International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Insider Interruption Identification and Protection by using Forensic Technique

Sale Kajal Ramchandra[1], Shinde Prajakta Sanjay[2], Waghmode Nikita Dashrath[3], Komal Kambale S[4]

[1,2,3,4]*Department of computer Science and Engineering, Shriram Institute of Engineering and Technology Centre, Paniv-Solapur, Maharashtra, India.*

Abstract:- Now a day's lot of the users use ids and passwords as login pattern for the authenticate users. However, many people share their login patterns with coworkers and request these coworkers to assist co-tasks, thereby making the pattern as one of the weakest points of computer security. Insider attackers, the valid users of a system who attack the system internally, are hard to detect since most intrusion detection systems and firewalls identify and isolate malicious behaviors launched from the outside world of the system only. In addition, some studies claimed that analyzing system calls (SCs) generated by commands can identify these commands, with which to accurately detect attacks, and attack patterns are the features of an attack. Therefore, in this paper, a security system, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. The IIDPS creates users' personal profiles to keep track of users' usage habits as their forensic features and determines whether a valid login user is the account holder 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.

***Key Words*: Data mining, insider attack, intrusion detection and protection, system call (SC), users' behaviour's.**

1. INTRODUCTION

In the previous decades, PC frameworks are wide used to create clients with simpler and extra advantageous lives. In any case, when people abuse incredible capacities and procedure intensity of workstation frameworks, security has been one in everything about serious issues inside the PC space since assailants appallingly some of the time endeavor to infiltrate PC frameworks and carry on malevolently, e.g., taking essential information of an association, making the frameworks out of work or possibly wrecking the frameworks. By and large, among all outstanding assaults like pharming assault, conveyed forswearing of-administration (DDoS), listening in assault, and lance phishing assault, corporate official assault is one in everything about most troublesome ones to be recognized because of firewalls and interruption identification frameworks (IDSs) once in a while safeguard against outside assaults. To prove clients, presently, most frameworks check client ID and word as a login design. Be that as it may, aggressors could introduce Trojans to filch unfortunate casualties' login examples or issue a larger than average size of preliminaries with the assistance of a dictionary to store up clients' passwords. When thriving, they'll at that point sign in to the framework, get to clients' non-open records, or alter or decimate framework settings. Serendipitously, most current host-based security frameworks and system based IDSs can find a recognized interruption amid a timeframe way. In any case, it's awfully troublesome to spot WHO the assailant is because of assault bundles region unit typically issued with cast IPs or aggressors could enter a framework with substantial login designs. despite the fact that OS-level framework calls (SCs) are somewhat progressively helpful in recognition aggressors and particular clients, process a larger than average volume of SCs, mining vindictive practices from them, partner degreed unmistakable feasible assailants for an interruption region unit as yet building difficulties.

The commitments of this paper are: 1) distinguish a client's scientific highlights by dissecting the comparing SCs to upgrade the precision of assault location; 2) ready to port the IIDPS to a parallel framework to additionally abbreviate its recognition reaction time; and 3) viably oppose insider assault. The rest of this paper is composed as pursues. Segment II presents the related work of this paper. Segment III portrays the system and calculations of the IIDPS. Trial results are appeared and talked about in Sections IV and V, separately. Area VI finishes up this paper

1.1 Algorithms

Algorithm 1: Generating a user i.e. u habit file.

1. W = |log file| - |sliding window;

2. For (i = 0; i<=W-1; i++)

{

3. For (j = 0; j <= W; j++)

{

Collect all C1-grams in current L-window;

Collect all C1'-grams in current C-window;

4. Compare C1-grams and C1'-grams;

5. If (identified SCs patterns already exit in habit file)

Count+1;

Else

Insert SC pattern into habit file with count = 1;

}

}

The mining server conjures Algorithm 1. A mining server removes SC-grouping created by a client u from u's log record, checks the occasions that a particular SC-design shows up in the document, and stores the outcome in _SC-design, appearance counts_ position in u's propensity document. After this, SC-examples' comparability loads are determined to sift through those SC-designs usually utilized by all or generally clients. At that point, the yield result is contrasted and every single other client's propensity documents in the fundamental framework to additionally distinguish u's particular SC designs. At last, the comparability weight is processed to create u's client profile..

Algorithm 2: detects an internal intruder.

1. User current input = SC'; SC' = ϕ;

2. While receiving user input denoted by 'h'

{

SC' = SC' U {h};

3. If (user input > sliding window)

{

For (j = SC' – sliding window; j>0; j++)

{

4. C-window = mid (user current window, j, sliding window);

5. Compare C1-gram and C1'-gram;

6. Calculate SC pattern similarity weighs;

7. Sort similarity scores for all users;

8. If (decisive rate for user profile < threshold)

System alert u as user profile;

Else

System alert u as attacker profile;

}

}

}

Detection server detects the internal intrusion using the algorithm 2. Detection server tries to identify the underlying user is an account holder or not by calculating the similarity score between the newly generated SCs, in the u's current input and usage habit stored in the in user's user profile to verify u.

There are three types of attacks are blocked by IIDPS.

1. A user of specific groups submits an SC, which the group members are prohibited to use.

2. An attack that launches a sensitive SC, which is defined as one that may erase or modify sensitive data or system settings, to change the environmental settings of the system or attack the system.

3. SC level attack patterns that are an attacker mixing specific SC can sometimes penetrate a security System.

1.2 Modules

IIDPS

IIDPS is a framework or security system, named Internal Intrusion Detection and Protection System (IIDPS), to detect Internal Intrusion and internal intruders. To authenticate users, currently, most systems check using login pattern using user id and password. And it's very quite common knowing login details of other user's, assistances within an organization or company, they may then log in to the system, access users' private files, or modify or destroy system settings. Those attacks we call it as Internal Intrusion Detection, and those attackers called internal intruder.

Detection and Protection

For this we are using system Calls (SC), means user operations on system. We collect SC-Sequences based on user operations, and store in user's habit data, and mine the data like calculate weight of the SC-sequence. Based on SC-sequence we mine the SC-pattern.

User

Here User nothing but a co-worker in a group of employees in a organization, user can log into system using his/her own login pattern. After login user perform operations like upload, download, update, send, view etc. User can get alert when s/he attacked. Based on user decision application will find the intruder, this is the user get protected.

Admin

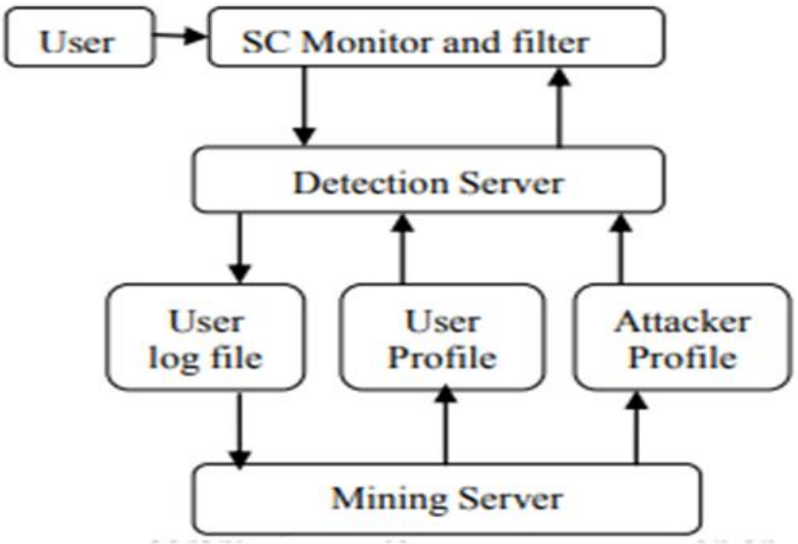
Admin is a main user of our system. Admin can verify the SC-Patterns of the user. Admin can maintain the data of attacks, like attack time and data, type of operating system, attacker details, and level of attack.

2. Architecture

Loading the dataset for the current user into the database. The dataset contains the user's behavioural data and do the pre-processing. The pre-processed data is stored into database. The threshold value is calculated from the pre-processed dataset from which the calculations for the nearest values are made. The user's behaviour pattern is found by the nearest value which is stored as User's profile.

When the authenticated user is log into the system his/her current system usage activities are updated in the data base. The Admin updates the user login details into the database. The logged user's behavioural values are stored as the User's log file. The comparison is made between the current user's profile which contains his/her behavioural pattern and user's log

file. If there is any deviations occur while the comparison it is notified that the currently logged user is attacking the system. Thus the Insider attack is identified.



System Architecture

3. CONCLUSION

In this paper, we have proposed a methodology that utilizes information mining and measurable strategies to recognize the agent SC-designs for a client. The time that a constant SC design shows up in the client's log file is checked, the most usually utilized SC-designs are filtered out, and after that a client's profile is set up. By recognizing a client's SC-designs as his/her PC use propensities from the client's present information SCs, the IIDPS opposes suspected aggressors. The test results show that the normal discovery exactness is higher than 94% when the definitive rate limit is 0.9, demonstrating that the IIDPS can help framework managers to bring up an insider or an assailant in a shut situation. The further examination will be finished by improving IIDPS's execution and exploring outsider shell directions.

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. Comput., 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," Comput. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.

[8] J.Choi,C.Choi,B.Ko,D.Choi,andP.Kim,"DetectingwebbasedDDoS 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," Comput. Commun., vol. 34, no. 3, pp. 468–484, Mar. 2011.

BIOGRAPHIES

Ms.Prajakat S.Shinde is currently pursuing B.E(computer) from Dept. of Computer Science and Engineering, Shriram Institute Of Engineering and Technology Centre, Paniv, Maharashtra, India. She has received Diploma(Computer Tech.) from Shriram Institute Of Engineering and Technology (Poly.), Paniv. Her area of interest is Network Security.

Ms. Kajal R.Sale is currently pursuing B.E(computer) from Dept. of Computer Science and Engineering, Shriram Institute Of Engineering and Technology Centre, Paniv, Maharashtra, India. She has received Diploma(Computer Tech.) from Shriram Institute Of Engineering and Technology (Poly.), Paniv. Her area of interest Is Network Security.

Ms.Nikita D. Waghmode is currently pursuing B.E(computer)from Dept. of Computer Science and Engineering, Shriram Institute Of Engineering and Technology Centre, Paniv, Maharashtra,India.Her area of interest Is Network Security.

Asst. Prof. Kambale Komal S. is currently working at Shriram Institute of Engineering and Technology Centre, Paniv, Maharashtra, India. She has received B.E(computer) from Dept. of Computer Science and Engineering from SVERI's, COE, Pandharpur, Maharashtra, India. Her area of interest Is Network Security and Operating System.(Having 1 year experience of assistant professor).