**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 5.258**

***IJCSMC, Vol. 5, Issue. 5, May 2016, pg.708 – 712***

# A Review of Logs, Protection of Log data & Computer Forensics

**Sourabh Choudhary, Dr. Deepti Sharma**

Advanced Institute of Technology and Management, Palwal

Advanced Institute of Technology and Management, Palwal

Email: Sourabhchoudhary1989@gmail.com, deeptiguria@gmail.com

---

***Abstract- Computer forensics process use log file data in finding electronic evidences for criminal investigations. Log files help in seizing computer and keeping records for use as evidence in federal rule of law. Log file are the files which are used to record the events that occurred in the operating system, message passing between different users of communication system or any software that runs on operating system. Thus logs are closely related to computer forensics. In order to ensure that logs are appropriate for court of law, it should be ensured that they are not tempered after being generated. Therefore it should be ensured that logs are authenticated and trust-worthy. In this paper, we will discuss the log file, their existing protection methods and management issues.***

***Keywords- trusted computing, log, forensics, secure log, protection log***

---

## I. INTRODUCTION

Forensics in computer industry is most growing concerns in these days [1]. Forensics in computer industry is same as in forensics in human world. In forensics, detectives track what happened at the crime scene, who did the crime, and what the criminal do to whom. In computer forensics, same method applies. Here the crime scene is the machine which is being hacked, the entity to which computer belongs is the victim and hacker who hacked the system is the criminal. Logs are the evidence that proves that some crime has occurred in the scene. Log file are the trail left behind by the hacker, which are the evidence of the crime scene. Thus computer forensics to be effective and validated, one must ensure secure, trust-worthy and accurate log data in file [2].

 

## II. LOG FILE

Log data is used to describe the behavior of events that occurred in the operating system, applications running on the operating system, user's interacting with the system or other services accessing the operating system's service. When the system is booted, one can find loopholes in the working of system by analyzing the logs, identifying weak areas in security, finding possible attacks and thus based on that take appropriate measures to enhance and straighten network control. Thus, logs security and trust-ability are important for maintenance and effective monitoring of the system [3]. This concludes that logs are important source for security audits system, due to this attackers mostly modify the data in logs to hide their behavior of invasion.

## III. EXISTING PROTECTION METHODS OF LOG

The main characteristics which ensures that security protection of logs is there is that log data is not changed. In other word, security of logs data ensures that log is trust-able. The integrity protection of logs can be ensured by Trusted Computing Base (TCB). Because trusted computing base is exposed with many vulnerabilities, that is why intruders are able to hack, which makes this protection unreliable. In current world, we have many log data protection methods, but in this section, we will cover four methods and problems associated with them.

Write-once media: This method is used to write-once media to store the log data. Thus because log are stored on the media which can be written once, so the log data cannot be altered. The problem with this approach is that with more data in logs, more hardware is required which also increases hardware cost.

Trusted host: This method is to transfer the log data to another host which has more security and protection level. This however requires another host machine where log data can be stored, ensuring that transferring the logs doesn't tamper the data.

Access Control: This method states that access control mechanism should be used for accessing the log data. As this requires special feature provided by operating system, it cannot be used for general users.

Encryption: This method states that encryption should be used to secure and protect log data. The problem with this approach is that restoring the log data is bit difficult [4].

| Feature / Method | Impossible to alter | Defect abandon | Applicable to application |
|---|---|---|---|
| Write-once media | ⊕ | | |
| Trusted host | ⊕ | | |
| Access Control | ⊕ | | |
| Encryption | | ⊕ | ⊕ |

## IV. CYBER FORENSIC REQUIREMENTS

Cyber Forensics to presentable in court of law, evidences need to be authentic, accurate, reliable, and admissible and trust worthy [3]. As per Dixon et al. [5], the end result of digital forensics should be confidential, have integrity and authenticity for identification, extraction, documentation and interpretation of data.

 

Thus to maintain the viability of digital forensics, a "chain of custody" has to be made and that has to be created following legal investigation procedures in picture [6].

In current available implementations, structures are manipulate-able and protocols used are vulnerable to intrusion and modification. This makes the evidence weak. A known example which is documented that Linux/Unix syslog were not designed and implemented keeping forensics in mind but were more of way to collect and consolidate debugging output from different events which occurred in the operating system [7].

## V. LOG FILES IN CYBER FORENSICS

The most important element of cyber forensics is authenticity of evidences presented in court of law. Just like airplane has black box in it, which tracks every event that occurred within it, same way logs track every event that occurs within the system, application interacting with the system and networks interaction with the system. Log files composed of log data that provide the data of events occurred in the system or network. Log data is created for each event that occurred in the system. The data in log files is the different entities of events which are required to understand the situation of the system when that log is created for the events [9].

## VI. LOG MANAGEMENT

With the evolution of Information technology field across the world, the number of forgery, threats and by-passing the security has greatly increased. Thus revolution of computer security started which require the log management and integrity to be need of the hour. Log management is required to ensure that log data is stored securely with complete details for appropriate time frame. Thus log management states to ensure that creating, transmitting, storing along with analyzing and disposing of log data is done under secure environment and that no tempering of log data is done. Thus the key characteristics to ensure are confidentiality, integrity, completeness and availability of logs.

## VII. CHALLENGES IN LOG MANAGEMENT

This section will discuss the common types of challenges. We mainly divide these into three groups. First one is the availability, confidentiality and integrity of generated logs could be compromised knowingly or unknowingly. Second is that there could be several problems with the generation of logs. This could be because of various different types and format of logs and their prevalence. Third one can be the person or people responsible for analyzing the log can be ineffectively prepared or reinforced.

1. Log Generation and Storage

This section covers the impact of different types of logs being generated from different source like operating system, security software and third party applications interacting with the system. This obscures log management in many ways, which are as follows

Multiple Log Source - As logs can be found in n-number of hosts in the same organization, so log management should be conducted thought out the organization. Even single log generation source can generate multiple logs of different types. A simple example of this would be a login application storing logged user event and network event in different log file.

Heterogeneous Log Content – As log file contains log data, which is nothing but certain piece of information of event occurred like in case of network activity, it would be client IP Address, server IP address, data requested, number bytes sent from server etc. As different server log data differently based on the different parameter, so it is difficult to make relationship between different log source and files. Sometime, the representation of log data even varies a lot. One such example would be date time of event occurred. One serve might log only date while other may log date and time as well. Also date format can vary like YYYY-MM-DD and other being DD-MM-YYYY [10], [11].

Inconsistent Timestamps – Timestamps are mostly being stored with every log record so as to identify each record uniquely. Inconsistent timestamp arise when different server have different local clock but records event same time. Thus if same event being recorded at two different server with different clock, their timestamp will be different.

 

Multiple Log Formats – Even the log format vary from server to server. Some server log data comma-separated, while can use tab separated text file. Some server use database tables to log the event. Extensible markup language (XML) format logging is used for human to easily read the log.

2. Log Protection

Records of system and network security are being recorded in log, so these should be secured and protected from breach and it should be ensured that their integrity and confidentially is maintained. The simple example of log data would be user credentials, his personal information which might be intentionally or inadvertently be stored in the server as log data. This causes privacy concern for the individual as his credentials and personal information is being compromised. The person accessing those logs as well as intruder can access to that information. If logs are not stored with security then those are susceptible to intentional and unintentional modification. The result of unsecured logs will be malicious activities being gone unnoticed or not able to identify the changes done by intruder. For example, malicious software are there which even removes the existence of logs source from log data [11], [12].

The availability of log is other important factor which organization should consider. Many logs have maximum limit on size or number of records that a single record file can store. When these limit are reached, log data may override the old log data. This can result in lose of historic log data, thus causing log unavailability. To overcome this, we should keep copies of log file. We can either take backup of old file before new log data override the old data. Or we can create a new log file with timestamp attached at the end of log file name and store new log data in that log file. If volume of logs is concern then we can only backup the required log data leaving log data that do not require to be archived. During this methods, confidentiality and integrity of logs should be ensured.

3. Log Analysis

Log analysis has been traditionally the responsibility of network and system administrator in the organization. This task has been mostly considered as low priority by administrator and management as well. Other task of administrator such as resolving security issues, handling operational vulnerabilities are considered more important. No training or special hand-on exercise is provide to administrator for handling the analysis of log data effectively and efficiently. Even traditionally, no effective tools were provided to help administrator in doing log analysis because of cost incurred to achieve license of those tools. Another problem is that this task of analysis of logs is considered to be boring and overhead, which provide little or no benefit as compared to time required to perform this task. The tendency is to do analysis after the problem occur but not as regular exercise. Traditionally, logs were not analyzed in real time, which caused the value of logs significantly condensed [12].

## VIII. CONCLUSION

Log data are used to store and evaluate the behavior of machine when some event occur inside machine or when some external application interact with the machine. Log file help in troubleshooting and efficient system administration in providing significant assistance in finding malicious end user in computer forensics. Since log file comprise of confidential information of individual, so these must be protected. Thus log security and authenticity should be ensured when used in court of law.

# REFERENCES

[1] Kessler, M. G. (2006) Kesseler's Corner: The growing field of computer forensics. The Kessler Report, 9(1), 7.

[2] Bernie Lantz, Rob Hall, Jason Couraud, "Looking Down Log Files: Enhancing Network Security By Protecting Log Files" Issues in Information Systems Volume VII, No. 2, 2006

[3] Lin Hui, Dou Min.Secure defense of system 10g[J]. Computer Engineering , 2003,29 (17) .

[4] Tetsuji Takada , Hideki Koike, NIGELOG: Protecting Logging Information by Hiding Multiple Backups in Directories

[5] D. Brezinski and T. Killalea, "Guidelines for evidence collection and archiving," United States, 2002.

[6] P. D. Dixon, "An overview of computer forensics," Potentials, IEEE, vol. 24, no. 5, pp. 7–10, Dec. 2005.

 

[7] T. Ceresini, "Maintaining the forensic viability of logfiles," SANS Institute, As part of GIAC practical repository, 5 2001.

[8] S. Peisert, "Forensics for system administrators," vol. 30, no. 4, pp. ??–??, Aug. 2005.

[9] Pavel Gladyshev "Formalising Event Reconstruction in Digital Investigations" Ph D. dissertation Department of Computer Science, University College Dublin, 2004.

[10] Carrier, B.D., Spafford, E.H "Defining Digital Crime Scene Event Reconstruction" Journal of Forensic Sciences, 49(6). Paper ID JFS2004127,2004

[11] Karen Kent and Murugiah Souppaya, "Guide to Computer Security Log Management", Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, 2006

[12] Stevens, M.W. "Unification of relative time frames for digital forensics", Digital Investigation journal, 1(3), pp. 255-239, 2004

## BIOGRAPHY

**Mr Sourabh Choudhary** is a M.Tech Scholar in the department of CSE at Advanced Institute of Technology & Management, Palwal, Haryana, India.

**Dr. Deepti Sharma** is Asistant Professor and Head in Computer Science Engineering Department in Advanced Institute of Technology & Management, Palwal.

 