external device.

5 CONCLUSION

In this paper MDP method is used to protect the external devices. Malware can be detected in short time and hence time computation is very much reduced. In future, this method can be extended to provide higher security while downloading files through internet.

REFERENCES

[1] Greoigre Jacob,Herve Debar,Eric Fillol,"*Behavioral detection of malware: from a survey towards an established taxonomy*",Springer-Verlag France.

[2] Mihai Christodorescu and Somesh Jha ," *Testing Malware Detectors*", in Proc. ISSTA'04, pages 33-44, Boston, MA USA, ACM Press.

[3] Gerard Wagener,Radu State,Alexandre Dulaunoy,"*Malware Behavior Analysis*",Springer-Verlag France.

[4] DataRescue, Inc. The ida pro disassemble www.datarescue.com/idabase.

[5] Arun Lakhotia , Aditya Kapoor , Eric Uday , "*Are Metamorphic Viruses Really Invincible ? Part 2*", Virus Bulletin.

[6] Fu-Hau Hsu,Min-Hao Wu ; Chang-Kuo Tso ; Chi-Hsien Hsu ; Chieh-Wen Chen "*Antivirus Software Shield Against Antivirus Terminators*" Dept. of Comput. Sci. & Inf. Eng., Nat. Central Univ., Jhongli, Taiwan.

[7] Xin Zhou, Bo Xu , Yaxuan Qi , Jun LiMRSI:, "*A Fast Pattern Matching Algorithm for Anti-virus Applications*" Res. Inst. of Inf. Technol., Tsinghua Univ., Beijing.

[8] Alsagoff, S.N.; Fac. of Sci. & Defence Technol., "*Malware self-protection mechanism*" Nat. Defence Univ. of Malaysia, Kuala Lumpur.

[9] Bo Li ; Eul Gyu Im "*A signature matching optimization policy for anti-virus programs*" Electron. & Comput. Eng., Hanyang Univ., Seoul, South Korea.

[10] Vinod P. , V.Laxmi,M.S.Gaur "*Survey on Malware Detection Methods*" Department of Computer Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan.