IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-10, Oct. 2018 E-ISSN: 2347-2693

Implementation of Intrusion Filtration Model

R. Dewanjee[1*], S. Barde[2]

[1,2]MATS School of Information Technology, MATS University, Raipur, India

[*]*Corresponding Author: rita.dewanjee1@gmail.com, Tel.: +91 7024468686*

Available online at: www.ijcseonline.org

Accepted: 13/Oct/2018, Published: 31/Oct/2018

***Abstract*—**Security from intrusions for alone system and in network nodes are always important. The protection and prevention methods available with antivirus and IDS/IPS are works on intrusions and provide security on all known intrusions. They have a database to match the pattern or signature of intrusion and based on that they complete the action of quarantine/repair or cleaning of file. Sometimes installation and configuration of such software occupies large space of memory and heavily slows down the speed of computer as well network. To work in full swing they must be updated time to time and also need the combinations of other security features including online facilities. Operating system and File system provided security features are not all default, they may be applied on interest of user. We are suggesting a model which will be default feature of operating system and will work for all files regardless of different interface of interaction with user.

***Keywords*—** Operating system, Network security, Intrusion Filtration model, IFS, TSC, token secuirty log, file log

I. INTRODUCTION
COMPUTER SECURITY

We can categorize computer security in following categories-

1.1. Network and Internet Security

1.2. Computer Security in standalone system

1.3. Accidental Data Losses

1.1- Network security dealt with the problems of Network and computers inside network. The Network Security problem can be of any size dealing with external issues, problems from users inside the network etc. Network security problems arise in issues of client server models. The selection of server and its configuration policy decides are the important parameters for level of Network security we are implementing. Improper configuration of servers , misuse of user rights and spamming to create DoS are major issues in network security.

Internet Security deals with malware and hackers. Internet is open zone any one can occupy web space by creating their own website and put malware to place in your computer or in server. We can categorize Internet among trusted and un trusted sites. The secure sites used lock symbol to represent safe site in the address bar of computer. Internet security mainly hacked by port scanning and packet sniffing. *Port scanning*, is the technique ports on your computer or server are accessed by hackers. They keep on trying, Once locate the open port, they can read access and manipulate data from computer.

1.2- Standalone computers refer to computers that are not connected to any network (but may be connected to Internet). For standalone computers major types of computer security are factors affecting on data. The major threat is stealthy techniques

1.3- Accidental Data Loss part is applicable to networks, computers nodes in networks and for standalone nodes whether connected or not with internet. A sudden crash of HDD and network failure during transmission creates problem of data loss.

II. LEVELS OF SYSTEM PROTECTION

There are four levels at which a system must be protected:

2.1 -From Physical thefts

The easiest way to damage any ones system to crash or run command of format, stealing storage devices etc. Misuse of user rights and diverting the root from authentic user.

2.2 - From Human

There is some concern which basically means fooling trustworthy people into accidentally breaching security. Phishing involves sending an e-mail or web site designed to fool people. E.g. spam e-mails pretending to be from authorized sites to share the credit card details. Dumpster Diving involves searching the trash and locations for passwords . Password Cracking involves divining users passwords

2.3 -From Operating System

DoS, violations of memory-access and stack overflow, launching of programs with excessive privileges etc must be taken care to protect OS.

2.4 - From Network This is a growing area of focus because wireless communications and portable devices become more prevalent.

III. SYSTEM SECURITY FEATURES FOR COMPUTER

3.1. Operating system security features - In various OS different features are included to protect the system and its data. Following are few of the points marked here in Windows and Linux which can implemented by user.

A) For Windows Operating System -

1: Creating a Strong Password.
2: Update Windows frequently
3: Update all software's time to time
4: Properly configure Firewall
5: Properly set restoring points
6:Use Encryption Software for sensitive data
7: Take periodic system Back-Ups
8: Install an antivirus

B) For Linux Operating System -

- Use a password protected Grub boot loader
- Keep Kernel and Software up to date
- Take the backup of critical data.
- Use a secure session
- Disable root Login
- Configure the DNS server not to receive dynamic updates
- Implement access control
- Use Firewall
- Use Network Information Service

Analysis -The feature marked here for security are somehow related easy to implement by user who are familiar with computer or having knowledge of internal settings of computer. User must have procure licensed versions to OS, antivirus, Firewall etc in order to update those frequently. Few of features are subscription based which must be updated time to time for better performance, somewhere imposes the financial burden and workload of doing all these. For a nontechnical person it will be really a hectic task.

3.2 File system security features - Other than security features provided by OS, file system also provide specific security features in order to protect the data integrity and security -

- using Digital signatures
- using File Encryption
- by Restricting access control
- by Inspecting documents

Analysis -

The provision of using digital signature is not easy for non technical users. It needs additional financial implication to get secured digital sign. The file encryption methods provided with Microsoft office applications like word, excel, power point etc. The rest files of image, audio and video, pdfs are not having default facility of encrypting the files. The user has to trigger the encryption and digital signatures if they wish to secure the files. It's not default feature of File system to encrypt every file or save it with digital signature.

The security provided through user access control are not much beneficial if we are working using admin credentials. The inspect document help user to remove metadata and hidden data attached with document but the facility is available only for Microsoft office package like word, excel and power point.

3.3 Antivirus Security Features -

Antivirus software helps to protect computer system from viruses , Trojans , worms , spyware , adware , rootkits and key loggers etc.

Analysis -

Antivirus slow down the PC or network speed. It occupies a lot of memory and storage space. Antivirus along with firewall need to be installed in order to provide full internet security. Only antivirus cannot protect system from remote attack. Antivirus software scans system based on the pattern and signature of intrusion database available with software. Antivirus scans system and list out the intrusions repair or clean one.

The details of scanning is store in system in different format like xml data in log files. Those log files may keep details of intrusions founds and repaired. Some antivirus software keeps only the file which were not repaired and information is sent to the main technical team if online antivirus package is configured.

Antivirus software do not tag any scanned and safe files for users. If user accessing or transferring any file after of few hours of full scanning of system then also, the file must be checked or scanned before sending through email or PD.

3.4 Intrusion Detection and prevention system

An Intrusion Detection System (IDS) is a software which send alerts when attackers or intrusions are trying for malicious activities or security policy violations. IDS works on monitoring approach. It automatically monitors the

Internet for the latest threats which could result in a future attack. IDS works on algorithms to detect the intruders.

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that prevent vulnerability exploits. The IPS configured with firewall provides a complementary layer of analysis. IPS configured inline to actively analyzing and triggering actions on all traffic flows entering into the network.

Analysis -
IDS and IPS has several advantages like-
- real time alerts
- regular updates for new threats
- They collect system logs from all devices of network can do analysis using one management console
- various types of IDS available in market and can be mapped and configured based on network environment
- After certain time of period it creates a normal network environment which helps to easily identify the deviation from normal environment because of suspicious or non-conformist behavior of intrusion.

IV. NEED of IFM

In above sections we have discussed how OS, file System, antivirus software's, IDS and IPS helps to protect from intrusions. With a lot of benefits, still there are chances of improvement likewise antivirus software works on intrusions.

They either repair the files or delete the corrupted files. IDS and IPS also works on intrusions. File system and OS includes features of security which can be applied on interest of users.

The security features where user access controls are suggested to limit the access on files, what will happen if we are working in admin login? Is there any provision that stop access of files if any unauthorized program or intrusion is trying to access it. Once the intrusions able to escape itself and entered into system it has n number of options to damage the system.

All above explained systems doesn't have any default security feature which works on safe files. We need a default security provisions which can secure files regardless of asking any interaction of user and shall be applied for all data available in system.

Some Antivirus software treats system files also as an intrusion. Antivirus doesn't list clean files. Intrusions are small executable files which disseminate itself using files and folders once the triggered on feasible conditions. They imitate as part of system files and folders because these are open for access without any security lock and executes itself before actual program so that doesn't require registry in system log for execution.

All protection software must be updated time to time to provide full security online and offline both.

The User interact with Operating system using Application software's which are registered in system log. The output of those applications software are files. The folders are logical partition in memory to separate the storage of various files. The files stored in memory are loaded to the RAM while any registered system program are accessing it. The Antivirus software, IDS and IPS scans the files and folders of system and identify the intrusions and takes appropriate actions to recover or repair the files. The Antivirus software has their own limitations. They can identify only those intrusions or malicious codes of which the signature or pattern is available in its database. If any new malware is created it won't be able to detect it.

The below diagram summarizes the process -

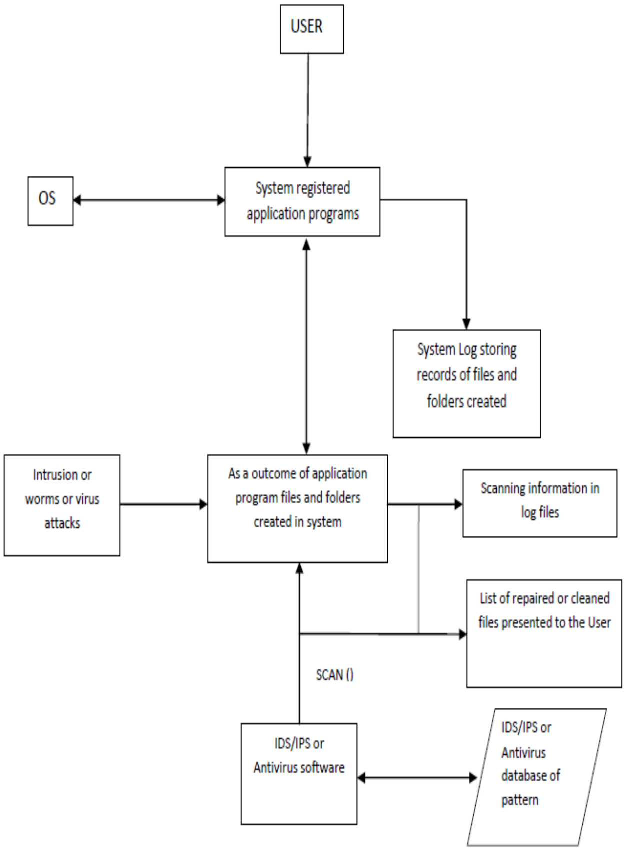

USER
OS
System registered application programs
System Log storing records of files and folders created
Intrusion or worms or virus attacks
As a outcome of application program files and folders created in system
Scanning information in log files
List of repaired or cleaned files presented to the User
SCAN ()
IDS/IPS or Antivirus software
IDS/IPS or Antivirus database of pattern

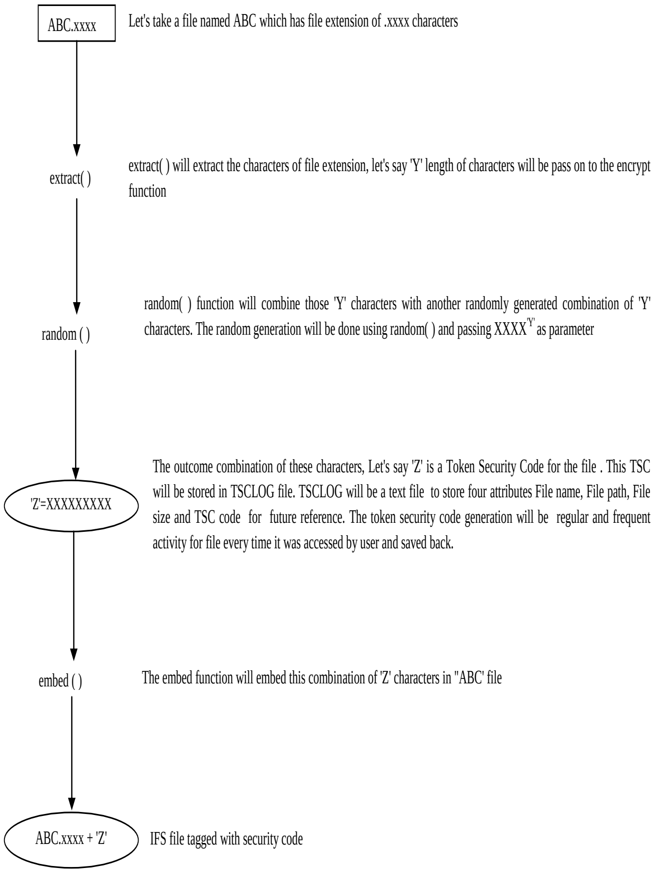
Fig 1: Normal Procedure of Operating system and Antivirus Antivirus Software databases needs frequent updates.

Sometimes some system generated files also treated as malware because their pattern matches with the intrusion one. To get solution on such issues the prevention software's must have online technical support. After scanning system these software's list out the intruder files identified by them and actions performed on them if any. They also send the information of new intruders to the technical support team for its solution. The various operating system's has provision to store the scan information in different format but default is all these are stored in log files. These log files keep sometimes information of only the dates and scan performed if all sorted out and in case if any severe threat found they also keep the detailed information about that threat. Log files stores data in encrypted format so it is not easily understandable for common users. While going through the log files it is found that intrusions are given a code which is a combination of digit, letter and special characters. The log files stores metadata and history of scanning. Which intrusion information is reported to online technical team.

V. INTRUSION FILTRATION MODEL

The model will have following features -

- Every Operating system will have a Public Key and Private key
- The model will work on Two step verification method
- The first step to check the TSC code in file stream buffer for verification of scanned secure file.
- The second step of checking of genuine process execution installed in system
- All files will be assigned unique token security code which will be generated using its public key and can be decrypted only using its private key
- The Token security code and Process Security Code will be in encrypted format
- The all computer system has registered programs entry in system log file and Files and folders created are indexed in File log which stores the details of every file created in system.
- Every installed program of computer system will be assigned a unique PSC and same will be stored in Process System Code Log (PSClog).
- Every time when a new file is created and saved in storage, Token Security code agent will generate a TSC (Token Security Code) and save this in TSC log (Token Security Code Log) along with its associated TSC.
- When any system program or user try to access any file, the token security code agent will first read the associated TSC code from log file decrypt it using systems private key and match the TSC embedded in file stream and check whether the file has entry in TSC log and its TSC code is matching with it or not.



Let's take a file named ABC which has file extension of .xxxx characters

extract( ) will extract the characters of file extension, let's say 'Y' length of characters will be pass on to the encrypt function

random( ) function will combine those 'Y' characters with another randomly generated combination of 'Y' characters. The random generation will be done using random( ) and passing XXXX$^{'Y'}$ as parameter

The outcome combination of these characters, Let's say 'Z' is a Token Security Code for the file . This TSC will be stored in TSCLOG file. TSCLOG will be a text file to store four attributes File name, File path, File size and TSC code for future reference. The token security code generation will be regular and frequent activity for file every time it was accessed by user and saved back.

The embed function will embed this combination of 'Z' characters in "ABC' file

IFS file tagged with security code

Fig 4.2 - Token Security Code(TSC) generation process

Fig.2 Token Security Code (TSC) generation process

- On confirmation of matched TSC in file and TSClog, the next step verification will be done for system registered application program from system log to prohibit the unwanted executable codes to be run in system.

- TSClog will store Token Security Code(TSC), Filename, Filesize, Path of File, PSC(Process security code).

- The Process Security Code Log will be created to store system and application programs installed in Machine. The every installed process will get Process Security Code(PSC) to verify the genuine process.

- The user when try to access any file the both TSC and PSC codes will be verified in log files to check for genuine process and secured filtered tagged file.

- If both codes are not authenticated user will be intimated for respective information and asked for antivirus scan.

- The following figure will explain the procedure of TSC code generation -

The below diagram shows the abstract process of IFM

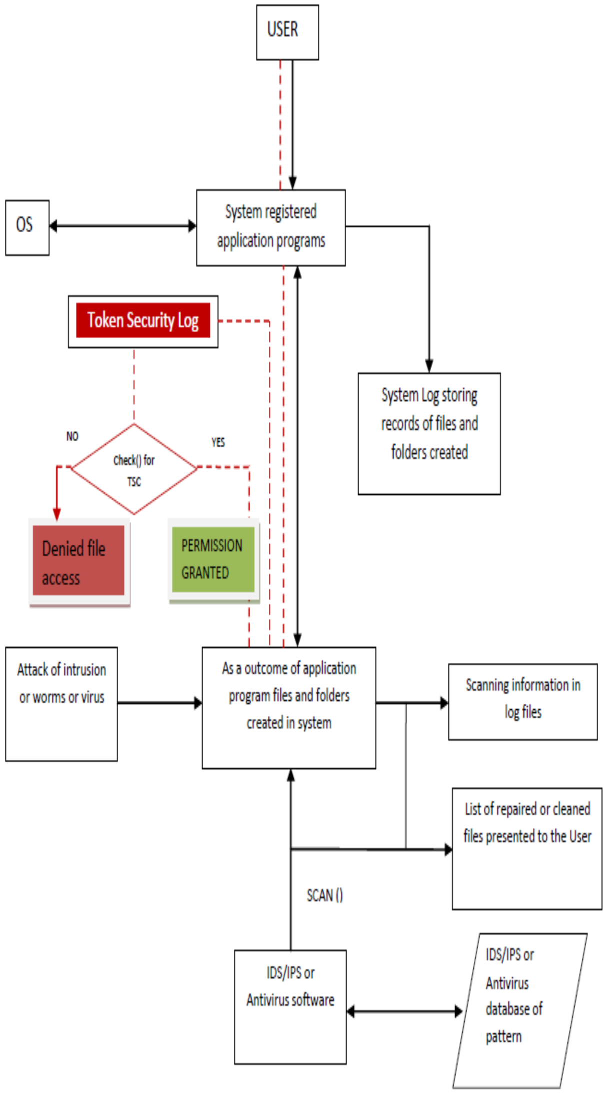

USER
OS
System registered application programs
Token Security Log
System Log storing records of files and folders created
NO
YES
Check() for TSC
Denied file access
PERMISSION GRANTED
Attack of intrusion or worms or virus
As a outcome of application program files and folders created in system
Scanning information in log files
List of repaired or cleaned files presented to the User
SCAN ()
IDS/IPS or Antivirus software
IDS/IPS or Antivirus database of pattern

Fig. 3 The abstract process of IFM

VI. CONCLUSION

The security of Network is always important and crucial point for organizations, managing data and its communication. The variety of Techniques are available for securing the Network implemented in hardware and software. The chunk of talented pool of IT sector, has 24 hrs eyes on the happenings of security area whether done through researcher for tightening the security or by hacker to breach the security. The method we are proposing here will be implemented through software. The Intrusion Filtration Model(IFM) will work with association of antivirus or Intrusion Detection System(IDS) available in Operating System. The IFM will help to do secure communication and use of filtrated data over the intranet and internet. IFM will ensure the uncorrupted files communication channels at the downloaded port.

Looking to the network security domain when each and all most every day a new threat is invented by hackers, the IFS is proposed to focus on circulation of filtered files, and provide the security of data in certain extent by not using the corrupted files.

IFM will be proposed to support the network security and provide the additional facility for user to stop using and distributing the corrupted files. Although the practical implementation of IFM is still pending. The coding and rest of the aspects of IFM and its comparison in detailed with existing techniques will be proposed to done in next paper.

After discussion on its overall performance it seems a possible new method of securing data inside and outside the system. IFM will be IPS system rather than IDS. The IFS is under research process.

IFM will stop circulation of corrupted files through removal disks and through internet as attachment hence support to network security. We tried here to explain all aspects and discuss its performance. I request the peers for their valuable suggestions feedbacks and critics to update the work.

The different categories of IDS are explained here with all their advantages. After deploying firewall technology in network the IDS are also becoming next logical step for many organizations at the network perimeter. IDS are capable of offering protection from attackers, whether internal or external. IDS, even can be used into those areas where traffic doesn’t pass the firewall, or uses it the least.

The IFM will be a system which will work internally as a utility program and mark the files as filtered or unfiltered. The security of IFM will be ensured through cryptography Technique. By proposing IFM we are trying to avoid the use of corrupted files and subsequently their distribution in the network.

VII. FUTURE WORK

The model proposed here requires higher end programming in order to get implemented in operating system. The code done here to show the processing of IFM is working with Text files only. To start the IFM all initial API packages must be implemented in back end programming so that different files can be accessed regardless of their type i.e. extension of file, TSC can be easily embedded and traced whenever required. Thus the actual implementation part of this research work is still left. Although it can be offered as utility program also but implementation with OS as an compulsory feature will be the best option to create a safe environment for user to work.

REFERENCES

[1]. Zhenfang ZHU, "Study on Computer Trojan Horse Virus and Its Prevention", International Journal of Engineering and Applied Sciences (IJEAS) ISSN: 2394-3661, Volume-2, Issue-8, August 2015

[2]. Hossein Rouhani Zeidanloo, S. Farzaneh Tabatabaei, Payam Vahdani Amoli and Atefeh Tajpour, " All About Malwares (Malicious Codes)" Faculty of Computer Science and Information System, University of Technology Malaysia(UTM) , Kuala Lumpur, Malaysia

[3]. Benjamin A. Kuperman, Carla E. Brodley, Hilmi Ozdoganoglu, T.N. Vijaykumar, and Ankit Jalote, " DETECTION AND PREVENTION OF STACK BUFFER OVERFLOW ATTACKS", COMMUNICATIONS OF THE ACM November 2005/Vol. 48, No. 11

Authors Profile

Ms Rita Dewanjee pursed Bachelor of Science from Pt Ravishankar Shukla University, India in 1998 and Master of Computer Management in 2004. She pusuied her MCA from Sikkim Manipal University in year 2008 and M.Phil from MATS University in 2009. She is currently pursuing Ph.D. and currently working as Associate Professor in MATS School of Information Technology, MATS University, India since 2005. She is a member of CSTA, CSI, UACEE, IACSIT, ISTE, IAENG & Science PG since 2015. She has published more than 9 research papers in reputed international journals including Springer and conferences including IEEE and it’s also available online. Her main research work focuses on Network Security, Intrusion Detection and Prevenion, Green Initiatives, Digitalization in CG. She has 14 years of teaching experience and 8 years of Research Experience. She has conducted 8 Seminar, Conferences and 9 workshops of national and International Level as Convenor.

Dr. Snehlata Barde is working as an Associate Professor in MAT'S University, Raipur, (C.G.). She received her Ph.D. in Information Technology and Computer Applications in 2015 from Dr. C. V. Raman University Bilaspur, (C.G.). She obtained her MCA from Pt. Ravi Shankar Shukla University, Raipur, (C.G.) and M.Sc. (Mathematics) from Devi Ahilya University Indore, (M.P.). She is a member of IAENG (International Association of Engineers) and CSI (Computer Society of India); She has published more than 3o research papers in reputed International and National Journals and Conferences. Her main research work focuses on Digital Image Processing and its Applications in Biometric Security, Forensic Science, Pattern Recognition, Segmentation, Multimodal Biometric, Soft Computing Techniques, IoT and Network security. She has 18 years of Teaching Experience and 7 years of Research Experience.