IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INTRUSION DETECTION AND IDENTIFICATION USING INTERNAL SYSTEM CALLS

[1]Shubham Gharde,[2]Sukruta Godse,[3]Dhananjay Indore,[4]Nilesh Baviskar

[5]Prof. Jyoti Kshirsagar

[1]*Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Savitribai Phule Pune University*
[2]*Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Savitribai Phule Pune University*
[3]*Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Savitribai Phule Pune University*
[4]*Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Savitribai Phule Pune University*
[5]*Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Savitribai Phule Pune University*

Abstract: In the era of advanced computers and Smartphone's, it has become a tedious task for us to remember our Ids and passwords. We start opting for a common pattern or password for every authentication especially for working professionals where one needs to enter N numbers of user Ids and passwords. Thus it becomes easy for us to remember but from a security point of view, it becomes very easy and vulnerable for an attacker to attack a system or network. Intrusion basically refers to someone out of our network tries to access the system in an illegal way i.e. get into our system by the wrong means. Thus intrusion detection basically refers to an act of detecting a network system for malicious or harmful activity. Our system tries to identify\detects the illegal action then raise an alarm/inform if any suspicious activity is tracked and observed. However here we are proposing a system that aims to identify internal intrusion in a network or system. Our proposed system will be using data mining techniques in the form of systems internal calls to identify internal intruders and take action accordingly.

Index Terms **- Intrusion Detection Systems, data mining, network, vulnerable, malicious, authorisation.**

I. INTRODUCTION

Recently everyone has moved them self to digital ERA, wherein all of us use digital devices and have become completely dependent on them. As we have moved to the platform this lead to an increase in chances of attacks. Enough though we have asked to authenticate each and every possible way. To get logged in to any application or network, we need to successfully authenticate by providing correct credentials etc. We humans always want to keep the passwords as simple as possible so that we can remember and memorize them. As the complexity of passwords reduces the same increases the chances of hacking. Which can lead to intrusion in our system or network? There is n number of attacks that can be done on our system or network.
Attacks can be like DOS attacks, phishing attacks, Trojan horse attacks, eves dropping attacks, etc. So in order to prevent this kind of attack at a certain level, we have proposed a system that will use the operating system's internal calls to identify and malicious activity. This paper proposes the design and implementation of a system to identify and alert the end user regarding the malicious attack on the system.

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:
In the Recent era, mostly all the users, applications, and systems use the credential in the form of Id and password to authenticate the genuine user. But it's also a common practice to share passwords while working to get any task done. This is unethical and gives the unauthorized user a chance to do any malicious activity under someone else account name and credentials. In this paper, the author has given a brief process regarding how operating system level internal calls can be used to identify unexpected and malicious attacks The system creates users' profiles to keep track of users' usage activities as their forensic features and determines whether a valid login user is the account holder or not by comparing his/her current computer usage behaviours with the patterns collected in the account holder's personal profile This paper aims at detecting intrusion attacks, keeping a trend and logs of the same and alerting system and network if any activity is found.

2. Bogus Biter: A transparent protection against phishing attacks.
Author: CHUAN YUE, HAINING WANG

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

III. PROPOSED SYSTEM

Our proposed system aims at providing a highly efficient intrusion detection system. The analysis method monitors and provides details of routers, firewalls, packets, servers for detecting unauthorized entities. As we are using system calls to detect intrusion attacks, this can be complimented using data mining and forensic techniques. Logs and report activities can be monitored using IPS. Here the duration of time is counted as it appears in the user's log file. These are then compared with the 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 then 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. The algorithm used for this identification process is the Decision Tree. Thus this would help in any harmful anonymous intrusion effect and prevent any type of attacks. This helps to stop the threat of attacks and is typically located between companies firewall and the rest of the network

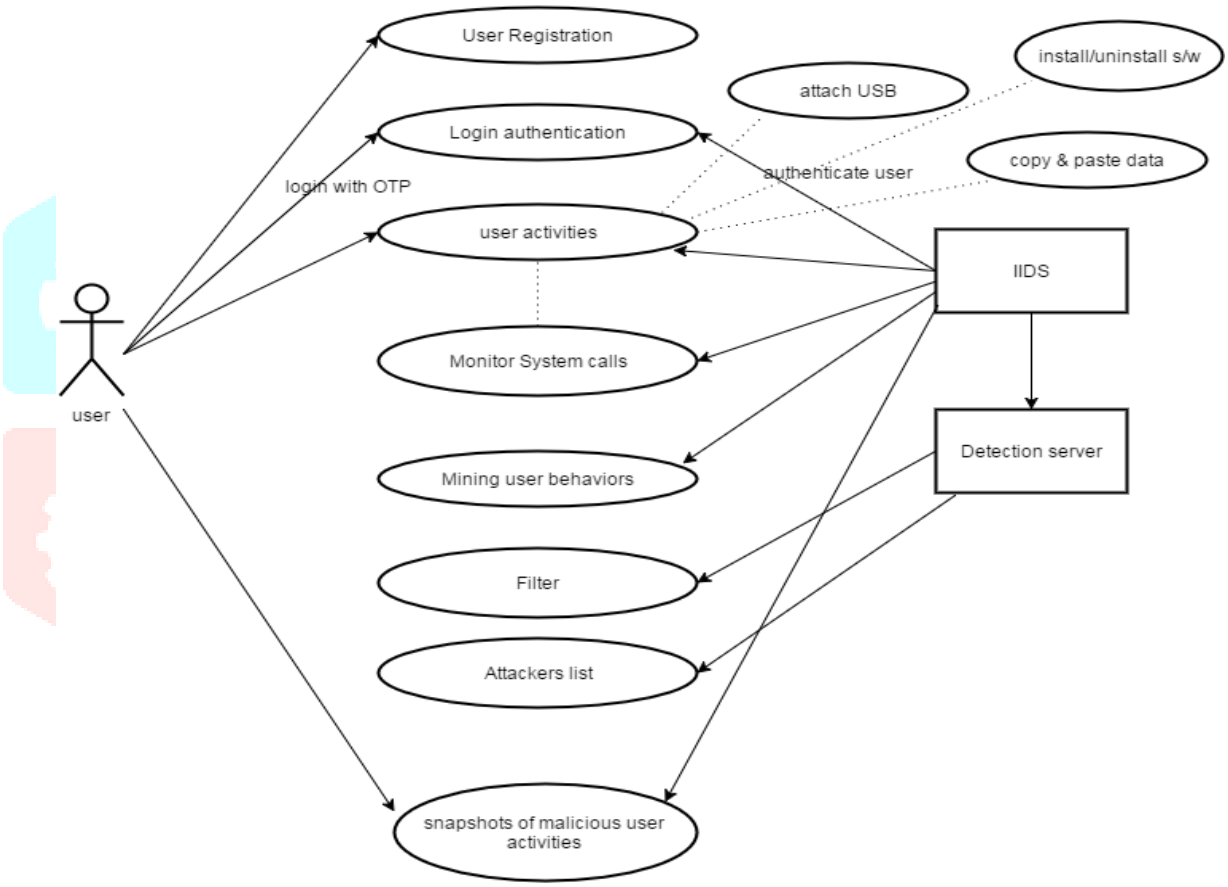

Fig. 1 (System Architecture)

IV. MATHEMATICAL MODEL

Step 1: let's consider the U as the user who login to the system.
U=f U1, U2Un g.

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

Step 3: the use U will perform some activities like attaching a USB device, copying some content from one place to another place, installing new software, etc.; the activities may be malicious activities. The system monitors the user activities by reading the log files generated by the system.

Step 4: The IIDS system will read the user log files i.e. user infrequent activities from the log details and compare them with the frequent activities

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

V. APPLICATIONS

1. System can be used in corporate organizations.
2. System also used in industries.
3. System also useful in the cyber cafes.
4. System also used for the government organizations.

VI. HARDWARE REQUIREMENT

- Hard Disk : 40 GB.
- System : Intel I3.
- Monitor : 15 VGA Colour.
- Ram : 4 GB.
- Mouse : Logitech.

VII. SOFTWARE REQUIREMENT

- Operating system : Windows 7 and behond.
- Coding language : JAVA/J2EE.
- IDE : Eclipse Kepler.
- Database : MYSQL,XAMPP

VIII. CONCLUSION

In this paper we have proposed, an internal intrusion detection of anonymous and preventions system. As the saying goes that prevention is better than cure, similarly we have aimed to build a system that prevents intrusion attacks and activities. This can be implemented from small-scale to large corporate and nontechnical areas as well. Also, we have provided multiple modules and scenarios where we can keep track and record all the users and their activities. It will also help us generate trends that we can store in the database and use for future reference. It will also serve the purpose of maintaining logs that 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.

IX. REFERENCES

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

[2] Q. Chen, S. Abdelwahed, and A. Erradi, A model-based approach to protection in a very ADP system, in Proc. ACM Cloud involuntary Comput.

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

[4] Z. Shan, X.Wang, T. Chiueh, and X. Meng, Safe facet effects commitment for OS-level virtualization, in Proc. ACM Int. Conf. involuntary Comput., Karlsruhe,Germany, 2011, pp. 111120.

[5] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, detective work web-based DDoS attack victimization MapReduce operations within the cloud computing surroundings, J. net 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 theme within the network-coding-based peer-to-peer streaming, in Proc. CA, USA, 2010, pp. 15.

[7] Z. A. Baig, Pattern recognition for detective work distributed node exhaustion attacks in wireless device networks, Comput. Commun. vol. 34, no. 3, pp. 468484, Mar. 2011.

[8] H. S. Kang and S. R. Kim, a replacement logging-based science traceback approach victimization data processing techniques, J. net Serv. Inf. Security, vol. 3, no. 3/4, pp. 7280,Nov. 2013.

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