



SELF MONITORING COMPUTER SYSTEM USING INTRUSION DETECTION

Ms. Rupali V. Gurav¹, Ms. Rafat R. Bagwan², Ms. Snehal V. Bhosale³, Ms. Girija V. Dixit⁴, Ms.
Aarti U. Godase⁵, Prof. S.A. Shegdar⁶

Abstract — Now a days, there are new attacks are emerging everyday due to that the system makes the insecure even the system wrapped with number of security measures. To find out the intrusion, IDS - an Intrusion Detection System is used. To find out the intrusion and respond in timely manner is its prime function. In other words we can say, IDS function is limited to detection as well as response. The system is not able to catch the state of the activity when an attack is detected. Hence, in original form, it's not possible to preserve the evidences against the attack. New security strategy is needed to maintain the completeness and reliability of evidence for later examination. In our project work, there proposed an automated Digital Forensic Technique with Intrusion Detection System. System will send an alert message to capture the current state of the system, to admin or authorized User followed by invoke the digital forensic tool Once an IDS detects an intrusion.

Keywords— Intrusion Detection Systems, Cryptography, Logs, Digital Forensic.

I. INTRODUCTION

Security of the computer systems has been one of the major issues in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously to authenticate users. To overcome from this problem we are going to propose a security system, named Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors launched toward a system.

In current system it is very difficult to identify who the attacker is because attack packets are often issued with forged IPs or attackers may enter a system with valid login patterns. Hence we got motivation to developed a system which detects malicious behaviors launched towards a system at SC level.

So our main purpose is to provide secure system which detects malicious behaviors in a a system at SC level. The system uses forensic profiling techniques and data mining and to mine system call patterns (SC patterns) defined as the longest system call sequence that has repeatedly happens multiple times in a user's log file.

I. LITERATURE SURVEY

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

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

Description:

Currently, users and systems as well as applications mostly worldwide use user ids and password for authentication purpose. But it's also a common practice to share passwords while working to get any task done. This is corrupt also gives user who is not authorized a chance to do any illegal activity under someone else account name and credentials. 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. A Model-based Approach for Self-Protection in SCADA Systems

Author: Qian Chen, Sherif Abdelwahed

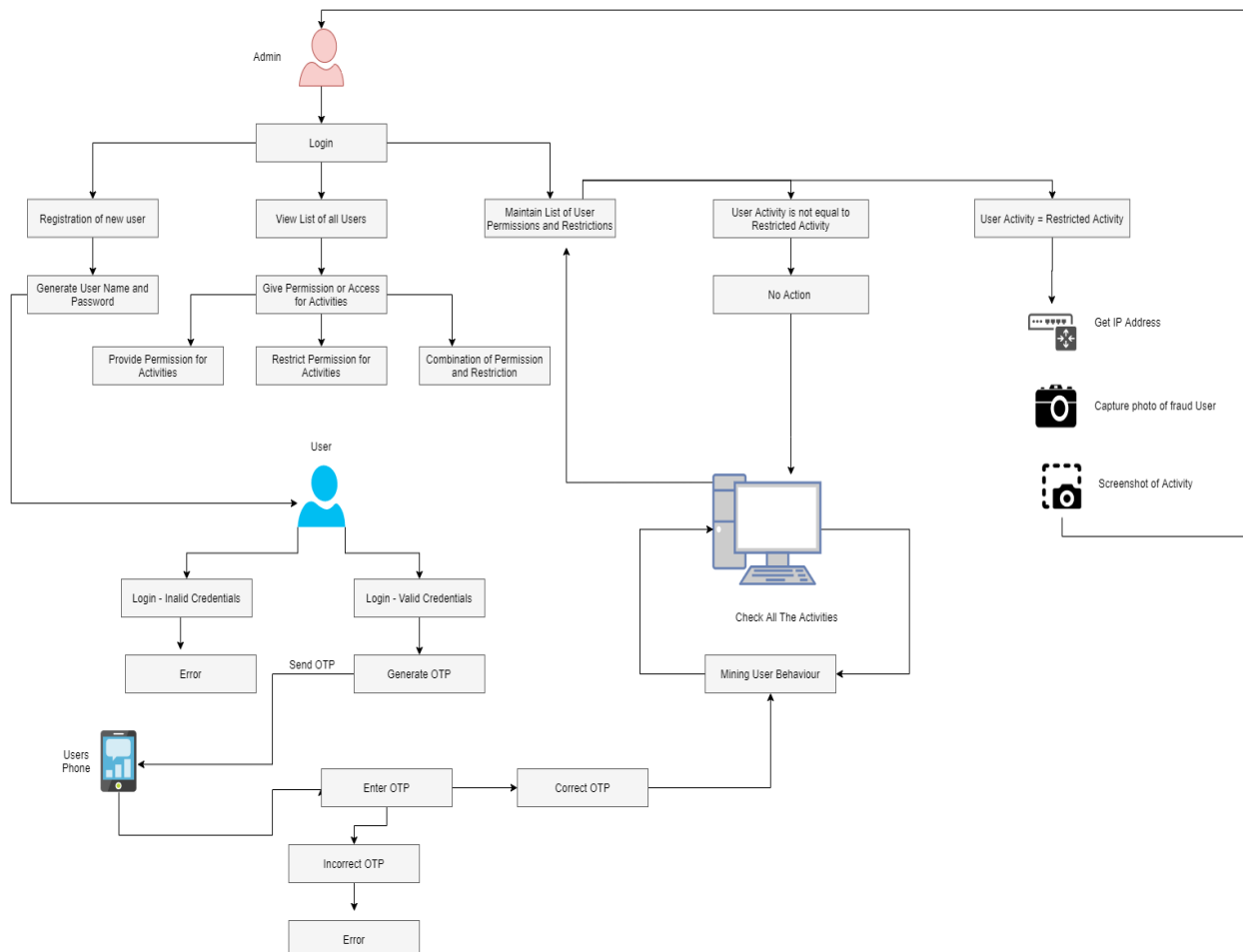
Description:

SCADA - Supervisory Control and Data Acquisition systems are highly venerable and easy catch for cyber-attacks. Now we are having many options that catch attacks and monitor for malicious activity. In this paper we present a self-prevention system to detect attacks. This proposed system does not rely on any external source and does self-prevention. This system is dynamic in nature. This approach has reduced d downtime as compared to current systems and has better efficiency and performance.

II. PROPOSED SYSTEM

In this proposed system we focus providing and improving high efficiency for Illegal action detection. The analysis method monitors and provides details of routers, firewalls, packets, servers for detecting unauthorized entities. As we are using system calls to detect the malicious attacks, this can be achieved using forensic techniques and data mining. 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 the length of time period is calculated 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 on that particular instance than it can be ignored as a warning. But if no special particular instance is found then it needs to be alarmed and reported to the right authorities. Thus this system is very helpful for avoiding attacks and to prevent from any type of attacks. This helps to stop threat of attacks and is typically located between companies firewall and rest of network.

Architecture:



Step 1: The authorized user will login in the Application using user name and password.

Step 2: The IIDS system will authenticate the user by sending the OTP to user mail and verify the user.

Step 3: The User will perform some activities like attaching USB device, 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. The SC (system calls) are always Monitor the activities of User from user history details i.e. log files.

Step 4: Using System calls our Application will sort or filter the log files of user i.e. with the help of detection server system will capture the user activities from attack list.

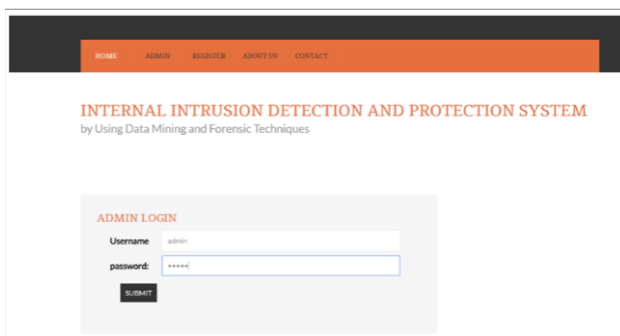
Step 5: If any malicious activity happens then the system S will reports the user actions by taking Users Photo, Ip Address of the System and snapshots of activities.

Output: Our system will detect the Malicious activity of user and to the Admin.

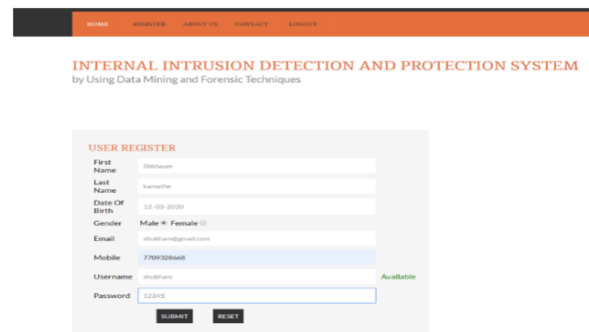
APPLICATIONS:

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

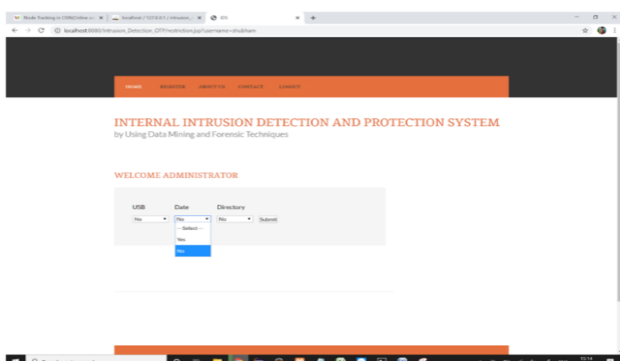
VIII. OUPTPUT



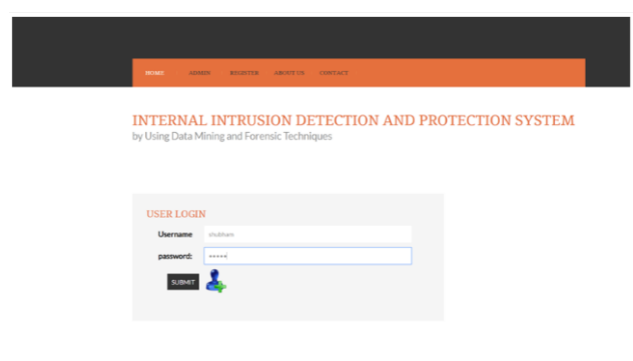
Admin Login



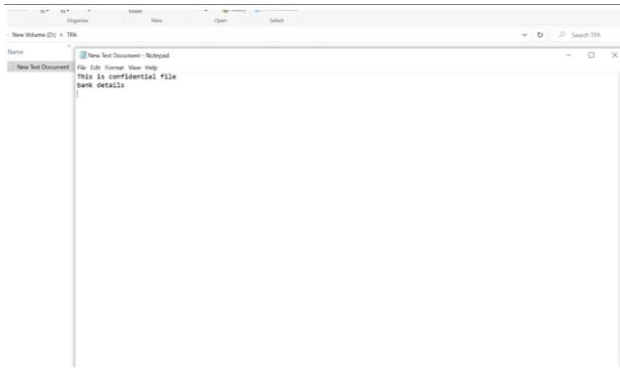
Registration of New User



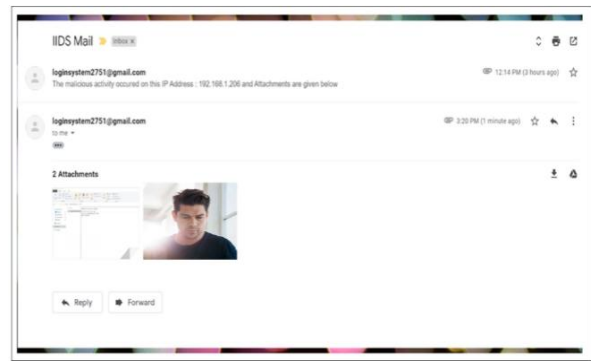
Permissions



User Login



Restricted Activity done by User



Notification to Admin

IX. CONCLUSION

In this paper that we have proposed, we have successfully implemented internal intrusion detection and prevention's 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 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 detection's and harmful attacks or activities which do not have good intentions.

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, 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.
- [3] H. Lu, B. Zhao, X. Wang, and J. Su, DifiSig: Resource differentiation 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 effects commitment 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 environment, 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 streaming, in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 15.
- [7] Z. A. Baig, Pattern recognition for detecting distributed node exhaustion 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 approach using data mining techniques, J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 7280, Nov. 2013.