International Journal of Research
eISSN: 2348-6848 & pISSN: 2348-795X Vol-5 Special Issue-13
International Conference on Innovation and Research in Engineering, Science & Technology
Held on 23rd & 24th February 2018, Organized by Tulsiramji Gaikwad Patil College of Engineering & Technology, Nagpur, 441108, Maharastra, India.

User Behaviour Tracking System

Aniket Anil Ganvir[1], Prof.Rajesh Babu[2]
[1]M.Tech Student TGPCET, Nagpur.
[2]Assistent Profesor, CSE Dept, TGPCET, Nagpur.
aniket.a.ganvir@gmail.com

Abstract:

An intelligent system for user behaviour tracking in computer network. The system provides on-line and off-line tracking and allows to detect anomalies in user behaviour. On-line tracking is carried in real time and used to predict user action. Off-line tracking is carried out after user has ended his work, and based on the analysis of statistical parameters of user behaviours. 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

The Internet can be a very powerful tool for good or bad. Being aware of the risks and how to use it safely can make it an enjoyable and useful experience. In this project software basically runs on desktop at regular intervals in stealth mode. This software not visible in the Task Managers Processes or Applications and also not be detected, by which we can monitor the activities of a user on desktop PC or on an Office network. By using this software you can review the users Internet activities by finding 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 viewable by this tool.

2. Invisible Mode Working

There are many ways to tracking 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 behaviour 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 which can called as invisible 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. Objective

- To provide Security in Hospitals, Banks, IT organizations, Institutions, Universities, Call-centers, and Government bodies.
- To overcome unauthorized accesses, prevention of confidential information leak from organization.
- To control network usage with tracking transactions over the Internet.
- To protect intellectual property and business secrets, prevent and stop sabotage and data theft, prevent Internet/email abuse, reduce workplace slackers.

4. Problem Definition

The Clipboard is a temporary storage area for information that you have copied or moved from one place and plan to use somewhere else. You can select text or graphics and then use the Cut or Copy commands to move your selection to the Clipboard, where it will be stored until you use the Paste command to insert it elsewhere.

For example, you might want to copy a section of text from a website, and then paste that text into an email message. The Clipboard is available in most Windows programs. The goal of this paper is to give an idea about some of the benefits that anyone can get from the complete monitoring of the system

network. Key logging programs, commonly known as key loggers, are a type of malware that maliciously track user input.

Keystroke logging, also known as key logging, is the capture of typed characters/number. Hiding software isn't support in this technique. Next is Internet Security, Spying on how user gone through Web Surfing like Transactions he done, Read articles doesn't supported by Hook based key loggers.

5. Proposed Methodology

Basically 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. Proposed Architecture

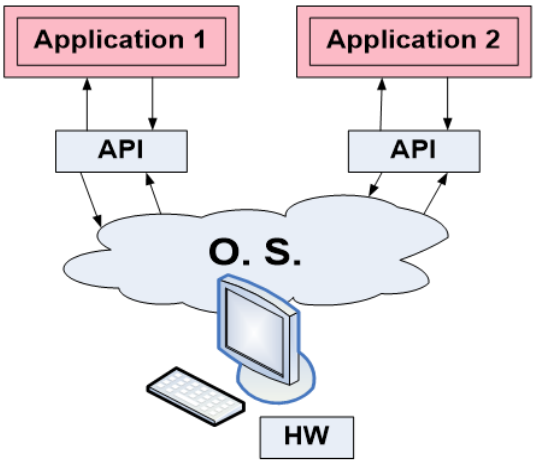

Figure 1. Proposed Architecture.

Above architecture shows the basic block diagram of how such a project will work. As we are saying that we are gathering the information but from where this is the main question as till studied we get that if any software needs some information from hardware or from system then software need to contact Operating system for the same. By executing some O. S. functions called as API software or user can get the system information or the hardware information and we will use same technology or concept.

5.2. Proposed Algorithm

Proposed algorithm of this paper consists of two main keyloggers which required for special functioning and implementing the ideas of tracking among the system.

5.2.1. Signature-based Keylogger. These are applications that typically identify a key logger based on the files or DLLs that it installs, and the registry entries that it makes.

Although it successfully identifies known key loggers, it fails to identify a key logger whose signature is not stored in its database. Some anti-spyware applications use this approach, with varying degrees of success. Most of the anti-virus software's detect Key logger application based on this approach.

5.2.2. Hooked-based Keylogger. Third-order headings, A hook process in Windows uses the function SetWindowsHookEx (), the same functions that hook based key loggers use. This is used to monitor the system for certain types of events, for instance a key press / mouse-click — however, hook based anti-key loggers block this passing of control from one hook procedure to another. This results in the key logging software generating no logs at all of the keystroke capture. Although hook based anti-key loggers are better than signature.

Based anti-key loggers, note that they still are incapable of stopping kernel-based key loggers. The mechanism used to intercept events using specific functions (e.g. sending Windows messages, data input via the mouse or keyboard) in Microsoft Windows is called 'hooking'. This function can react to an event and, in certain cases, modify or delete events.

6. Flowchart

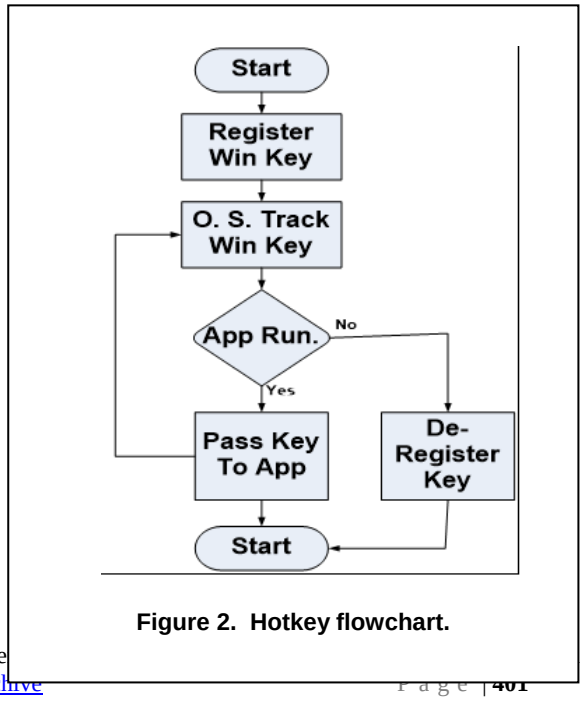

Figure 2. Hotkey flowchart.

Above hotkey flowchart shows actual flow of project. Where first uses some API function to list the win Key, which is by in the software. Then arrangement will trap this key and pass this to listed application until the application is running. When request is close the OS will be list the win key. Now this key can use by other request also.

7. References

[i] 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.

[ii] 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.

[iii] G. Hoglund and J. Butler, Rootkits, " Subverting the Windows Kernel ". Addison-Wesley Professional, 2005.

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

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

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

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

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