Network security - Intrusion Filtration Model

[1]Rita Dewanjee, [2]Dr Snehlata Barde
[1]Research Scholar, [2]Supervisor
[1,2] MATS School of Information Technology,
[1,2] MATS University, Raipur, India

Abstract : Operating systems allows all registered application program to run and allow user to work in computer. It's not necessary that all application programs installed in computer system are known by users or shall be matter to be known by them. The outcome of all application program are stored in folders and files. The built in facility of file system provides security to data and files inside the system using access control, encryption, RAID and recovery methods. Apart from these facility of securing files and folder we use antivirus software to detect and prevent files from intrusions. The model we are going to explain here will strengthen the security of scanned files by tagging them. Model proposed here will stop unnecessary repeatedly scanning of all files and proposes a new mechanism of accessing files by system applications. The access of files will be permitted to User and system application based on encrypted security tokens. Hence stopping the un wanted unauthorized access of files and folder by intrusions.

Index Terms **- Intrusion Filtration Model, , Intrusion Detection System, IDS, Network Security, Token Security Code(TSC), antivirus, OS, Logs, Token Security Log, TSClog, access control**

I. HISTORY AND SECURITY PROBLEM

Exploitation of Computer Security in history happened during the 1970s when the operators of Telephone intentionally misdirected calls and eavesdropped on conversations. The operators started this as fun to listen the conversation between parties and make free call in long distances. Copper cables are used in Telephone wires to pass signals from which signals can be tapped easily and conversation can be heard.[1] A group of people known as phreakers exploited the weakness of digital switching telephone systems for fun.

The next exploitation target of hackers are bulletin boards because this uses sharing of passwords, credit card numbers etc. Mr Ian Murphy's broken the security of AT&T's computers and Kevin Mitnick's stolen computer manuals of Pacific Bells's switching center. The Govt. then formed CERT and handed over the project ARPANET to encounter increasing threats to security. In 1990s more hacking activities started like "Michelangelo" virus, credit card details cracked by hacker Kevin Mitnick.
In 1998 Solar Sunrise attack targeted computers centers of Pentagon by Ehud Tenebaum. The growth of the Internet and business-related information increased threats safety technologies like firewalls, antivirus programs and on other hand viruses, Trojans, and worms were proliferated.

The problem of secure communications over internet increased and the concept of cipher and cryptography started.[3]
Every organization is focusing in security aspect of technology. The Computer security shall be consider for both hardware and software threats. The hardware threat can be given security by constant surveillance, locking system, and by physical guarding. The security of software is more sensitive because it could happened in presence of user also. The branch of IT which works for protection of data on a network or a stand-alone desktop taking it utmost important. [2]

II. CATEGORIES OF THREATS

Security threat can be categorized into four parts and these categories are the ways or forms through which threats can be carried out on a network.

2.1 UNSTRUCTURED THREATS

Unstructured security threat is the kind of threat created by an inexperienced person trying to gain access to a network. They commonly use common hacking tools, like shell scripts, and password crackers. A good security solution should easily thwart this kind of attack. In other words, these kinds of hackers could not be underestimated because they can cause serious damage to network.

2.2 STRUCTURED THREATS

Unlike unstructured threats, structured threat hackers are well experienced and highly sophisticated. They use sophisticated hacking tools to penetrate networks and they can break into government or business computers to extract information. On certain occasions, structured threats are carried out by organized criminal gangs or industry competitors.

2.3 EXTERNAL THREATS

Some unauthorized people outside the company who do not have access to the company's computer system or network could cause external threat. They usually break into company's network via the Internet or server. Both experienced and inexperienced hackers could pose external threats.

2.4 INTERNAL THREATS

This kind of threat could be by a disgruntled employee who has authorized access to the company's network. Like external threats, the damage that could be caused by such a hacker depends on the expertise of the hacker. (Orbit-Computer Solutions 2012). Packet fragmentation attacks that retransmit sequence numbers so that the IDS sees only what a hacker wants it to see.

III. TYPES OF SYSTEM THREATS

Network security is a phenomenon which is more than what people always thought it to be, malware, virus, Trojan, hackers. Network attacks could be caused by unintentional human error and it could be compromised by human nature as well. A common issues that most organizations are facing sometimes has to do with their employees and its various errors they make. However it is not only human errors that can cause problem to network security, problems can also be caused by natural forces like fire breakouts, earthquakes, floods lightning etc. The ways network administrators think about securing networks has been changed by an increasingly dynamic and technically challenging risk environment. New business models rely on open networks with multiple access points to conduct business in real time, driving down costs and improving response to revenue generating opportunity by leveraging on the ability to quickly exchange critical information, share business files or folders and improve their competitive position.

The task of Intrusion detection system is very challenging due to expertise demands and its highly collaborative nature. The system needs a significant specialization in both technical and organizational. Network experts requires to have the knowledge of their own unique network environment, since what is characterize as a security event in one network may not be considered it in another network. Attaining this degree of expertise is complicated, as much of the necessary knowledge is tacit and may be organization specific. Further complicating Intrusion system task is its collaborative nature that drives the need for practitioners to coordinate with other organizational stakeholders.

To obtain a bird-eye-view of the challenges and issues, we use data from two papers to perform a cognitive analysis of the three Intrusion system phases (pre-processing, monitoring, analysis, response). In general, they propose that all phases are challenging, but that the monitoring and analysis phases are the most cognitively demanding for practitioners. This high cognitive load obtained from the need to integrate various sources of information in these two phases, including background knowledge on the network and the user base and information generated by the various tools involved in ID, such as the output of an IDS and network logs.

There are many common threats for systems.

- Trojan Horse
- Trap door
- Logic Bomb
- Stack and buffer overflow
- Viruses
- worms
- port scanning
- Denial of service

3.1 Trojan horse is a malicious program which occurs unexpected changes in system settings and creates unexpected activities. Trojan horse is a type of software which interpret itself as a part of regular software program of system like utilities, games etc. Mostly Trojans are introduced via email attachments. Some most common Trojans are Backdoor Trojan, Downloader Trojan, Info stealer Trojan, Remote Access Trojan, Distributed Denial of service attack Trojan. Trojans can delete, copy, modify, block or disrupt the performance of targeted computer

Prevention methods from Trojan Horse -

- periodic diagnostic scans
- update operating system software's
- Stop visiting unsafe websites
- Do not download or click on unknown links[8] [11]

3.2 Trap door are the block of codes left by programmer intentionally or unintentionally to test and debug the program which becomes secret entry point inside a program to gain access without usual security procedures. This block of codes become threats when used to gain unauthorized access. Trap doors controls are difficult to implement in operating system.[13]

Prevention Methods from Trap Doors -

- Install a good antivirus
- Keep antivirus updated
- Keep antivirus protection enabled at all times.

3.3 Logic Bomb is a piece of code inside OS and other application program which triggers on certain specific conditions like, on specific date, when met of certain conditions specific etc. [14]

Prevention Methods from Logic bomb - [14][15]
- Use the concept of Least Privilege
- Stay up to date
- Use secure system configuration
- Use Integrity Checker
- Use Antivirus

3.4 Stack and buffer overflow happens when a program occupies more than the storage area allocated for it. The extra space occupied by the program is called stack overflow or buffer overflow. It is dangerous because the extra data may have codes to damage files, change system settings, access confidential personal information and corrupt or overwrite the data where it is hold.[7]

Prevention Methods from Stack and Buffer Overflow [7][8][9]-
-Operating systems are now using address space layout randomization (ASLR). Non-executable stacks (i.e., data execution prevention (DEP)) to prohibit some areas from stack overflow.
- To detect and eliminate such source code by doing source code auditing, before execution of program or software put to use
- By avoiding such languages which has unbounded copying functions or unchecked buffer lengths

3.5 Virus and Worms are self-replicating malicious programs that are designed to infect and gain control of system. It spreads itself into other executable code or documents. Viruses spread via emails. [10] Worms often use components of OS that are self triggered and not visible to the user. Worms replicates itself computer across network connections, email, infected Web page or instant messages and Internet Relay Chat (IRC). [11]

Prevention Methods from Virus and Worms -
- Avoid unknown email to be opened
- Don't open unsolicited executable files
- Avoid downloading double extension files
- Always send scanned files
- Scan all new files with virus software
- Turn on firewall alert for harmful sites
- Frequently update antivirus software

3.6 Port Scanning - All services of computer are associated with well known port number. Port scanning is a threat which simply sends request to connect to the target computer and for that it scans each port sequentially and makes a note of each ports to attack deeper. It is the easiest way to discover services and can break into.

Prevention Methods from port scanning -
- Use of Firewall
- close unnecessary services on the targeted systems
- employ TCP Wrappers
- Avoid default installation of operating system **[12]**

3.7 Denial of service is an attack to shutdown a machine or to make inaccessible for intended users or imposing it for crash.DoS attacks often target web servers. Flooding and crashing are two most common DoS attacks. Flood attacks when server needs too much load for buffering , causing their performance slow down and stop. Most common flood attacks are Buffer overflow attacks, ICMP flood, SYN flood. Crashing is done by bugs in the target that crashes or severely destabilize the system from user access or by being used. [13]

Prevention Methods from DoS -
- Deploy an antivirus program and firewall
- Design proper firewall policy
- third party services for highly confidential and sensitive information [14]

IV. INTRUSION FILTRATION MODEL

As the computers and networked systems increases in the world of today, the need for increase and strong computer and network security also becomes increasingly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure, one can see that the need for increased network security is vital and important in every organization.

The security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment. There is no laid-down procedure for

designing a secure network. Network security has to be designed to fit the needs of one organization network and not anyone else's.

For instance, a small sized law company would allow access to case information for authorized users on the outside of the network, and at the same time ensure that full access to the internet is always available to staff on the inside of the network, in other cases to access a case file from the office or on the road. Good network security protects a network in a manner that is consistent with its purpose and precautions must be taken when choosing a network provider for an organization especially one like a law firm.

Intrusion detection and prevention are the two most important aspects in Network security. Security in organizations in terms of confidentially and privacy is most important nowadays. Numerous Intrusion Detection systems are available; each having specific features and design goals. Researchers from worldwide are doing comprehensive and rigorous study on this emerging field with different techniques of intrusion detection. As the network is growing day by day and exploring itself the security of data is also becoming very crucial. Intrusion Detection is serving as one of the most popular tool to provide security. Intrusions can be detected and prevented by using these IDPS. The objective of the research contribution is to propose a Model for Network Security.

The Operating system will be equipped with new feature of Token security code and token security log, which will be default system files in all operating system. The TSC log file will store TSC issued to the file in encrypted format and this code will be cross checked every time when user want to access any file in system. Once TSC found and matched with TSC log the next checking will be done for registry of system application. After of both confirmation, file will be allowed to open for access. The proposed model is presented here in diagram -

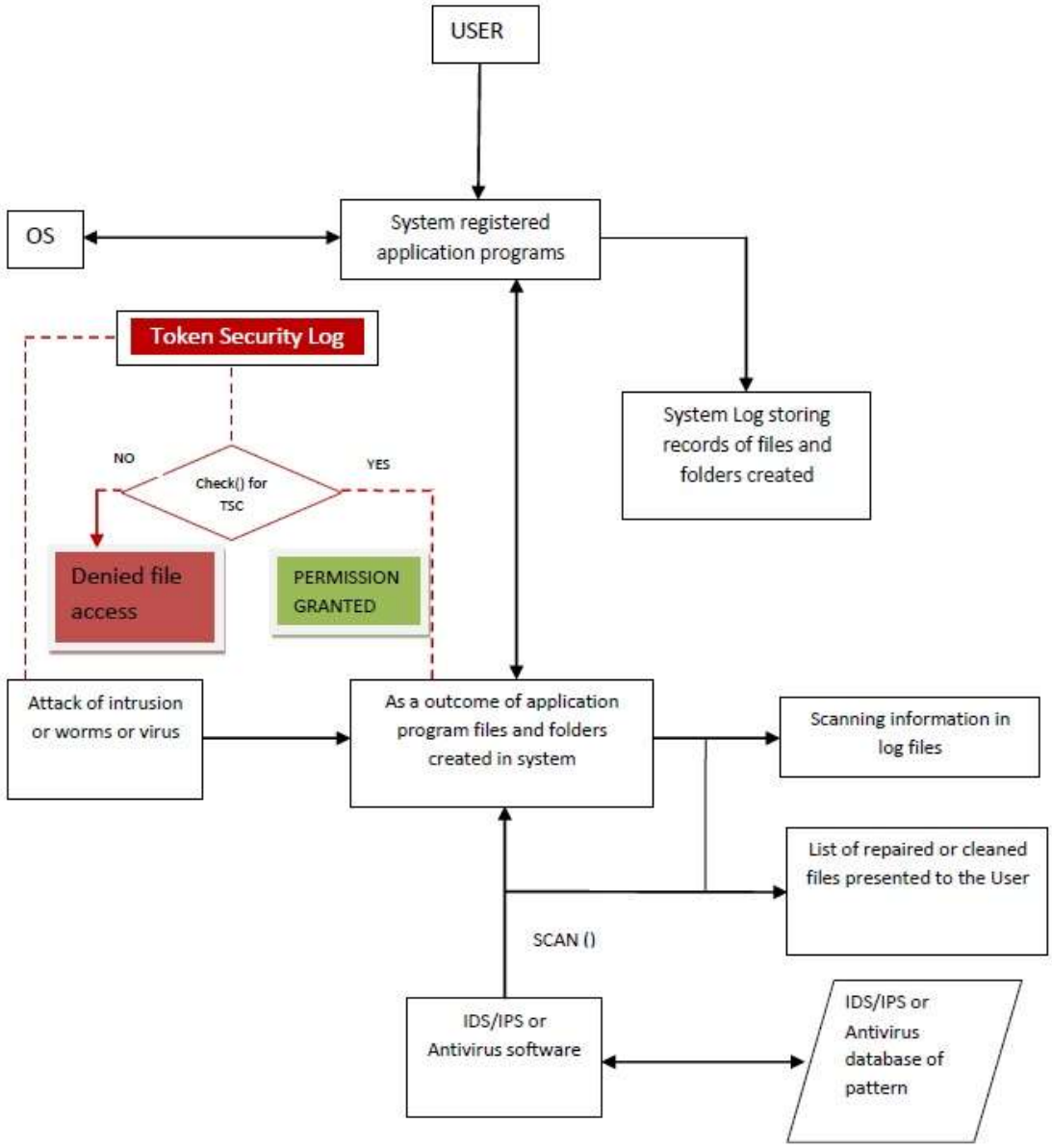

Fig 1. Intrusion Filtration Model

Network User's are getting more dependent on online transaction and computerized system. They are doing most of the dealing through online. Customers are getting habitual of doing routine works through online like bill payments, purchasing, and other communication. Hence attackers are also getting more options to trap the data and make the session vulnerable. Hackers also targeting mass of network users to exploit the authenticity of confidential matters of people, companies, governmental and non-governmental issue. Intrusion detection systems are the tools help us not only to secure the network as well as to find out the source of failure.

The Intrusion Filtration Model will work on all kinds of files. We are proposing a model which will tag all files at the time of its storage and for security purpose issue a token for all files. These tokens will be cross checked when user or any system programs want to access any of the system files. The model can be implemented in operating system as a default feature.

V. CONCLUSION

The Model proposed here will be default security system for all files. The model will work on two step authentication process. In first step we will check for filtered tagged file by checking TSC code in file stream buffer and in second step we will check for the process whether it is authenticated process and registered process of system or virtual process initiated by threats to get entry in system. We are going to use system log and file log features of OS. The logs created because of this will hardly store in few Kbs so no much worry for storage one. Files and folders are secured with encryption code so unauthorized access will be automatically reduced.

VI. ACKNOWLEDGMENT

I Convey my gratitude to all my colleagues and My Supervisor my family members who provoke me directly or indirectly to write and publish the paper. Their motivational behavior has given me courage to complete this paper with all other responsibilities.

REFERENCES

[1] Brenner Susan W. (2007),History of computer crime, https://www. sciencedirect.com/ science/article/pii/B9780444516084500262

[2] "Types of Computer Security: Threats and Protection Techniques", https:// techspirited.com /types-of-computer-security

[3] Rao Umesh H., Nayak Umesha (2014, September 01), History of Computer Security, https://link.springer.com/ chapter/10.1007 /978-1-4302-6383-8_2

[4] kumar Arun (2011, December 12), Trap Doors in Softwares (Trapdoor VIRUS), https://arunkumarhn .wordpress. com/2011/12/12/ trap-doors-in-softwares-trapdoor-virus

[5] Robillard Nicolas, (2004, January), Diffusing a Logic Bomb, https://www. giac.org /paper /gsec/3504/diffusing-logic-bomb/105715

[6] Infosec Institute (2014, May 23), Windows 7 Security Features, https://resources .infosec institute.com/windows-7-security-features/#gref

[7] Sharan Akash(2018, July), Buffer Overflow Attack with Example, https://www.geeksforgeeks .org/buffer-overflow-attack-with-example

[8] Kuperman Benjamin A., Brodley Carla E., Ozdoganoglu Hilmi, Vijaykumar T.N., and Jalote Ankit (2005, November), DETECTION AND PREVENTION OF STACK BUFFER OVERFLOW ATTACKS , https://cacm.acm.org/magazines /2005/11/6077-detection-and-prevention-of-stack-buffer-overflow-attacks/abstract

[9] Synopsys Editorial Team (2017, February 7), How to detect, prevent, and mitigate buffer overflow attacks, https://www.synopsys.com/blogs/software-security/detect-prevent-and-mitigate-buffer-overflow-attacks/

[10] Judge Kevin (2018, August 3), What is a Computer Virus?, https://antivirus.comodo.com /blog/computer-safety/what-is-virus-and-its-definition

[11] Robinson Erin (2012, October 5), What is a Computer Worm?, https://blog. product central.aol.com /2012/10/05/computer-worm

[12] Christopher Roger (2001, October 5), Port Scanning Techniques and the Defense Against Them, https://www.sans.org/reading-room/whitepapers/ auditing/ port-scanning -techniques-defense-70

[13] Rouse Margaret (2017), denial-of-service attack, https://searchsecurity.techtarget. com/definition/denial-of-service

[14] The Windows Club (2017, March 31), Denial of Service Attack: What it is and how to prevent it, https://www.thewindowsclub .com/dos-denial-of-service-attack

[15] Kumar Arun (2011, May 18), " Understanding Computer Security - Types of Computer Security " **,**https://www.brighthub. com/ computing/smb-security/articles/61722.aspx

[16] Delgado Rick (2014, September 23), Digital Dangers: A Brief History of Computer Security Threats, https://www.information security buzz. com/articles/digital-dangers-brief-history-computer-security-threats

[17] Horan Martin (2017, March 15), Main Types of Computer Security Threats That Harm Your Company, https://blog.ftptoday.com/main-types-of-computer-security-threats-that-harm-your-company

[18]Pandey Shailja (2011, May), MODERN NETWORK SECURITY: ISSUES AND CHALLENGES, https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems /15_Security.html

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

[20] Zeidanloo Hossein R., Tabatabaei Farzaneh S., Amoli Payam V. and Tajpour Atefeh (2010, July 12-15), All About Malwares (Malicious Codes), Proceedings of the 2010 International Conference on Security & Management, SAM 2010, July 12-15, 2010, Las Vegas Nevada, USA, 2 Volumes

[21] Computer hope (2018, January 4), Virus, https://www. computerhope.com /jargon/v/ virus.htm

[22] Judge Kevin(2018, August 3), What is a Computer Virus?, https://antivirus. comodo.com /blog/computer-safety/what-is-virus-and-its-definition

[23] Ruddick Gayle (2012, October 11th), What is a Trojan Horse Virus?, https://blog.productcentral.aol.com/2012/10/11/ what-is-a-trojan-horse-virus

[24] INFORMATION SECURITY EDUCATION & AWARENESS IS (2004-2016), Introduction to Operating System Security: What is an operating system?, http://www .infosecawareness.in/draft-syllabus-cbse-os-security-and-cyberlaws

[25] Soffar Heba (2017, April 19), The advantages and disadvantages of Anti-virus software, http://www.online-sciences.com/ computer/the-advantages-and-disadvantages-of-anti-virus-software

[26] Intrusion Detection System (IDS), https://www.techopedia .com/definition/3988/ intrusion-detection-system-ids