ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 8, March 2018

An Internal Intrusion Detection & Protection System for Securing Files

Preethi.V [1], Ramya.C[2], Reshmaa T.R[3], Shanmugaprasath S[4], Hemalatha.C[5]

UG Scholar, Department of CSE, Saranathan College of Engineering, Trichy, India[1,2,3,4]
Professor, Department of CSE, Saranathan College of Engineering, Trichy, India[5]

Abstract: Computer systems have been widely employed to provide users with easier and more convenient lives. However, when people exploit powerful capabilities and processing power of computer systems, security has been one of the serious problems in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously, e.g., stealing critical data of a company, making the systems out of work or even destroying the systems. 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 order to detect insider attacks at SC level, the proposed system uses Internal Intrusion Detection and Protection System (IIDPS) using data mining and forensic techniques. The IIDPS creates users' personal profiles to keep track of users' usage habits 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. Once the system detects the insider attacker, automatically logout the current session and sends OTP notification message to the corresponding user. If the user has to proceed further he/she has to use OTP number for further login.

Keywords: IIDPS, authenticate user, SC, OTP.

I. INTRODUCTION

Internet is a global public network. With the growth of the Internet and its potential, there has been subsequent change in business model of organizations across the world. More and more people are getting connected to the Internet every day to take advantage of the new business model popularly known as e-Business. Internetwork connectivity has therefore become very critical aspect of today's business.

There are two sides of business on the Internet. On one side, the Internet brings in tremendous potential to business in terms of reaching the end users. At the same time it also brings in lot of risk to the business. There are both harmless and harmful users on the Internet. While an organization makes its information system available to harmless Internet users, at the same time the information is available to the malicious users as well. Malicious users or hackers can get access to an organization's internal systems in various reasons. They are

· Software bugs called vulnerabilities
· Lapse in administration
· Leaving systems to default configuration.

The malicious users use different techniques like Password cracking, sniffing unencrypted or clear text traffic etc. to exploit the system vulnerabilities mentioned above and compromise critical systems. Therefore, there needs to be some kind of security to the organization's private resources from the Internet as well as from inside users as survey says that eighty percent of the attacks happen from inside users for the very fact that they know the systems much more than an outsider knows and access to information is easier for an insider.

Security is one of the serious issue in the computer domain as many attackers try to do that. There are many ways by which the attacker tries to get into the user system to do malicious activities. Few activities are penetrating into the computer system, stealing the data of a reputed company, making the system out of work and destroying the system. These attacks are very difficult to detect as the systems available concentrates more on the outsider attackers than the insider attacker. But there is a serious issue with this type of attacks as the user is highly affected. These attackers are called insider attackers. They are the one

All Rights Reserved © 2018 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 8, March 2018

who pretend to be a valid user with valid username and password.

Different organizations across the world deploy firewalls to protect their private network from the Public network. But, when it comes to securing a Private network from the Internet using firewalls, no network can be hundred percent secured. This is because; the business requires some kind of access to be granted on the Internal systems to Internet users. The firewall provides security by allowing only specific services through it. The firewall implements a policy for allowing or disallowing connections based on organizational security policy and business needs. The firewall also protects the organization from malicious attack from the Internet by dropping connections from unknown sources.

A. Definition

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security.

Moreover, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall.

Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

The rest of the paper is organized as follows. The related work is introduced in Section 2; in Section 3, we present our proposed system framework; finally we make a conclusion in Section 4.

II. LITERATURE SURVEY

A. Decision Tree And Forensic Methodology For Detecting And Preventing Internal Attackers

Jayamagarajothi et al [2] propose Decision Tree and Forensic Methodology for Detecting and preventing internal attackers. Decision Tree and forensic Methodology creates user profile for users to keep track of their usage habits called as forensic features. Decision Tree and forensic Methodology work with intrusion detection mechanism. Network based attacks are identified by predefined algorithm. Decision Tree and forensic Methodology collected in the class limited system call list, as a key component of the system call monitor and filter. Decision Tree and forensic Methodology feasibility and accuracy are verified by Decisive rate threshold. User's Forensic features are identified and analyzed by corresponding system call sequence. Decision tree and forensic methodology able to port into parallel system to enhance the accuracy of attack detection and shorten the attacker's response time.

Limitations

Need to improve performance and response time to effectively oppose the insider attacker.

B. Model-Based Approach To Self-Protection In Computing System

Q. Chen et al [11] proposes Self protection SCADA system monitor the industry environment condition of physical infrastructure. The application of SCADA is nuclear power plant and municipal water system. SCADA (Supervisory Control and Data Acquisition) gather the information from the system if any leakage in the system it just give the alarm to the central site. SCADA use methods supervisory control procedures. It involves HW[field solution],SW[set or control] and GUI procedures. SCADA mainly focus on system design, coding and verification control application. SCADA use signature based ids detection . It effectively resist the upcoming attacks.

Limitations

Cannot find the suspicious neighbor that sent it a corrupted block.

C. HOST BASED INTERNAL INTRUSION DETECTION AND PROTECTION TECHNIQUES

Megha Mandlik et al [3] propose a security system, named the Host Based Intrusion Detection System (HIDS), is projected to find Insider attacks at SC level by optimizing

All Rights Reserved © 2018 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 8, March 2018

data processing and rhetorical techniques. The HIDS creates user's personal profiles & log file to stay track of user's usage habits as their rhetorical options and determines whether or not a sound login user is that the account holder or not by scrutinizing his/her current system usage behaviors with the patterns collected within the account holder's personal profile & log file. When intrusion is detected then image will be captured by system and then will send it to administrator and then system will automatically shutdown as the intrusion is detected.

Limitations

1. Only encryption algorithm is used to provide the security to the file which getting send over the network.
2. Difficult to find out large volume OS system calls and different behavior.
3. Harder to manage.
4. Not suited for detecting network scans because the IDSs only sees those network packets received by its host.

III. PROPOSED SYSTEM

Computer systems have been widely employed to provide users with easier and more convenient lives. However, when people exploit powerful capabilities and processing power of computer systems, security has been one of the serious problems in the computer domain since attackers very usually try to penetrate computer systems and behave maliciously, e.g., stealing critical data of a company, making the systems out of work or even destroying the systems [1]. 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 order to detect insider attacks at SC level, the proposed system uses Internal Intrusion Detection and Protection System (IIDPS) [1] using data mining and forensic techniques. The IIDPS creates users' personal profiles to keep track of users' usage habits 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. Once the system detects the insider attacker, automatically logout the current session and sends OTP notification message to the corresponding user. If the user has to proceed further he/she has to use OTP number for further login.

Figure 1.1: System Architecture for the proposed system

The IIDPS creates users' personal profiles to keep track of users' usage habits 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. The IIDPS, as shown in Fig. 5.1, consists of an SC monitor and filter, a mining server, a detection server, a local computational grid, and three repositories, including user log files, user profiles, and an attacker profile.

SC monitor and filter

Collects those SCs submitted to the kernel and stores these SCs in the format of uid, pid, SC in the protected system where uid, pid, and SC respectively represent the user ID, the process ID, and the SC
are submitted by the underlying user.

Mining server

Analyzes the log data with data mining techniques to identify the user's computer usage habits as his/her behavior patterns, which are then recorded in the user's user profile. There are several data mining techniques that can be used to analyze the logs.

Detection server

Compares users' behavior patterns with those SC-patterns collected in the attacker profile, called attack patterns, and those in user profiles to respectively detect malicious behaviors and identify who the attacker is in real time.

All Rights Reserved © 2018 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 8, March 2018

Generally these attack patterns are those that differ from the normal user's behavior.

IV. CONCLUSIONS

The proposed system uses Internal Intrusion Detection and Protection System (IIDPS) using data mining and forensic techniques. The IIDPS creates users' personal profiles to keep track of users' usage habits 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. Once the system detects the insider attacker, automatically logout the current session and sends OTP notification message to the corresponding user. If the user has to proceed further he/she has to use OTP number for further login. This work can be extended by providing alarm notification along with OTP message at the time of detecting inside attacker.

REFERENCES

[1] Fang-Yie Leu, Kun-Lin Tsai and , Yi-Ting Hsiao, and Chao-Tung Yang "An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques", in Proc. 1932-8184, 2015 IEEE.

[2] M.Jayamagarajothi and P. Murugeswari, "Decision Tree and Forensic Methodology for Detecting and Preventing Internal Attackers", International Journal of Computer Science and Engineering Communications, Volume.4, Issue.2 (2016): Page.1402-1409.

[3] Megha Mandlik, Trupti Akolkar, Prachi Dusa, Aishwarya Donta, Prof. Rahul Raskar, "Host Based Internal Intrusion Detection and Protection Techniques", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 9, September 2016.

[4] Fang-YieLeu, Kun-Lin Tsai, Yi-Ting Hsiao, and ChaoTung Yang,'' An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques", IEEE Int. Conf. Avail., Rel. Security, Taiwan,pp 1932-8184,2015

[5] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers—Or how to thwart a phisher with trusted computing," in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, Apr. 2007,pp. 120–127.

All Rights Reserved © 2018 IJARTET