Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 7, Issue 4, April-2020

An Internal Intrusion Detection and Protection System by Self Monitoring using Data Mining Techniques

Smriti Jolad[1], Harshada Thigale[2], Ashwini Hawa[3], Priya Tanmane[4], Prof. Minaxi Doorwar[5]

[1,2,3,4,5]*Information Technology, G.H. Raisoni College of Engineering and Management, Pune University*

Abstract — In the 21st century where use of advanced computer and Smartphone's has increased drastically, it has become a tedious task for us to memorize Ids and passwords. Especially for working professionals where one needs to take care of N numbers of user Ids and passwords, In order to avoid this we start opting for a common pattern or password for every authentication. Thus it becomes easy for us to remember but as from security point of view, it becomes very easy and vulnerable for an attacker to attack a system or network. Intrusion basically refers to some outsider who does not belong to the group or community and is trying to intrude i.e. get into our system by wrong means. Thus intrusion detection basically refers to an act of detecting network system for malicious or harmful activity. It is an application which tries to identify and rise an alarm/inform if any suspicious activity is tracked and observed. However we have propose a security system, named Internal Intrusion Detection and Protection System (IIDPS) by self monitoring using data mining. We are going to use data mining techniques to identify internal intruders and take action accordingly.

Keywords: ***Intrusion Detection Systems, data mining, network, vulnerable, malicious, authorisation.***

I. INTRODUCTION

In the digital era, computer and its digital devices have become so handy that all our day to day life is completely dependent on it. But due to increased chances of attacks we are asked for authentication at each and every step. We need to login into system or any application or any network, we require and need to successfully pass through authentication step. But in order to remember and store password, we have human tendency to keep a simple or mostly a common password or pattern for every authentication purpose. This in turn increases the chances of intrusion. Security till date remains one of the biggest challenges and continuous efforts are taken to improve it. Still we face with large number of attacks such as DOS attack, phishing attack, eves dropping attack, spy email attack, Trojan horse attack, etc. All these attacks are easy to be detected at system call i.e. operating system level. Thus in this paper we propose a security system, that detect malicious harmful behavior basically called as Advance Intrusion Detection and Prevention System. Intrusion prevention monitors system structures for malicious activity or threat. It's a proactive approach which every organization should follow for safety and security purpose.

II. LITERATURE SURVEY

1. An Internal Intrusion Detection System by Using Data Mining and Forensic Techniques

Author: Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao- Tung Yang

Description:

Majority of application and systems users uses the credential in the form of Id and password to authenticate the genuine user. But it is observed that sharing passwords is common practice while working or to get any task done. This is unethical and gives unauthorized user a chance to do any malicious activity under someone else account name and credentials. 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. This paper aims at detecting intrusion attacks, keeping a trend and logs of same and alerting system and network if any activity is found.

2. BOGUSBITER: A TRANSPARENT PROTECTION AGAINST PHISHING ATTACKS.

Author: CHUAN YUE, HAINING WANG

Description:

In general many anti-phishing mechanisms move their focus currently on helping users verify whether a Web site is genuine. However, usability studies have demonstrated that prevention-based approaches alone fail to effectively suppress phishing attacks and protect Internet users from revealing their credentials to phishing sites. In this paper, instead of preventing human users from "biting the bait," They have proposed a new approach to protect against phishing attacks with "bogus bites." They have also develop Bogus Biter, a unique client-side anti-phishing tool, which transparently feeds a relatively large number of bogus credentials into a suspected phishing site

3. A MODEL-BASED APPROACH TO SELF-PROTECTION IN COMPUTING SYSTEM.

Author: Qian Chen, Sherif Abdelwahed, Abdelkarim Erradi

Description:

This paper reveals the model based security approach to detect and identify the security attacks along with planning a set of actions to protect the networked computing system. This approach has the sensors involved, that collects the system and network parameters and sent to system for verification. Their proposed approach is demonstrated on variants of case studies including Denial of Service (DOS) attack and many more.

III. PROPOSED SYSTEM

Our proposed system aims at providing highly efficient and robust intrusion detection system. The self analysis method continuously monitors and provides details of user activities for detecting unauthorized entities. As internal system calls (SC) are used to detect the intrusion attacks, this can be implemented using data mining and forensic techniques. It would help to identify and provide detailed information about a user and its SC patterns. IPS can be configured to monitor log and report activities. Here time of user activities is counted as it appears in the user's log file. After which the most commonly used SC patterns are filtered. These are then compared with user's daily habits and if any deviation is found then the reason for that needs to be identified. If the user has an exception condition at that instance than it can be ignored as a warning. But if no exceptional instance is found then it needs to be alarmed/informed and reported to the right authorities. Thus this would help in any harmful anonymous intrusion effect and prevent from any type of attacks. This helps to stop threat of attacks and is typically located between companies firewall and rest of network.

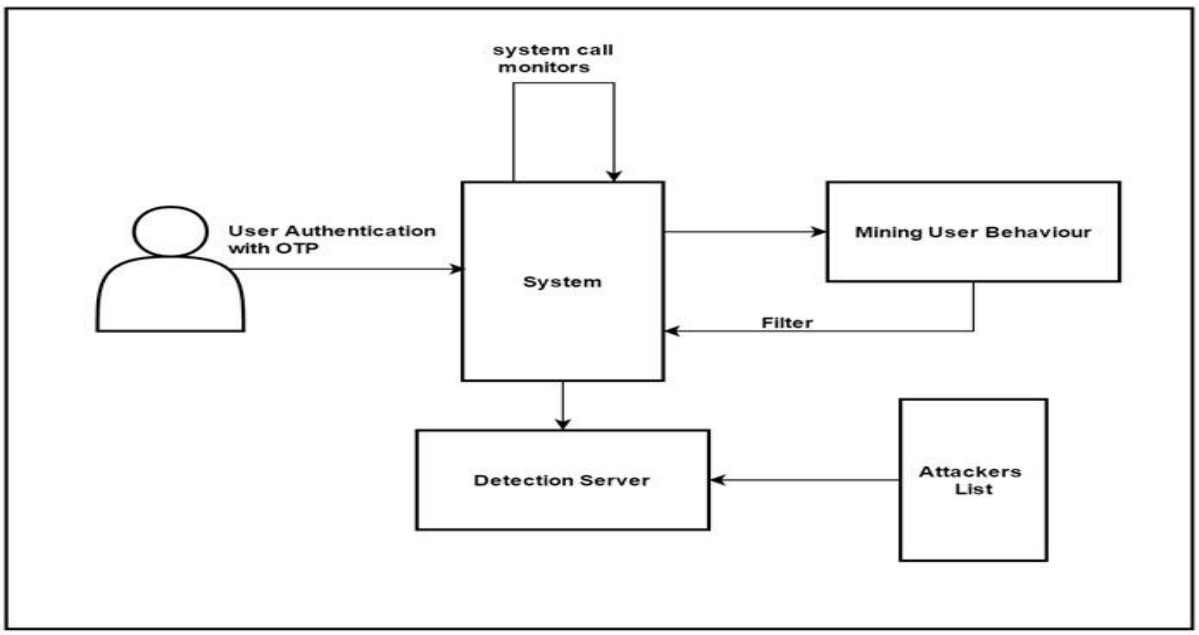

Fig. : System Architecture

Steps:

Step 1: let's consider the U as the user of system who logins to the system.

U=f U1, U2Un g.

Step 2: Let say S as System that will authenticate the user U by sending the OTP to user mail and verify the user.

Step 3: The user U will perform some activities like inserting USB device in USB port, copying some content from highly secured drive or folder to another place, installing new software etc.; the activities may be malicious activities. System monitors the user activities by reading the log files generated by system.

Step 4: The IIDPS system will reads the user log files i.e. user infrequent activities from attack list A with the help of detection unauthorized access D.

Step 5: The system S will alert the malicious user activities by capturing snapshots of activities at real time of performing those activities. Output: The system will identify the malicious attack on system.

IV. APPLICATIONS

1. System can be used in corporate organizations.
2. System also used in Educational Institutes.
3. System also useful in the cyber cafes.
4. System also used for the government organizations where 24/7 surveillance is needed.

V. GOALS AND OBJECTIVES

1. In the terms of accuracy & Efficiency, our proposed system leads in terms with other systems.
2. Internal Intrusion Detection and Protection System (IIDSP), which detects malicious behaviours of users.
3. As other systems consumes for time for data analysis as compare to IIDSP. This can also detects malicious behaviours for system employing GUI interfaces.

VI. CONCLUSION

Our proposed system has successfully demonstrated in this paper .i.e. internal intrusion detection and protection system by using data mining and forensic techniques. We have aimed to build a system that prevents and alert intrusion attacks and our system. We have various modules that store and keep track of all the users in system. All the users' activities will be monitored and get recorded in log file. If system finds the abnormal activities .i.e. the activity which matches with the activities restricted for the user, then system will generate an alert message to the admin. System has self monitoring function that means it continuously keep on monitoring the user activities.

VII. REFERENCES

[1] C. Yue and H. Wang, BogusBiter: A transparent protection against phishing attacks, ACM Trans. Int. Technol., vol. 10, no. 2, pp. 131, May 2010.

[2] Q. Chen, S. Abdelwahed, A. Erradi: A model-based approach to self-protection in computing system, in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 110.

[3] H. Lu, B. Zhao, X.Wang, and J. Su, DifiSig: Resource dier- entiation based malware behavioral concise signature generation, Inf. Commun.

[4] Z. Shan, X.Wang, T. Chiueh, and X. Meng, Safe side eects commit- ment for OS-level virtualization, in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe,Germany, 2011, pp. 111120.

[5] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, Detecting web based DDoS attack using MapReduce operations in cloud computing environ- ment, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 2837, Nov. 2013.

[6] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer stream- ing, in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 15.

[7] Z. A. Baig, Pattern recognition for detecting distributed node ex- haustion attacks in wireless sensor networks, Comput. Commun.vol. 34, no. 3, pp. 468484, Mar. 2011.

[8] H. S. Kang and S. R. Kim, A new logging-based IP traceback ap- proach using data mining techniques, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 7280,Nov. 2013.

[9] VIRTUAL KEYBOARD. 2007. Hacker demos how to defeat Citibank virtual keyboard. http://blogs.zdnet.com/security/?p=195