User Behavior Tracking System

Aniket Anil Ganvir[1] , Prof. Roshni Talmale[2] , Prof. Rajesh Babu[3]
[1]aniket.a.ganvir@gmail.com, [1]+91-9561449800,
[2]roshnitalmale.cse@tgpcet.com, [3]rajeshbabu.cse@tgpcet.com

Abstract: In this project, we are using an intelligent system for user behavior tracking in computer network. This system can run in the background mode. Because of this, user doesn’t know that the system is actually running in the computer system. This system helps to recognize the unauthorized transactions, illegal communications, gaining access to the confidential and sensitive data of administration. It also stands as a proof for further investigation purposes. Proposed system is implemented using agent approach and can be used in different domains in security system, Web, economic and business system, etc.

Keywords: *Keyloggers, Productivity monitoring, Network tracking, Internet tracking.*

*****

1. Introduction

In today’s world, Internet can be a very powerful tool for good or bad things happened. It can also be enjoyable and efficient tool if we aware of its risks and how to use it safely. In this system software basically runs on desktop at regular intervals. This system software not visible to the user and also not recognize by the Task Managers Processes or Applications. This will also not be detected, by which we can track the activities of a user on desktop PC or on an Office network. By using this system software admin can easily review the users Internet activities by searching the websites and pages viewed recently on any computer and also the offline activities. This tool covertly gathers user information and activity without the user’s knowledge. Essentially whatever one does on the computer is completely tractable by this system software.

Sensitive data is well-defined as information that is secure against unwarranted revelation. Access to sensitive data should be protected. Protection of sensitive data may be required for legal or ethical motives, for issues relating to personal privacy, or for patented considerations.

Personal information: Sensitive personally identifiable information (PII) is information that can be monitor back to an individual and that, if revealed, could result in harm to that person. Such information includes biometric information, medical data, personally identifiable financial information (PIFI). This also includes the unique identifiers such as passport or Social Safety numbers. Threats include not only offenses such as identity theft but also revelation of personal information that the individual would prefer remained private. Sensitive PII should be converted both in transit and at rest.

Business information: Sensitive business information contains anything that positions a risk to the company. Such information includes trade secrets, achievement plans, business information and supplier and client information, among other possibilities. With the ever-increasing amount of data generated by businesses, methods of securing corporate data from unauthorized entree are becoming essential to corporate security. These methods include metadata management and document purification.

Classified information: Classified information relates to an institutional, government body and is restricted according to level of sensitivity (for example, restricted, private, secret and top secret). Data is generally classified to protect security. Once the risk of harm has passed or decreased, classified information may be declassified and, possibly, made public.

2. Background Mode

Background mode working refers to the running software without knowing the user that software actually running in the background. There are many ways to monitoring the user information about his activity on the system. These types of systems are used by many companies now a day. The project is basically a User behavior tracking system. This project is used to keep track on the user work on the system and create log of it. Main feature of this project is that it is working in back ground that’s why we can named it as background mode working.

This is newest tool for tracking user activity on a computer. It records all keystrokes into an encrypted log file. A log file contains information about the user working on the computer. You can view it any time you want with the help of a built-in program. Besides, this tool logs information about the Internet addresses the user has visited. Using this tool you will always know who used the computer, when he used it and for what purpose. This tool can run only under administrator privileges and capable of restricting access to other windows vulnerable applications.

3. Logging & Monitoring

From monitoring you can detect hacking attempts, tracking, virus or worm infections and propagation, configuration problems, hardware problems and many others. Monitoring is most important factor to maintain stability for the network. Information security focuses on ensuring confidentiality, integrity and availability, accountability. From network monitoring you can detect attempts to access to exclude information or resources such as unauthorized access, which in turn ensure confidentiality. You can detect attempts to change or alter information such as file modification, which ensure integrity. And you can detect any kind of problems that can affect the availability of the information such as DOS or DDOS attack. The main goal of this paper is to give an idea about some of the benefits that anyone can get from the complete monitoring of the network. Logging can give detailed information about any access or change for any of the network resources.

A log is a record of the occasions happening inside an association's frameworks and systems. Logs are made out of log passages; every section contains data identified with a particular occasion that has happened inside a framework or system. Logs were utilized principally for inconveniences hooting issues, however logs presently serve numerous capacities inside most associations, for example, advancing framework and system execution, recording the activities of clients, and giving information helpful to researching pernicious action. The far reaching organization of arranged servers, workstations, and other figuring gadgets, and the regularly expanding number of dangers against systems and frameworks, the number, volume, and assortment of PC security logs has expanded extraordinarily.

This has made the requirement for PC security log administration, which is the procedure for producing, transmitting, putting away, investigating, and discarding PC security log information. Logging can be a security head's closest companion. It resembles an authoritative accomplice that is dependably at work, never gripes, never gets worn out, and is dependably in control. On the off chance that legitimately educated, this accomplice can give the time and place each occasion that has happened in your system or framework.

4. Objective

Generally, objective of this User behavior tracking system includes the following major fields:

- Bank sectors
- Medical / Hospitals
- IT Organizations
- International Call Centers
- Institutions / Educational Departments
- Government Bodies
- Internet Business Organizations

5. Methodology

In this system software proposed methodology conclude of proposed architecture and proposed algorithm. Proposed architecture revolve around how the project will work. Whereas proposed algorithm consists of signature-based key logger and hooked-based key logger. Signature-base and hooked-base key logger having different characteristics and processing.

5.1 Modules

Basically user behavior tracking system includes the four main modules. These modules are Folder logging, snapshots, keystroke logging and clipboard. Folder logging feature store all details of folder modification, folder visiting, folder deletion, and folder changes. How many times the user modifies folder or how often user open folder logs. Snapshots feature shows periodical images of user’s desktop or window open in system.

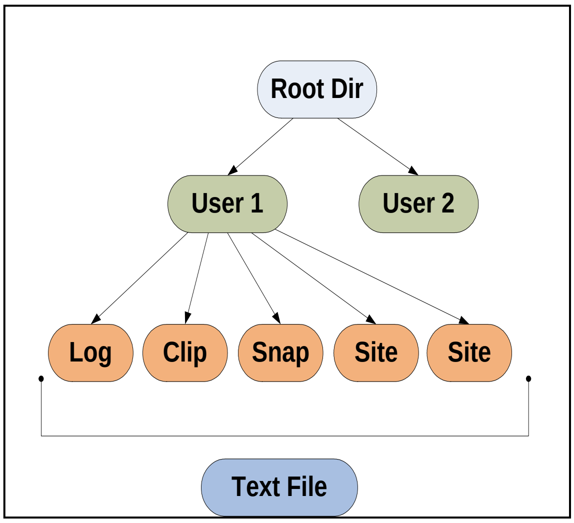


Fig. 5.1: Structure of Log

It will simply take a picture of desktop image and save it to hard disk. Keystrokes log tracks each and every key pressed by user. Keystrokes log consists of messages, codes, file, url name, etc. These information are fetched from keyboard buffer.

5.1.1 Folder Log

Generally folder log stores all details of folder like folder modification, folder visiting, folder deletion, and folder changes. How often the user tries to open some confidential folder on drive. How often user visits the particular folder structure. This module will keep track of visited or opened folder. It will show details of accessed folder by the user.

5.1.2 Snap Shots

Snapshot module takes all snapshots, whatever user doing, all desktop images stores in the server system. Snapshot feature simply take a picture of desktop image. All snapshots are then saved to hard disk. This will ensure the more security for confidential data, administrative files, and all other important information

5.1.3 Keystrokes Log

Keystrokes log is the third module and deals with tracking each and every key pressed by the user. Keystrokes log keep tracks of keystroke details like messages, codes, file, website name, etc. This module helps to monitor the working of users whether they are doing good or bad or worst. Keystrokes log fetched details form Keyboard buffer.

5.1.4 Clipboard Log

Basically clipboard module keeps monitoring the clipboard data. Clipboard data includes the recent copied or cut text and how often user uses the clipboard log. This feature helps to access the recent working structure of the user. Clipboard log ensures that how user doing their job and their responsibilities within the institute or department.

6. Design of Experimentation

System requirement includes the overall system functionalities required to execute the project software. In order to execute the project software in proper manner, these requirements are required to fulfill by the system configuration.

6.1 User Interface

User interface consists of easily understands menus and navigation tools. The firstly open windows consists of setting, start logger, hide logger, stop logger, log view and exit navigation in the upper top navigation section. Application setting allows to change functioning or disable/enable the features. Start logger activates the logger and start to track the user behavior. To work software in background without knowing to user that software running in background start the Hide logger navigation tool.

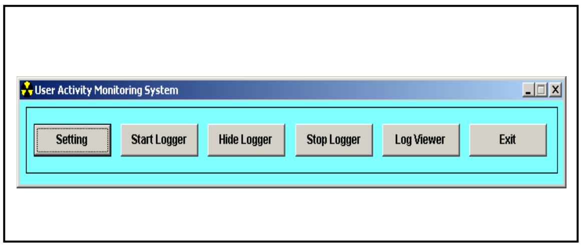
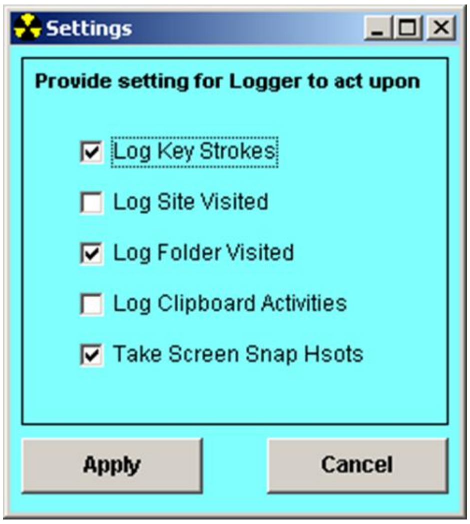


Fig. 6.1.1 Menu and tools user interface.

User interface menu and tools shows the UI of main window which consists of Setting, start logger, hide logger, stop logger, log viewer and exit.



Provide setting for Logger to act upon

☑ Log Key Strokes

□ Log Site Visited

☑ Log Folder Visited

□ Log Clipboard Activities

☑ Take Screen Snap Hsots

Fig 6.1.2: Setting window user interface

Settings manage all the functionalities and allow disable/enable particular feature. Setting window consists of five options to activate or deactivate. These options are log key strokes, log site visited, log folder visited, log clipboard activities, take screen snap shots. All these functionalities are shown in above figure.

7. Conclusion

Thus, we have managed to utilize information from system to track the user and provide security to admin by monitoring his behavior among the departments. Whether it is good for company or user just targeting to leak the confidential data of the company. How often user can interact with the system environment. This will also helps to recognizing the unusual activities like transactions, communications, modifying confidential data, etc

8. References

[1]. Preeti Tuli, Priyanka Sahu,―System Monitoring and Security Using Keylogger‖, IEEE Technology and Society

Magazine, IJCSMC, Vol. 2, Issue. 3, March 2013, pg.106 – 111.

[2]. Hangjin Zhang, Kevin Almeroth, Monica Bulger, ―An Activity Monitoring System to Support Classroom Research‖, IJRES, Vol. 1, No. 2, July 2012, pp. 49~54, CA 93106.

[3]. G. Hoglund and J. Butler, Rootkits, ― Subverting the Windows Kernel ‖. Addison-Wesley Professional, 2005.

[4]. Tom Olzak, ―Keystroke Logging (Keylogging)‖, IJAREIE, Vol. 2, Issue 4, April 2013.

[5]. Bauer, Michael D, ―System Log Management and Monitoring of Building Secure Servers‖, IJAIEM, Volume 4, Issue 5, May 2012.

[6]. Babbin, Jacob et al, ―Security Log Management: Identifying Patterns in the Chaos‖, IJARCCE, Vol. 3, Issue 2, February 2014.

[7]. Christopher Miller, Sarah Chasins, Carolyn Farris, ―An Integrated Monitoring System for Smartphones‖, IJAREIE, Vol. 3, Issue 5, May 2014.

[8]. Stout, Kent, ―Central Logging with a Twist of COTS in a Solaris Environment.‖, SANS Institute, March 2002.