International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Protection and Detection System by using Data Mining and Rhetorical Techniques

Dr Sreepathi .B[1], Santhamma[2], Goutami Sri Rai[3], Shanthala .J[4], Sowjanya .M.V[5]

[1]*Hod dept of ISE, RYMEC, Ballari, Karnataka, India*
[2] *Assistant professor dept of ISE, RYMEC, Ballari, Karnataka, India*
[3,4,5] *Student of dept ISE, RYMEC, Ballari, Karnataka, India*

Abstract - *The most computer systems use user IDs and passwords as the login patterns to 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. In this paper, presents an intelligent learning approach using Ant Colony Optimization (ACO) based distributed intrusion detection system to detect intrusions in the distributed network. The algorithm improves the efficiency of intrusion detection, reduces false positives of intrusion detection. The results obtained as, the value of rates obtained from and increased efficiency of ACO is increased up to (97% approx.)*

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

1. INTRODUCTION

Computer security is one of the serious problems in the computer domain. Attackers are very usually trying to penetrate the computer security and behave maliciously. Intruders mainly grouped into two types; they are Internal Intruders and External Intruders. Internal intruders are the persons have some access privileges in the network and they are trying to penetrate the security system intentionally or unintentionally. The External intruders are the outsiders from the network.

The security systems like Intrusion Detection Systems (IDS) and firewalls usually block the attacks from outside network so the insider attack is one of the hardest attacks to be detected. The insiders have some access privileges in the network and using that privilege they are trying to penetrate the security in the network. To authenticate users computer systems use different type of authentication techniques. Authentication through username and password is the commonly used technique. If anyone shares their login pattern such as username and password to their friends or co-workers then it will be the weakest point of security.

In this paper we explain a security system called Internal Intrusion Detection System (IIDS) using data mining and biometric technique to detect the internal intrusion. The basic idea of IIDS is IIDPS [2]. Along with IIDPS we use a continuous authentication mechanism using typing speed to authenticate the user.

IIDPS can detect the internal attacks at system call level. IIDPS store the user's computer usage habit by analyzing the system calls sequences that has stored in the user's log file. IIDPS can block internal intruders and can identify the intruders [3] in the network.

1.1 Existing System

To authenticate users, currently, most systems check user ID and password as a login pattern. However, attackers may install Trojans to pilfer victims' login patterns or issue a large scale of trials with the assistance of a dictionary to acquire users' passwords. When successful, they may then log in to the system, access users' private files, or modify or destroy system settings. Fortunately, most current host-based security systems and network-based IDSs can discover a known intrusion in a real-time manner. However, 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. Although OS-level system calls (SCs) are much more helpful in detecting attackers and identifying users, processing a large volume of SCs, mining malicious behaviors from them, and identifying possible attackers for an intrusion are still engineering challenges.

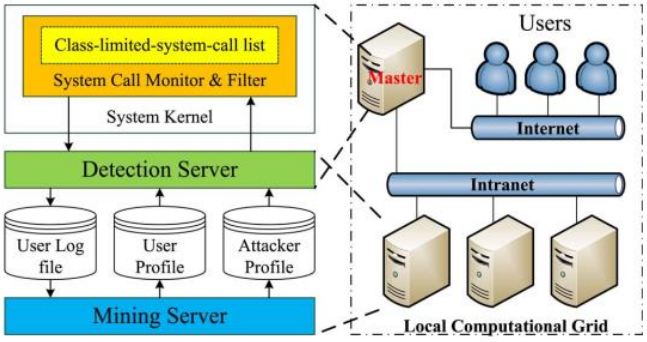
1.2 Proposed System

We propose a security system, named Internal Intrusion Detection and Protection System (IIDPS), which detects malicious behaviors launched toward a system at SC level. The IIDPS uses data mining and forensic profiling techniques to mine system call patterns (SC-patterns) defined as the longest system call sequence (SC-sequence) that has repeatedly appeared several times in a user's log file for the user. The user's forensic features, defined as an SC-pattern frequently appearing in a user's submitted SC-sequences but rarely being used by other users, are retrieved from the user's computer usage history.

2. SYSTEM FRAMEWORK

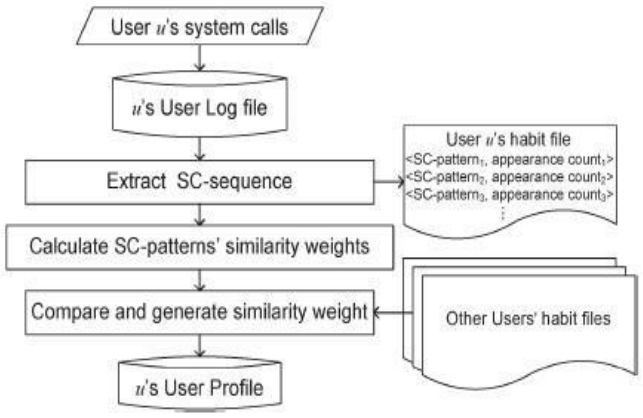
A proposed security system named as Internal Intrusion Detection and Protection System (IIDPS). The main modules of this system are SC Monitor and Filter, Detection server, Mining Server, Computational Grid and three Repositories – User Log File, User Profile and Attacker Profile. The Fig -1 shows the IIDPS system framework.

Fig-1:IIDPS system framework.



The main module of IIDPS is the SC Monitor and Filter which is a loadable module in kernel of the system. It collect all the SC submitted to the kernel and store in the user log file like <u_id,p_id,SC>. U_id is the user ID, p_id is the process ID and SC is the system call submitted by the underlying user. The Mining Server analyzes the user's log file using mining techniques. It identifies user's computer usage habit as user behavior pattern and saves to user profile. The detection server compares the user's behavior pattern with the SC pattern collected in the attacker profile. If any malicious pattern detected, it notifies the SC Monitor and Filter to isolate the user from the protected system. Using this IIDPS can detect the intruders in real time. The computational grid accelerates the IIDPS real time detection. Both detection sever and mining server run on the local computational grid. The generation of user profile can be explains using the control flow diagram. The Fig -2 shows the control flow diagram of generating user profile.

Fig-2: Control Flow of the Generation of a User Profile.



The Mining server creates the user profile using the SC's collected in the user log file. Mining server extract specific SC patterns using data mining techniques [2] from the user log file and store in the user's habit file. After this SC pattern's similarity weights are calculated and compare it with the other users habit file and make sure that none of them have same SC patterns.

3. CONCLUSION

In Intrusion Detection Data Mining refers to the process of extracting hidden, previously unknown and useful information from large databases. It is a convenient way of extracting patterns and focuses on issues relating to their feasibility, utility, efficiency and scalability. Thus data mining techniques help to detect patterns in the data set and use these patterns to detect future intrusions in similar data.

REFERENCES

[1] Fang-YicLcu,Kun-Lin Tsai"A Internal Intrusion Detection and Protection system by Using data Mining".

[2] Ya-Ting Fan l and Shiuh-Jeng Wang," Intrusion Investigations with Data -hiding for Computer Log-file Forensics", IEEE 2010.

[3] R. Araeteh, M. Debbai, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence. " Digital Investigation 4S,pp,82-91,2007.

[4] Karen Scarf one & Peter Mell, National Institute of Standards and Technology (NIST) Special Publication 800-94," Guide to Intrusion Detection and Protection Systems" ,Feb 2007.