Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

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

Volume 6, Issue 12, December-2019

ADVANCED INTERNAL INTRUSION DETECTION AND PROTECTION FOR COMPUTER SYSTEMS

Ayush Nair[1], Siddhant Pandagle[2], Pratik Baviskar[3], Swapnil Madav[4]
Prof. Sonali Lunawat[5]

[1]ayush772084@gmail.com, [2] siddhant.pandagle1998@gmail.com, [3]pratik1697@gmail.com, [4]swapnilmadav01@gmail.com

[5]sonali.lunawat@pccoer.in

[1]*Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Ravet, Pune University*
[2]*Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Ravet, Pune University*
[3]*Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Ravet, Pune University*
[4]*Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Ravet, Pune University*
[5]*Computer Engineering, Pimpri Chinchwad College of Engineering and Research, Ravet, Pune University*

Abstract

In the revolution of modernization, the use of digital devices like Tablets, Smartphone's and computer systems etc have reached to higher extent. As these systems have became an important part of daily life, so it must be protected & kept safe from any intruders or hackers. Currently there are user ids and passwords to protect the crucial system from intruders. To memorize those passwords for human being have become tedious task. And to keep them safe from hackers and intruders is also alike impossible as there are chances that credentials may accidentally get disclosed or get shared with unintended authority. Intrusion is concept where someone who does not belong to group of community but tries to access the system i.e. get into system by unauthorized way. So, the advanced intrusion detection system detects and protects the network system from malicious or harmful activity carried out by intruder's ore hackers. However, we have proposed the system that will alert the authorized user when a suspicious activity is tracked and observed. Our system will not only provide alert but also protect our system at real time. With the help of data mining we are going to achieve the intrusion detection and protection.

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

I. INTRODUCTION

In the recent the years, technology has revolutionized our daily lives. Digital devices have become so important that we are totally dependent on them for most of our daily activities. The world in which we live in is totally **dependent** on technology in much way. Modern technology has paved the way for multi-functional devices like the computer system and the Smartphone. Computers have becoming more and faster, more portable, and higher-powered than ever before. Using these devices, we can do things like transfer money instantly and make purchases for everything from clothes, food delivery, groceries, furniture, and more. So, to keep them safe we have authentication at each and every step. Sometimes only authentication itself is not enough to keep our system protected from intruders. In this form it has always been a challenging task to keep our system attack free. There are several types of computer security **threats** such as Trojans, Malware, Virus, Adware hackers etc. Safe guarding the systems using the login credential sometimes may not work at those extents. So, to safeguards our system we have proposed security system that detects malicious harmful behaviour that refers as **Advanced Internal Intrusion Detection and Protection for Computer Systems.** Which continuously monitor our system in real time and protect it from Intrusion by sending the alert message to authorized users.

II. LITERATURE SURVEY

I. Research on Anomaly Intrusion Detection Technology in Wireless Network

Author: Dunyi Yu, and Chao- Tung Yang

Description:

This paper states the types and detection principles of wireless network intrusion detection, it adopts the information statistical analysis method to detect the network intrusion, constructs the traffic statistical analysis model of the network abnormal intrusion, and establishes the network intrusion signal model by combining the signal fitting method.
This is unethical and gives unauthorized user a chance to do any malicious activity under someone else account name and credentials. A security system, named the **Advanced Internal Intrusion Detection and Protection for Computer Systems** is proposed to detect insider attacks at SC level by using data mining and forensic techniques. This system creates users' personal profiles to keep track of users common behaviours 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 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. RRPhish: Anti-phishing via mining brand resources request

Author: Guang-Gang Geng, Zhi-Wei Yan, Yu Zeng, Xiao-Bo Jin.

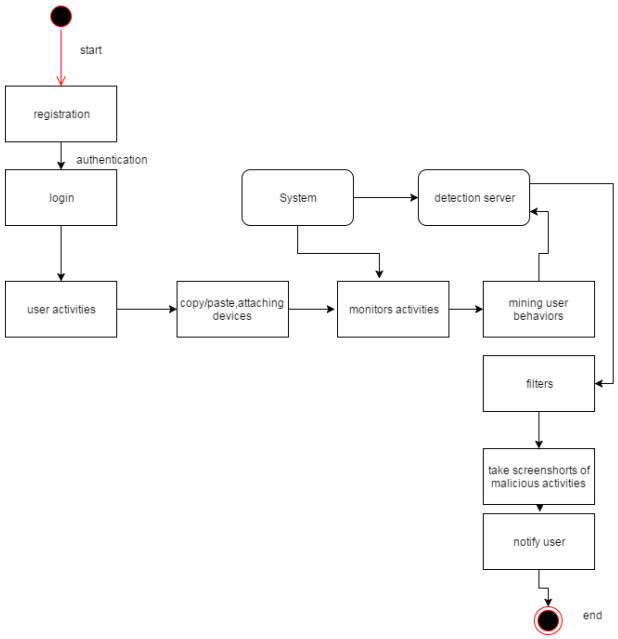
Description:

In recent years a variety of anti-phishing approaches have been identified, phishing fraud has become common now a days. Especially with the popularity of electronic banking and mobile payment, phishing attacks have become more profitable. In this paper they have mentioned that exploring efficient and practical anti-phishing technology is particularly necessary and urgent, by analyzing the resources (CSS, JS, and image files) request characteristics of phishing sites. They propose a novel anti-phishing method - RRPhish. RRPhish as an enhanced blacklist technology can detect not only phishes in blacklist, but also emerging phishes. The experiments demonstrate the effectiveness of RRPhish.

III. PROPOSED SYSTEM

Our proposed system is highly smart and efficient in intrusion detection & protection. Using data mining technique our system continuously keeps on monitoring itself against the intrusion. System is highly trained using the concept of data mining. Self monitoring consists of keeping the watch on routers, firewalls, packets, server for detecting unauthorized entities. System will be granting the roles to everyone based on his/her designation or type of work is assign. It would help to identify and provide detailed information about a user and its SC patterns. These assigned roles are stored as data set with respect to each user. For each user log file gets generated and maintained by the system, based on this system compares the daily logs for each user. If any deviation is found than reason for it needs to be identified. Based on certain criteria it can be an exceptional path. But if not, then system send an alert to an authorize user along with complete machine address. Also warns the intruder before sending the alert. Thus, providing alert in real time or that instant of time helps in detection and protection from malicious attack.
This helps to stop threat of attacks and is typically located between companies' firewall and rest of network.

Flow of Proposed System.



STEPS:

Step 1: user i.e. U will be login to the web Application.
U=f U1, U2Un g.

Step 2: The System S will validate the user U by sending the OTP to authorised user mail and verification will be done.

Step 3: the use U will perform some activities like attaching USB de- vice, copying some content from one place to another place, installing new software etc., the activities may be malicious activities. The system generated call i.e. SC (system calls) are maintain monitoring on user activities i.e. log files.

Step 4: Our Propose System will filter the user activities from attack list A using detection server D.

Step 5: the system S will report the malicious user activities by taking snapshots of activities at time of performing those activities.

Output: Our Proposed system will catch the malicious activity of user at the time of attack.

IV. APPLICATIONS

1. System can be used in financial organizations where highly secure system is needed.
2. System also used for colleges, for exam hall monitoring.
3. Cyber cafes.
4. System also used for the government organizations.

V. CONCLUSION

We have successfully proposed our idea, in the form and **Advanced Internal Intrusion Detection and Protection for Computer Systems**. Considering the security threats, we have aimed to build a system that prevents intrusion attacks and activities. Our targeted system will be useful in many firms like colleges, MNC, small scale to large corporate and non-technical areas as well. Also, we have provided multiple modules and scenarios where we can keep a track and record of all the users and their activities. It will also serve the purpose of maintaining logs which can be sent to higher and dedicated authorities for checking and preventing intrusion detections and harmful attacks or activities which do not have good intentions.
.

VI. REFERENCES

[1] 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.

[2] VIRTUALKEYBOARD. 2007. Hacker demos how to defeat Citibanks virtual keyboard. http://blogs.zdnet.com/security/?p=195

[3] H. Lu, B. Zhao, X.Wang, and J. Su, DifiSig: Resource dier- entiation based malware behavioral concise signature generation, Inf. Commun. Technol., vol. 7804,pp. 271284, 2013.

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

[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] 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. 110.