IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

WINDOWS REGISTRY ACCESS FOR ENHANCED SECURITY IN DISTRIBUTED SYSTEM ENVIRONMENTS

Mr.Jibin N [1] and, [2]Dr. E.J. Thomson Fredrik

[1]Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore - 641 021.

[2]Professor, Department of Computer Applications, Karpagam Academy of Higher Education, Coimbatore-641 021

Abstract

In this era of fourth industrial revolution everything is moving to digital, and the Cyber security has become a major challenge in this scenario. In this paper we present an intrusion detection mechanism using windows registry access. Microsoft windows operating system is one of extensively used operating system and is every so often attacked. Windows uses registry as database to store its low-level settings for the operating system. All the applications that run on windows will use the windows registry. For a forensic investigator the windows registry is a vital source for the evidence. In this paper we discuss an anomalous behaviour dictator for windows registry. The paper further discuss about here will learn attacks on host machine by looking in the anomalous behavior in windows registry access.

Keywords: **Windows Registry Access, Registry anomaly detection, MAC Address, Motherboard ID, Registry keys**

I. INTRODUCTION

In the last few years, everything is moving towards the digital platform, and cyber security has become the most serious challenge to the information system. Microsoft Windows is the operating system used by most of the users in this era of digitalization. In this pandemic situation there is a huge increase in usage of digital devices and also the number of digital crimes also increased. In the digital investigation process identifying digital evidence is very important. The windows registry is one of the core components that helps the investigators to get the digital evidence related to the cyber crimes that are committed. This paper discusses about the Windows registry and its

keys and its importance from the point of view of cyber investigator for monitoring, observing, and recording activities of a user. This registry repository contains default settings, user and system defined settings of your windows computer. For analyzing or investigation purpose the data from windows registry can be accessed via different registry viewer, Regshot, Registry Browser tools.

II. WINDOWS REGISTRY

Window Registry is a databased that stored on your hard drive, that contains important information about your Windows Operating System and also about the other programs installed on your computer. The Registry is a robust solution that developed by Microsoft for storing so many setting about the software that are implemented in our system. All the programs like the device drivers, service software solutions etc. that are installed on the computer can access the windows registry [1]. We can access the registry files through registry editors. When we open the registry editor, we can see a massive array of items called the registry keys, which contains information about the various activities happened in your computer. When we install a new program on our Windows operating system, a new file is added into the registry that contains information about the program such as program location of installation , version , how to start the program etc. The database also contains information about the user configurations and devices connected to the system [2]. Due to these reasons, we can say very clearly say the windows registry is vital source of information during the MS Windows forensic analysis process. The various settings that are saved in the registry will decide how the system is looked and countered to user request and other configuration, this helps a forensic investigator to get data about the different types of applications used in the system.

III. WINDOWS REGISTRY ARCHITECTURE

The registry contains a hierarchical tree structure with five folders called hives and each folder status with a keyword HKEY, the abbreviation of handle to a key. The nodes in the tree are called key. These keys can contain both subkeys and data entries called its values. In some situation both of these are required but sometimes the program in your computer access the registry and open the key and uses the values associated with it and this can contain any value.

We have five registry hives in the windows registry. The main folders that you can send the windows registry is called Hive and are made of combination of some sub folders. Each sub folder is called keys and subsequently these folders contain sub folders called the sub keys. The table given below (Table:1 Windows registry hives) shows the information about the windows registry hive.

Hive	Description
HKEY_CLASSES_ROOT (HKCR)	It helps to link the files to the corresponding programs and is used by the OS.
HKEY_CURRENT_USER (HKCU).	All the different user level settings and various configurations associated with current logged in users are saved here
HKEY_LOCAL_MACHINE (HKLM)	It is the container for all the software programs settings of your system
HKEY_USERS (HKU)	hold the details about the users including logged in users of the system
HKEY_CURRENT_CONFIG (HKCC)	help us to link the current hardware profile settings in the HKLM

Table: I Windows registry hives

Since the information contained in the windows registry is not limited the physical storage but in the Volatile memory while you do processing. Another scenario while you analyze windows registry is that the registry information may be deleted in such cases you need to recover the data using various windows registry recovery tools.

IV. METHDOLOGY

A. Data Extraction

You can access the registry files from the physical location that are located under the folder Windows\System32\Config. Once the extraction is done it needs to be represented in readable format where the original registry file will be in the .REG format. Regripper tool will help us to do this conversion, where it will convert the .REG file to a .txt file. Another method for accessing the windows registry is from RAM. RAM stores everything passes through it in the plain text format.

B. Data Representation and Analysis

The data that we extracted using window registry need to be represented in the readable format for that purpose we can use the representation using string search. This helps the investigators to search the required keys as well as other available keys. Some major challenges faced by investigators when they tried to analyze the data are lack of data completeness of the data extracted , the time and cost required for the investigation and most importantly the missing data that reduces the accuracy of the result.

C. Real-Time Anomaly Detector

We have a tool called Registry BAM that will collect registry information in the background whenever a read or write happened. So, this can be used as real time anomaly detector. The normal registry usage will be recorded by the RegBAM. This normal usage is analysed, and a threshold is identified and those access exceeding the threshold is considered as anomalous. The users can customize this threshold and can set alarm based on the requirements. This alarm will give use the ability to stop the process that access the registry. This RAD will give facility to get alert about wrong actions taken by the users. The alarm system on the real-time version of RAD also gives the user the ability to kill a running process or to add the specific binary of the process to a whitelist so it is not incorrectly killed in the future. Thus, RAD provides user control over incorrect actions applied by the real-time version of RAD. The audit sensor, model generator and an anomaly detector are the three components of the algorithm. The real time data is gathered by the audit sensor, and it’s stored for the training purposes. The stored data is accessed by the model generator and creates a model for the normal behavior, this model is further used by the anomaly detector to check whether the registry access was consistent or not, if not it will mark that as anomalous access. The RAD data model basically have five features that are gathered from the registry sensor. Firstly, it will store the process name which is trying to access the registry and the query being sent to the registry will be stored. Then it stores the actual key that was accessed. That is very important here.

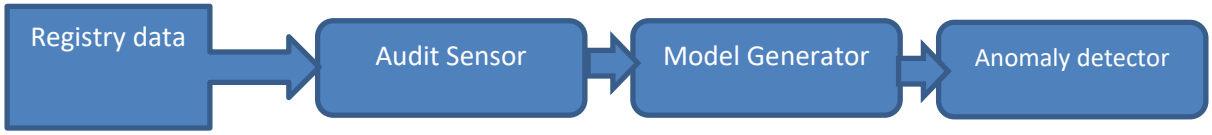

Figure: I Anomaly detector

C. Client Server communication anomalous behavior Detection

In client server architecture model of communication, the IP address and MAC address and disk and motherboard ID are unique and can be used. HKEY_CURRENT_USER hold the current logged in user and also the IP, MAC address and can be retried from Windows Registry of client and server are compared. The unique id of mother board and hard disk ID can be used to identify the users who are using the system maliciously. This can be done in two phases.

In first phase all the information about the users who is trying to connect to the server is collected and if the address and other information matches with the data in server, then user is identified as white list user and they are allowed to access to the server. The second phase followed by our phase one will check whether the IP is blacklisted or not if yes it will block that anomalous access.

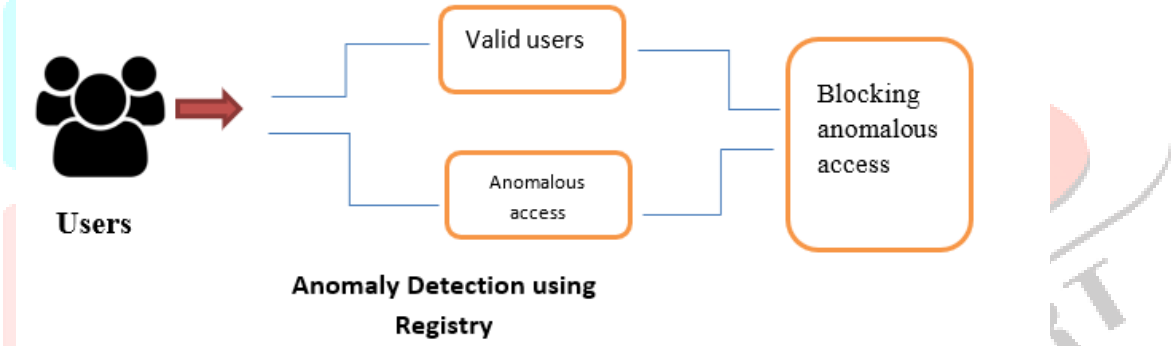

Figure II: Anomaly Detection using Registry

V. RESULT AND DISCUSSIONS

The registry data extracted from the physical sources, and it is found that the data is 99% accurate. Windows registry as we have discussed is an effective source of evidence for cyber investigations and also to prevent manicous access to the registry. When any client request something from the sever, it is responsible for providing the requested data or content, but there is certain situation where the client may not be valid. The IP base protection have some drawbacks and it can be overcome by the use of MAC and Mother board ID and hard disk ID is used for protection against such anomalous access. This ensures better prevention mechanism against such activities.

VI. CONCLUSION

In this highly connected world, we need to ensure the security and privacy. The windows registry has been identified as repository of user information and other operating system related information. Whenever some activities are happening in the related data will be stored in registry. The running programs will access some of the keys in the registry also and this will help to get some important information about the user activities also. The anomaly detection tool helps to identify the users that are not supposed to access the server and also can identify the anomalous access by using this anomaly detector

VII. REFERENCES

[1]. Vintaytime, "6 Best Most Popular Desktop Operating Systems in the World," 2017. [Online]. Available:

[2]. J. Kennedy and M. Satran, "Registry," 2018. [Online]. Available: https://docs.microsoft.com/en us/windows/desktop/sysinfo/registry. [Accessed: 23-Jun-2019]

[3]. B. Singh and U. Singh, "A forensic insight into Windows 10 Cortana search," Comput. Secur., vol. 66, pp. 142–154, 2017

[4]. T. Roy and A. Jain, "Windows Registry Forensics: An Imperative Step in Tracking Data Theft via USB Devices," Int. J. Comput. Sci. …, vol. 3, no. 3, pp. 4427–4433, 2012

[5]. D. N. Patil, "RegForensicTool: Evidence Collection and Analysis of Windows Registry," Int. J. CyberSecurity Digit. Forensics, vol. 5, no. 2, pp. 94–105,2016.

[6]. Yet Another Registry Utilility (YARU), 2012 TZWorks Limited liability Company http://tzworks.net/prototype_page.php?proto_id=3

[7]. P. Tuli, P. Sahu, "System Monitoring and Security Using Keylogger," International Journal of Computer Science and Mobile Computing, Vol.2, Issue 3, 2013, pp:106-111

[8]. A.Sivaprasad and S. Jangale, "A Complate Study on Tools and techniques for Digital Forensic Analysis", 2012 International Conference on Computing, Electronics and Electrical Technologies (IECCEET), 2012, pp: 881 – 886

[9]. A. Vastel, P. Laperdrix, W. Rudametkin, and R. Rouvoy, "Fp-Scanner: The Privacy Implications of Browser Fingerprint Inconsistencies," in 27th USENIX Security Symposium (USENIX Security 18), Aug. 2018, pp. 135– 150.

[10]. "Google Safe Browsing API (v4)," 2020, accessed 21 Feb 2020. [Online]. Available: https://developers.google.com/safe-browsing/v4

[11].] W. Meng, B. Lee, X. Xing, and W. Lee, "TrackMeOrNot: Enabling Flexible Control on Web Tracking," in Proceedings of the 25th International Conference on World Wide Web, 2016, pp. 99–109

[12]. S. Englehardt and A. Narayanan, "Online Tracking: A 1-Million-Site Measurement and Analysis," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1388–1401.

[13]. Eleazar Eskin. Anomaly detection over noisy data using learned probability distributions. In Proceedings of the Seventeenth International Conference on Machine Learning (ICML-2000), 2000

[14]. H. Carvey, Windows registry forensics: advanced digital forensic analysis of the Windows registry, Amsterdam:Syngress, an imprint of Elsevier, 2016.

[15]. SANS Digital Forensics and Incident Response Blog", SANS Digital Forensics and Incident Response Blog | Finding Registry Malware Persistence with RECmd | SANS Institute.

[16]. Y. Kim and D. Hong, "Windows Registry and Hiding Suspects' Secret in Registry", 2008 International Conference on Information Security and Assurance (isa 2008), pp. 393-398, 2008.

[17]. Z. Tang, H. Ding, M. Xu and J. Xu, "Carving the Windows Registry Files Based on the Internal Structure", 2009 First International Conference on Information Science and Engineering, pp. 4788-4791, 2009

[18]. T. D. Morgan, "Recovering deleted data from the Windows registry", Digital Investigation, vol. 5, 2008.

[19]. Shuhui Zhang, Lianhai Wang and Lei Zhang, "Extracting windows registry information from physical memory", 2011 3rd International Conference on Computer Research and Development, pp. 85-89, 2011.

[20]. Giulia Bruno, Paolo Garza, Elisa uintarelli, Rosalba Rossato," Anomaly Detection in XML databases by means, IEEE July 2007.

[21]. Xiuyao Song, Mingxi Wu, Christopher Jermaine, and Sanjay Ranka" Conditional Anomaly Detection", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 19, NO. 5, MAY 2007.