Host Based Automated Digital Forensic Technique with Intrusion Detection Systems

Aher M. R[1], Gadge L. P[2], Jadhav V. B[3], Yewale D. S[4].
BE Computer Engg. S.V.C.E.T. Rajuri, Pune-412410[1, 2, 3, 4]
ahermayur999@gamil.com[1] *laxman.gadge08@gmail.com*[2] *jadhav.viju17@gmail.com* [3]
ydeepak999@gmail.com[4]

***Abstract*—Now a day's lot of the users use ids and password as login pattern for the authenticate users. However making patterns is weakest point of computer security as so many user share the login pattern with the co-workers for the completed co-task, inside attacker is attacked internally and it will be valid attacker of system, As using intrusion detection systems and firewalls identify and isolate harmful behaviors generated from the outside world we can find out internal attacker of the system only. In some of the studied define examine that system calls generated by some commands and these command help to find detect accurate attacks, and attack patterns are the features of an attack. However in the paper security System define as the Internal Intrusion Detection and Protection System (IIDPS), is help to detect internally attacks by using data mining and forensic technique at SC level. For the track the information of users usages the IIDPS creates users' personal profiles as their forensic features and investigate that the valid login user is account holder can login or not by comparing his/her current computer usage behaviors with the patterns collected in the account holder's personal profile. The experimental results demonstrate that the IIDPS's user identification accuracy is 94.29%, whereas the response time is less than 0.45 s, implying that it can prevent a protected system from insider attacks effectively and efficiently.**

***Index Terms*—Data mining, insider attack, intrusion detection and protection, system call (SC), users' behaviors.**

I. INTRODUCTION

HIS document In the past 10 years, computer systems Thave been largely employed to provide users with easier and more perfect lives. However, System securities is the one of the serious issue in computer domain when users take advantages of powerful capabilities since attackers very usually try to forcely enter in the computer systems and behave spitefully or harmfully, e.g. corrupt critical data of a company, making the systems out of work or destroying the systems. pharming attack, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack generally all this attack are well known attacks [1], [2], insider attack is most difficult for the detected because firewalls and intrusion detection systems (IDSs) normally fight against outside attack. Now days, To Authentic users, most systems check user ID and password as a login pattern. However, attackers may be install Trojan to hack the password and When successful, they may then log in to the system, access users' private files, or modify or destroy system settings. Fortunately, most current host-based security systems [3] and network-based IDSs [4], [5] can discover a known intrusion in a real-time manner. Attack packets are often issued with forged IPs or attackers may enter a system with valid login patterns that's why it's very difficult to identify who is attacker. However in Operating System level system calls (SCs) is more helpful to find out attacker and identify the exact attack [6], processing a large volume of SCs, detecting harmful behaviors from them, and detecting possible attackers for an intrusion are still engineering challenges Therefore, in this paper, we propose a security system, at SC level which detects harmful behaviors launched toward a system named Internal Intrusion Detection and Protection System (IIDPS). To mine system call patterns (SC-patterns) defined as the longest system call sequence (SC-sequence) that has repeatedly appeared several times in a user's log file for the user the IIDPS uses data mining and forensic profiling techniques. The user's forensic features, define is as an SC Pattern find out in submitted by users SC sequences but normally used by other users computer usage history.

The contributions of this paper are: 1) identify a user's forensic features by analyzing the corresponding SCs to enhance the accuracy of attack detection; 2) able to port the IIDPS to a parallel system to further shorten its detection response time; and 3) effectively resist insider attack.

II. Literature Survey

In Computer forensics science, we can views computer systems as crime scenes, aims to identify, preserve, recover, analyze, and present facts and opinions on information collected for a security event [7]. exactly what attacker done such things will be recognized such as spreading computer viruses, malwares, and malicious codes and conducting DDoS attacks [8].Intrusion detection techniques most of the focus on how to find harmful network behaviors [9], [10] and based on the histories recorded in log files we acquire the characteristics of attack packets, i.e. attack patterns[11], [12]. In [13] Author used self-developed packets for compare to collect network packets with which to discriminate network attacks with the help of network states and packet distribution. In [14] from system log files we acquired network intrusion and attack patterns. These files contain tracked information of misuse computer. It means that, from synthetically generated log files, these traces or patterns of misuse can be more accurately reproduced. In [15]Author overviewed research progress of applying methods of computational intelligence, including artificial neural networks, fuzzy systems, evolutionary computation, artificial immune systems, and swarm intelligence, to detect malicious behaviors.

The author can compare different intrusion systems and systematically summarized the details hence allow us to described existing research challenges. To network security these aforementioned techniques and applications truly work finely. When unauthorized user log in to the system with valid ID and password that time they not able to easily authentic remote login user and detect specific type of intrusion. In previous work [16], for collects forensic features we can use security system for users at command level rather than at SC level, by invoking data mining and forensic techniques, was developed. Moreover, if attackers use many sessions to issue attacks, e.g., multistage attacks, or launch DDoS attacks, then it is not easy for that system to identify attack patterns. In [17] Author presented an intelligent lightweight IDS with the help with this forensic technique identify users behavior and a data mining technique to carry out cooperative attacks. The authors claimed that the system could detect intrusions effectively and efficiently in real time. However, they did not mention the SC filter. In [18] Author provided another example of integrating computer forensics with a knowledge-based system. For allowing SC Sequence to be executed, the system adopt predefine model. Same will be employed by a detection system to restrict program execution to ensure the security of the protected system. And same will be needful the identified issue a series of harmful SC's and on the knowledge based identified attack sequence which have been collected.

When an undetected attack is presented, the system frequently finds the attack sequence in 2 s as its computation overhead. In [19] Author explored the effectiveness of a detection approach based on machine learning to combine the expressive power of generative models with good classification accuracy capabilities to infer part of its knowledge from incomplete training data so that the network anomaly detection scheme can provide an adequate degree of protection from both external and internal menaces. In [20] to enhance the security of advanced metering infrastructure through an IDS Author analyzed the possibility of using data stream mining. The advanced metering infrastructure is crucial part of smart card which works as bridge for operating both side of information flow between the user's domain and the utility domain.

III. Proposed System

Use In this approach, log file is stored into two different forms as well as in two different places. Log file in plain text from is stored on target host and a copy of same log file is stored in another host called log manager. When intruder tried to acquire log file IDS running on the based host to detect exact intrusion and then it will be give an alert to security administrator about the intrusion which is take require decision to mitigate them.

A. System Framework

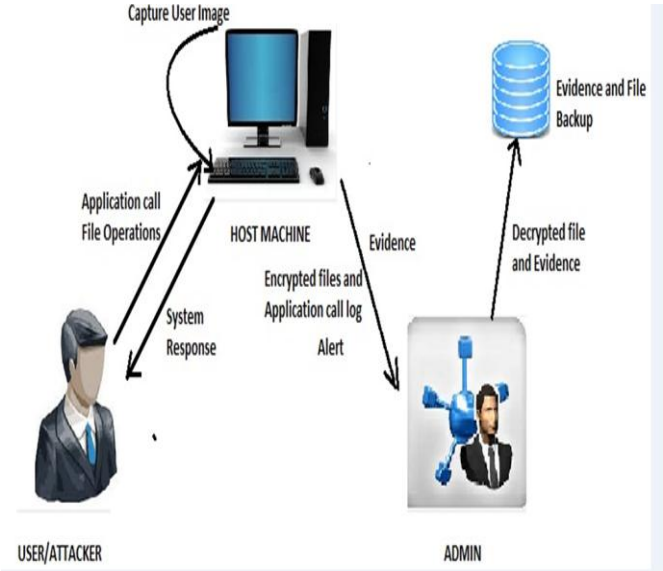

Fig.1 System architecture

1. Target Host

In the Target Host, Crucial data (i.e. log files) is stored. To preserve the integrity and confidentiality need to be Continuous monitor of log file is prime requirement of the data stored in it. To achieve this, IDS is deployed on target host and it is a continuous process round the clock. Whenever an attacker tries to intrude the target host, IDS running on

target host detects the intrusion; sends an alert message to security center as well as log server. After that it will be capture the state of the system (RAM image and log file image) by using Digital Forensic Tool. Then the captured log file has been compared to previous log file image to confirm the intrusion. Target host is nothing but our OS as it was host based system. The intrusion can try to use information of the system but if he tries to make changes in the system properties and access the access the records then IDs comes in to the picture.

2. Server

Server maintained the copy of the log file in an encrypted form. Log file maintained the Encryption keys and it kept secret. Periodically back up of the Target host log file is taken and it is stored on the log server. It will be receiving log file as backup and encrypted the file and store within it. Whenever the log server receives an alert message from target host, it decrypts the log file, computes the image of the decrypted log file using digital forensic tool and sends it to the target host to perform the comparison. The main job of the Log server is encryption and decryption of log files such that the intruder doesn't have access to them. If the intruder gets to know the location and condition of the log file shall only be available with the owner and nobody else. It shall be provided at the time of delivering the software as a complete product.

3. SECURITY CENTER (ADMIN)

This is the system used by the security administrator to monitor the alerts generated by IDS. It receives alerts from Target Host. Once the target host has sent the alert to the Security center, the job of the Security center starts. The attack is hence detected and looked into at the Security center. The Security center is the most essential component of the IDS. Its job is track the intrusion he tries to hack the system, an alert should be sent to the real owner. This will be accomplished by webcam image and same will be prove the again court of law. If the intruder tries to access the files without the net connection, the system shall shut down by itself within 10 seconds, and if he has the net connection intact, then we shall also be able to inform the true owner about the intrusion with the help of an e-mail.

In proposed system we are detecting the intrusion through many things like integrity, checking currently running processes by key log etc. These all activities are performed by user. The first activity is file integrity. We are detecting intrusion through file integrity. In file integrity concept if any user delete the file or modify file or insert file into specific directory then by using our system we can detect it. If any file delete or modify of insert into specific folder then that file will save in folder which is specified by client. Then file integrity log send to server. Server sends the integrity of that file to the clients email id. So that client will easily know which file is modified. So that we can recover that modified files from specified backup folder.

B. Flow of System

This system can be used to detect the host intrusion detection where host machine comprises the confidential files. Attackers can attack on host machine that attacks would be detected by the system and updated files can be recovered by system. This system can detect the files modification and also prevent the file modification. If files deleted from the host machine permanently then system cant recovered the files.

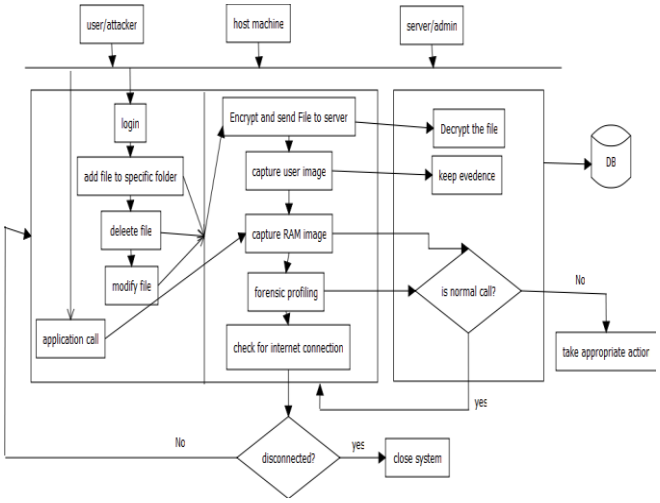

Fig. System flow

C. Algorithms

- Input: U's log file where U is user of the host machine.
- Output: U's habit file or Attack Detection.
- Procedure:

```
G = |LogFile|-|SlidingWindow|
|SlidingWindow| = |L-Window| = |C-Window|
 for(i = 0; i < G-1; i++)
{
  for( j = 0; j < G-1; j++)
 {
   add K grams of L window in L window
   add K' grams in current C window
```

Compare K-grams and K' grams with subsequent algorithm.

```
If (the identified pattern is already existing in habit file)
  Increase count of SC- pattern by 1
  Else
 {
  Check the pattern in attacker profile
  If (Present in profile)
  Insert SC-pattern into habit file with counter = 1
   Else
 Consider as attack.
  }
 }
}
```

IV. EXPERIMENTAL RESULT

The proposed technique applied on system call this process are shown below:

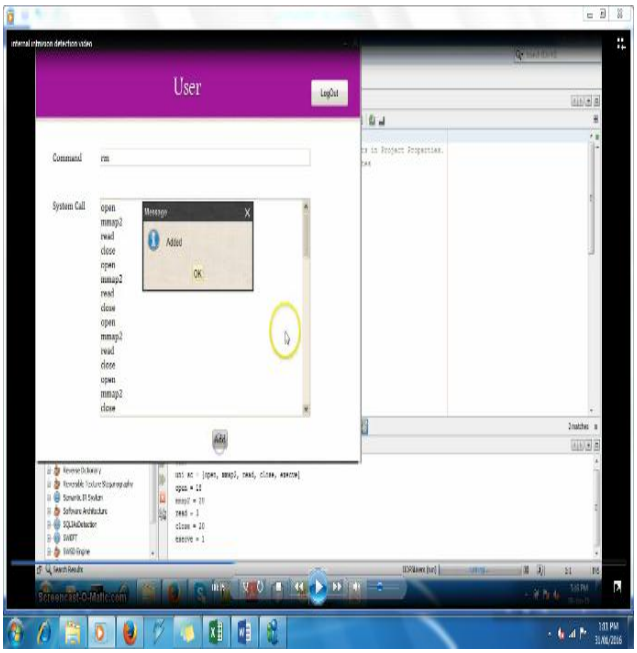

Fig.1 User added in System Call

This is the user GUI where user will access the commands of computer and try to attack on the computer. From here user or attacker can access the files of computer. If misbehave detected then alert will send to the administrator of the system.

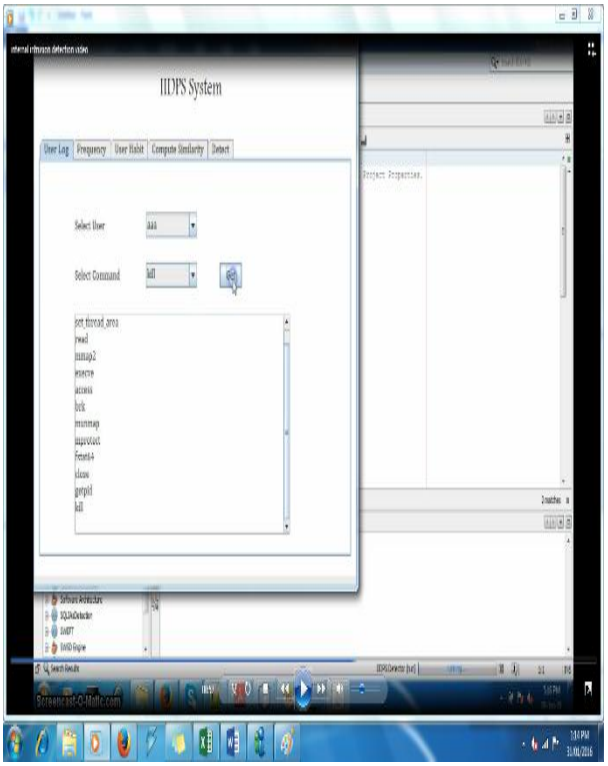

Fig. 2 Select User and Command

In the second screen shot it shows the command accessed by the user of system. Here user can access the commands or system calls for which he has permission. Here attack is detected. To detect the attack here we have used common habit generation algorithm. This will detect the malicious activities done by user.

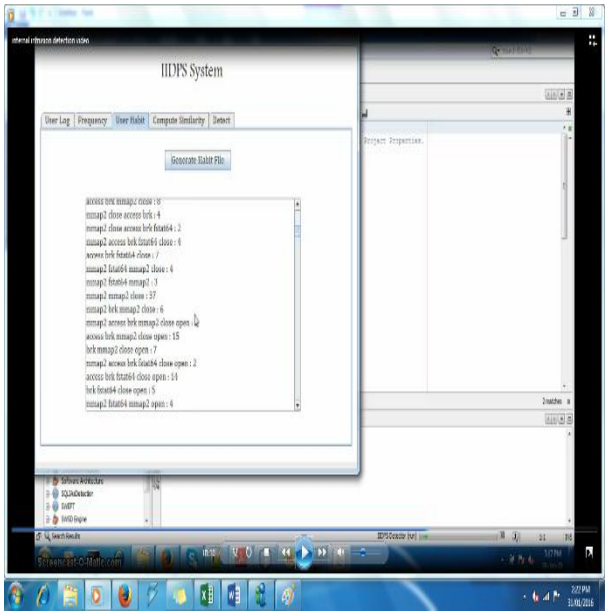

Fig.3 Generate Habit File

System can generate habit file.

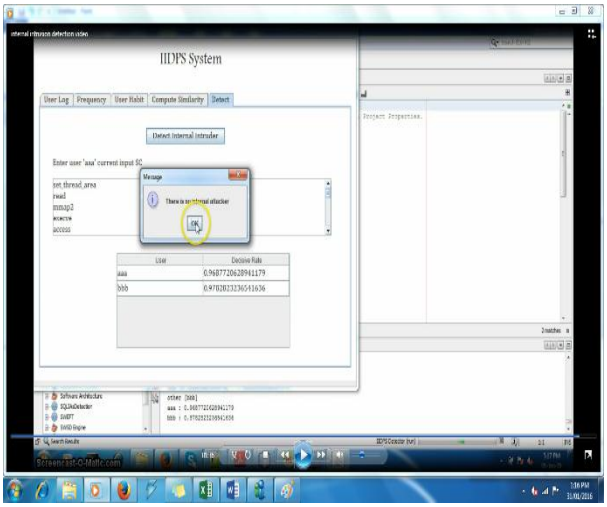

Fig.4 Detect internal intrusion

To detect the attack here we have used common habit generation algorithm. This will detect the malicious activities done by user.

V. ACKNOWLEDGMENT

We are thankful to our project guide Prof. Shaikh T. S. for her proper guidance and valuable suggestions. We are really grateful to them for their kind support. We are grateful to Prof.

Patil H. K., Head of Computer Engineering Department, S.V.C.E.T. Rajuri for his indispensable support, suggestions. We are also greatly thankful to other faculty member and our friends to help us.

VI. CONCLUSION

In this paper for the identify SC pattern for the user we can use data mining and forensic technique. Most commonly used SC-patterns are filtered out when the time that a habitual SC pattern appears in the user's log file is counted, and then a user's profile is established. By identifying a user's SC-patterns as his/her computer usage habits from the user's current input SCs, the IIDPS resists suspected attackers. The experimental results demonstrate that the average detection accuracy is higher than 94% when the decisive rate threshold is 0.9, indicating that the IIDPS can assist system administrators to point out an insider or an attacker in a closed environment. The further study will be done by improving IIDPS's performance and investigating third-party shell commands.

References

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers—Or how to thwart a phisher with trusted computing," in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, Apr. 2007, pp. 120–127.

[2] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.

[3] Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 1–10.

[4] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," J. Parallel Distrib. Computer. vol. 68, no. 4, pp. 427–442, Apr. 2008.

[5] H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation based malware behavioral concise signature generation," Inf. Commun. Technol., vol. 7804, pp. 271–284, 2013.

[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.

[7] M. K. Rogers and K. Seigfried, "The future of computer forensics: A needs analysis survey," Computer. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.

[8] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web based DDoS attack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.

[9] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1–5.

[10] Z. A. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," Computer. Commun., vol. 34, no. 3, pp. 468–484, Mar. 2011.

[11] H. S. Kang and S. R. Kim, "A new logging-based IP traceback approach using data mining techniques," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 72–80, Nov. 2013.

[12] K. A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera, "Analyzing log files for postmortem intrusion detection," IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev., vol. 42, no. 6, pp. 1690–1704, Nov. 2012.

[13] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in Proc. Int. Conf. Commun. Softw. Netw., Singapore, 2010, pp. 313–317.

[14] S. O'Shaughnessy and G. Gray, "Development and evaluation of a data set generator tool for generating synthetic log files containing computer attack signatures," Int. J. Ambient Comput. Intell., vol. 3, no. 2, pp. 64–76, Apr. 2011.

[15] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Computer., vol. 10, no. 1, pp. 1–35, Jan. 2010.

[16] F. Y. Leu, K.W. Hu, and F. C. Jiang "Intrusion detection and identification system using data mining and forensic techniques," Adv. Inf. Computer. Security, vol. 4752, pp. 137–152, 2007.

[17] Z. B. Hu, J. Su, and V. P. Shirochin "An intelligent lightweight intrusion detection system with forensics technique," in Proc. IEEE Workshop Intell. Data Acquisition Adv. Computer. Syst.: Technol. Appl., Dortmund, Germany, 2007, pp. 647–651.

[18] J. T. Giffin, S. Jha, and B. P. Miller, "Automated discovery of mimicry attacks," Recent Adv. Intrusion Detection, vol. 4219, pp. 41–60, Sep. 2006.

[19] U. Fiore, F. Palmieri, A. Castiglione, and A. D. Santis, "Network anomaly detection with the restricted Boltzmann machine," Neurocomputing, vol. 122, pp. 13–23, Dec. 2013.

[20] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-streambased intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," IEEE Syst. J., vol. 9, no. 1, pp. 1–14, Jan. 2014.