International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 4 21 – 23

Literature Survey on Employee Activity Tracking Tool in an Intranet based System for Security and Performance Evaluation

Mrs. Rashmi Rane, Akshay Velankar, Harshal Tayade, Omkar Rajmane, Rushikesh Joshi
Department of Computer Engineering,
Maharashtra Institute of Technology, Pune

ABSTRACT - In the digital world aided by Networked Computers, it is a daunting task toenforce security measures, especially when the data is potentially confidential to the firm at hand. With high efficiency systems in place, like firewalls and honey pots, to negate any attack over the network, the perpetrators now concentrate on breaking the weaker links in any organization, the employees.
For an enterprise it is very important for employer to have a performance evaluation of his employees and to detect insider attacks and to keep company's data safe and prevent leaking of the companies secure data. An employee activity tool is a tool which allows an employer to track the activities of an employee in his working environment. The employee activity tool is based on remote administration concept. This tool will have a platform on which various plug-in can be written. The employee activity tracking tool will be multiplatform. The loss of productivity and intellectual theft are major concerns in any organization. In this paper we have studied various operations to be performed needed to be performed to enforce security measures against insider attack and to track and increase employee's productivity.

INDEX TERMS - Reverse TCP; WebRTC; Silent; Daemon; Multi OS.

*****

I. INTRODUCTION

.

With so much of today's commerce being conducted electronically, providing staff with internet access has become a business necessity. The internet, e-mail and instant messaging have become essential tools that staffs use to communicate, collaborate and carry out research. Yesteryear, it was relatively easy for organizations to create
Acceptable Use Policies (AUP's) that clearly specified permissible uses for internet and e-mail. The evolution of Web 2.0 has, however, made that a much more difficult process. Wikis, weblogs, forums, social-networking websites and instant messaging are no longer strictly leisure time technologies – they have become vital business resources used in marketing, research and communication and collaboration. But they are resources which can also be misused or abused. How much time do your employees spend surfing the internet ("cyber slacking")?
What do they do during their time online? Search for the best vacation deal, visit an internet casino or look for their perfect partner? How many of the e-mails that are sent and received are work related and how many are forwarded jokes and videos that unnecessarily consume both the employee's time and the company's bandwidth? Do employees use e-mail to harass their colleagues? Do employees obtain information from the organization's
network and use that information for immoral or illegal purposes? Lost productivity is not the only computer-related risk that organizations face. The improper use of e-mail and instant messengers can lead to extremely expensive lawsuits, and the proliferation of mobile devices has made it considerably easier for errant employees to steal sensitive information.

II. LITERATURE SURVEY

The insider-threat problem is one that is constantly evolving and is having devastating impact on organisations worldwide. Those who operate within an organisation are often trusted with highly confidential information such as financial records and customer accounts, and often have detailed knowledge of operational procedures. Further the set of individuals who operate within the organisation is not always restricted to only employees, since contractors and suppliers may also have some level of access or knowledge of organisational procedure[7]. Any individual who chooses to act maliciously has great potential to cause serious financial and reputational damage to the organisation. A malicious insider is a person who violates an authorized level of access in a software system[1]. There are many commercial softwares that are being currently used to monitor the employees in an organization such as Veriato, NetVisor, PearlSoft. For instance consider Veriato which is a employee monitoring software that provides unmatched visibility in the online and communications activity of employees and contractors. Veriato 360 is the system of record, presenting detailed, accurate, and actionable data for use in incident response, high-risk insider monitoring, and productivity reporting.

Media attention has highlighted numerous cases in recent years of both businesses and governments who have been compromised, where confidential information has been exposed[8]. Insider threats and attacks are a known problem. Within an enterprise it is very difficult to detect and identify insider attacks and abuse against Information Systems. A study was conducted by observing a group of IS security analysts who detect and identify insider attacks. Commonalities and generalizations were made based o4 the study to create an insider attack detection model. This model allowed other IS security analysts the ability to increase detection of insider attacks and reduce false positives[3]. In recent years, a large number of businesses and universities have installed Local Area Networks (LANs) based on the Windows NT domain model as their primary computing environment. The system administrators of these new computing environments are finding that the simple remote administration capabilities available in UNLY based LANs are not available. The Windows NT operating system, out of the box, does not provide a simple solution to perform remote administration. The remote administration can be achieved, if an administrator has the expertise in writing Windows scripts using the Windows Resource Kit or writing commands in the Per1 language[2]. The majority of current system administrators do not have time to acquire such knowledge. Hence there is a need of such a tool which will allow the system administrator to remotely control the distributed LAN systems.

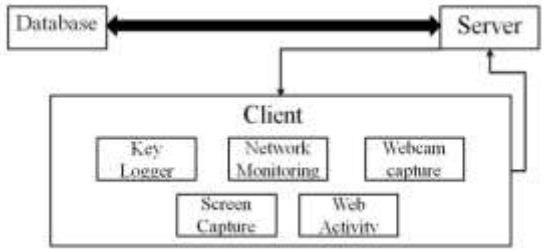
The periodic data acquisition is essential to accurate monitoring in the control loop of cyber-physical systems (CPS). However, providing periodic communication for large-scale CPS is a challenging issue, because the network resources are shared by a large number of nodes. Consequently, it usually happens that, though the sender periodically sends messages, the arrival intervals of messages on the receiver are larger than the period. The threat posed by insiders is very real, and is one that requires serious attention by both organisations and individuals alike. Technological advancements are constantly changing the way that organisations, and the people who act within the organisation, conduct their business. It has become common practice that employees now access documents from organisational file servers, communicate with both internal and external contacts via e-mail, and research information using the Internet. In addition, working practices have changed, so that employees may connect to organisation networks from home, or abroad, to provide flexibility in how we all choose to conduct the work-life balance[7]. Software development teams face a critical threat to the security of their systems: insiders. Unfortunately, when creating software, developers do not typically account for insider threat[4]. Students learning software development are unaware of the impacts of malicious actors and are far too often untrained in prevention methods against them[1]. A few of the defensive mechanisms to protect against insider threats include eliminating system access once an employee leaves an organization, enforcing principle of least privilege, code reviews, and constant monitoring for suspicious activity[6]..

III. LITERATURE GAP

The architectures and softwares studied previously are with certain issues and gaps. Therefore, proposed system will overcome those issues. The difference between current system and proposed system is highlighted in the table given below.

Parameter	Current system	Proposed system	Advantage
Programming module	.net framework	Python	Python is more lightweight and provides easy system level access.
Network architecture	Cloud based	Intranet (LAN)	Less security threats as compared to cloud
Platform	Dependent	Independent	Can be used in multiplatform environment.
Security	More vulnerable	Less Vulnerable	More efficient and high performance

IV. PROPOSED SYSTEM ARCHITECTURE



Server side:
Server chooses a node from the network for monitoring purpose. After establishing connection with the desired node (client) it selects the required functionality to be run on the client machine in order to extract the required information.

Client side:
A programming is running in background in the silent mode. After it receives a request of functionality from the server it runs the required code and passes on the result to the server without client realizing about it.

Database (backend functionality):
The information retrieved by the server is stored in the database storage which is built on MySQL. The reason of using MySQL is its ability to handle structured data efficiently.

V. CONCLUSION

The Employee Activity Toolkit can be established inside an organisation's intranet which would prove to be advantageous for monitoring the employees and detecting any type of insider attacks using various features that includes webcam capturing, remote desktop monitoring, Keylogger, web activity tracking. Moreover the proposed system works in hidden mode on the client side. Hence it is possible to check every client without being detected. Also, the toolkit can work across multiple platforms and hence can be deployed in network with nodes running different operating systems.

REFERENCES

[1] An Insider Threat Activity in a Software Security Course, Daniel E. Krutz, Andrew Meneely, and Samuel A. Malachowsky; 2012; Rochester Institute of Technology {dxkvse, axmvse, samvse}@rit.edu.

[2] Distributed Remote LAN Administration Tool for Windows NT & 2000-based LANs: Preliminary Work; 2013 S. Muknahallipatna J. J. Kane J. Hamann; Dept. of Electrical &Computer Engineering, University of Wyoming sureshm@uwyo.edu.

[3] Developing Insider Attack Detection Model: A Grounded Approach; 2014;

[4] Gary Doss NOVA Southeastern University gdoss@nova.edu Guvirender Tejay NOVA Southeastern University tejay@nova.edu.

[5] Adaptive Periodic Communication over MQTT for Large-Scale Cyber-Physical Systems; Hyun-Chul Jo; Hyun-Wook JinCyber-Physical Systems, Networks, and Applications (CPSNA), 2015 IEEE 3rd International Conference.

[6] Web RTC Implementation Analysis and Impact of Bundle Feature, Kiran Kumar Guduru; Sachin Dev Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference; 2015.

[7] Employee Monitoring - An essential component of your risk management strategy (White paper); Rhonda Turner; Deep Software Inc. #250-625 Agnes Str. New Westminster, BC, Canada V3M 5Y4 www.softactivity.com

[8] IEEE Conference 2015, Caught in the Act of an Insider Attack: Detection and Assessment of Insider Threat, Philip A. Legg, Oliver Buckley, Michael Goldsmith and Sadie Creese Cyber Security Centre, University of Oxford, UK.

[9] White paper – Implementing activity and behavioural monitoring program using Veriato.