# Developing Software Based Key logger and a Method to Protect from Unknown Key loggers

**Sivarajeshwaran S., Ramya G., Priya G.**

***Abstract- Key loggers are hardware or software used to harvest confidential information. Keystroke logging also known as keylogging or keyboard capturing, that record the keys struck on the keyboard. The main aim of this project is to develop user-space software keylogger and a method to detect and close the unknown keylogger running in stealth mode. Software based keylogger is a set of computer program implanted on a machine to capture the user activity by logging keystrokes and delivering them to a third party though their email account and also save them as a file in a specified folder without knowing to the owner of the computer. Keyloggers are also used for legitimate purposes such as surveillance in company and parental monitoring infrastructures. Software based Anti keylogger are used to detect and close software in which keylogger running in stealth mode. It will be done by comparing the executable files of the running software.***

***Keywords:- keylogger, software, Keystroke, running, project***

## I. INTRODUCTION

Keystroke logging, often referred to as Keyboard Capturing or keylogging, is the action of recording the keys struck on a keyboard, typically in a stealth mode so that the person using the keyboard is unaware that their actions are being monitored. It provides a great problem to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cyber criminals can get account numbers and PIN codes for e-payments systems, user names, email address, email passwords etc. It also has very legitimate uses in studies of human-computer interaction. There are numerous keylogging methods; they are hardware and software-based approaches. Software-based keylogger are computer programs designed to work on the target computer's software. Software-based keylogger have several categories based on the privileges they require to execute.Keylogger with full privileges will work in kernel space and unprivileged keylogger work in user space.

**Kernel-based**: A program on the machine 'gets root' and hides itself in the OS, and starts intercepting keystrokes (because they always go through the kernel).Such keyloggers reside at the kernel level are difficult to detect, especially for user-mode applications that don't have root access. A keylogger using this method can act as a keyboard device driver for example, and gain access to any information typed on the keyboard as it goes to the operating system.

**API-based**: These keyloggers hook keyboard APIsinside a running application. The keylogger registers for keystroke events, as it is a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it. Get Async Key State, Get Foreground Window. These functions are used to get the keyboard events, mouse events and current window titles. Software based anti keylogger used to protect from unknown keyloggers. It will get all process running in the computer and compare the executable files of the software, if it matches then all running process of the specified software will be killed. So, keylogger running in stealth mode will also get closed.

## II. LITERATURE SURVEY

In order to understand about keyloggers more clearly, it is necessary for a reader to grasp detailed knowledge about what is keyloggers, why they are so easy to implement, why countermeasures taken till know is fail to provide adequate solution for it. To answer this type of questions we will discuss about the approaches proposed so far to address the problem and why they are not satisfactory and disadvantages of these approaches. Keyloggers are used to harvest the user’s input is a privacy-breaching activity that can be done at many different levels. When physical access to the machine is available, an attacker might wiretap the hardware of the keyboard to grasp the confidential information. The use of the external keyloggers designed to depend on some physical property, either the audio emanations produced by the user typing or the electromagnetic emanations of a wireless keyboard [4]. External hardware keyloggers are implemented as tiny device to be placed in between keyboard and motherboard, all these strategies require the attacker to have physical access to the target computer. Keyloggers are implemented on computer machine intentionally to monitor the user keystrokes logging activity and eventually delivering them to a third party [1]. These keyloggers are seldom used for legal purposes. Keyloggers are often maliciously used by attackers to steal secret information. Many credit card passwords and numbers have been stolen using keyloggers which makes them one of the most dangerous types of spyware known to date [2][3]. Keyloggers can be implemented as tiny hardware devices or more conveniently as software. Software-based keyloggers can be further classified based on the privileges they require to execute. Keyloggers implemented by a kernel module run with full privileges in kernel space. Conversely, a fully unprivileged keylogger can be implemented as a simple user-space process.

**Manuscript Received on May 15, 2015.**

**Sivarajeshwaran S.,** Vishwakarma Institute of Technology, Vellore-632014, Tamilnadu, India.

**Ramya G.,** Vishwakarma Institute of Technology, Vellore-632014, Tamilnadu, India.

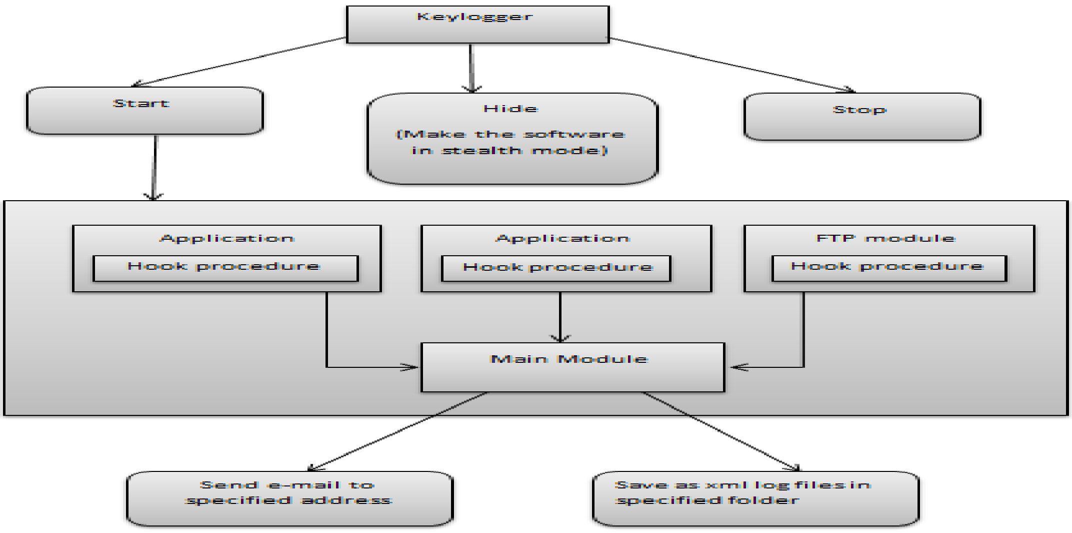
**Priya. G,** Vishwakarma Institute of Technology, Vellore-632014, Tamilnadu, India

It is important to notice that a user-space keylogger can easily depend on documented sets of unprivileged APIs commonly available on modern operating systems (OSs). This is not the case for a keylogger implemented as a kernel module. In kernel space, the programmer must rely on kernel-level to intercept all the messages dispatched by the keyboard driver, Furthermore, a keylogger implemented as a user-space process is much easier to deploy since no special permission is required.

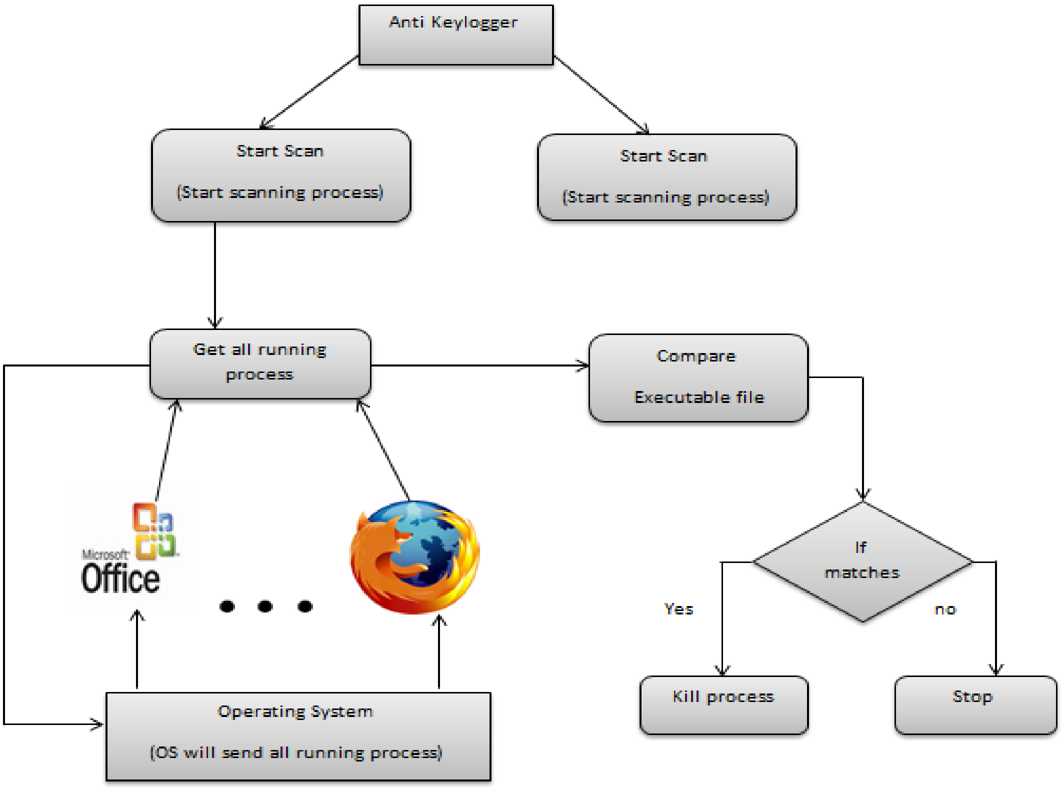
Anti-hook technique is based on the fact that each processes either hidden or on display uses hooks APIs for the purpose of hooking. So if we become able to scan all the processes and static executable and DLLs and detect the suspicious processes or files, which uses hooks. Then we can get the complete detail about that particular file or process. We can also terminate its execution or existence to secure the system. This paper focuses the anti-hook technique by keeping in view the Key loggers development process so that personal privacy and security can be ensured [8].

## III. ARCHITECTURE DIAGRAM

### 3.1 SOFTWARE BASED USER-SPACE KEYLOGGER:


Keylogger
Start
Hide
(Make the software in stealth mode)
Stop
Application
Hook procedure
Application
Hook procedure
FTP module
Hook procedure
Main Module
Send e-mail to specified address
Save as xml log files in specified folder

### 3.2 ANTI-KEYLOGGER:



## IV. MODULE DESCRIPTION

### 4.1KEYLOGGER:

User-space key loggers do not require any special privilege to be deployed. They can be installed and executed regardless of the privileges granted. So it is easy to get all information from user.

### *4.1.1 MONITORING USER DATA*

Function used to get the keystrokes and mouse events will start to work. It will capture all keystrokes what users typing in the keyboard and also capture the mouse clicks. It will get the current window title. It also displays the following details in the screen. It will hook all keystrokes using keyboard API. So without knowing to user of the system all their data will be monitored by the owner of the software.

### *4.1.2 SENDING SECRET INFORMATION*

We have two options in this software, they are save monitored data and send that data through e-mail. We can select any option. We can save the collected information in a specified folder in a particular time interval. We can send the collected information to specified e-mail id in a particular time interval. So user keystrokes and mouse events will be shared to third party. By this way the confidential information like bank passwords, pin numbers, username are known to the cyber criminals.

### *4.1.3 MAKE THE SOFTWARE IN STEALTH MODE*

This module is used to make the software in stealth mode. We can hide the software from the owner but in running state. So without the knowledge of the owner the software will run in hidden mode. To unhide the software we need to press certain combination of keys specified by the developer of the software. Stop button is used to stop the running hook function in the software. So the software will not get any keystrokes or mouse events pressed by user.

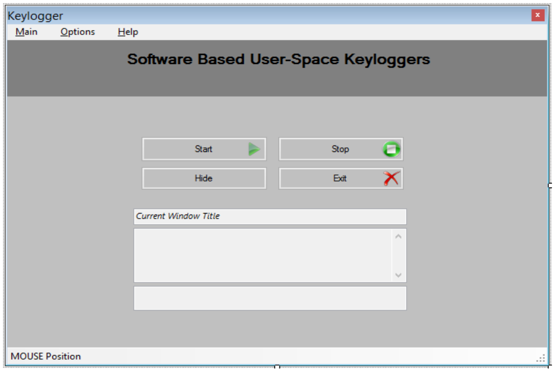
### 4.2 ANTI KEYLOGGER

Anti keylogger is used to detect and close the software in which keylogger is running in stealth mode in the system. It is software based anti keylogger.

### *4.2.1 SCAN FOR KEYLOGGER*

Anti keylogger is used to turn off the keylogger working in the computer system. In this project software based anti keylogger is developed. Once the start scan button in the anti keylogger software is pressed it will get all running process from the operating system. It will compare whether specified executable file name and the running process executable file name get matches. If it matches then the software will be closed. So if any keylogger running in that software in stealth mode will also get closed. Stop scan button will stop the scanning process.

## V. HOMEPAGE



## VI. CONCLUSION

We modeled the behavior of a software based user-space keylogger to get all confidential information from user of the system by getting their keystrokes events and mouse clicks without the knowledge of the user. So user of the system is unaware of things happening in background. We then discussed the problem of the user .In order to overcome this problem we presented an implementation of our detection technique by executing the software based anti keylogger which is developed. Software based anti keylogger will detect the specified software and close it. It will be used to find and close software, so any keylogger running in that software without the knowledge of the user of the system will also get closed. We successfully evaluated our protection method in the Microsoft visual studio software. We believe our approach considerably raises the bar for protecting the user against the threat of software based keyloggers.

## REFERENCE

1. T.Holz, M. Engelberth, and F. Freiling, “Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones,” Proc. 14th European Symp. Research in Computer Security, pp. 1-18, 2009.
2. San Jose Mercury News, “Kinkois Spyware Case Highlights Risk of Public Internet Terminals,” http://www.siliconvalley.com/mld/siliconvalley/news/6359407.htm, 2012.
3. N. Strahija, “Student Charged After College Computer Hacked,” http://www.xatrix.org/article2641.html .
4. Martin vuagnoux and sylvainpasini. Compromising electromagnetic emanations of wired and wireless keyboards, in proceeding of the 18th conference on USENIX security symposium, USENIX Association. USA 2009.
5. J.Han, J.Kwon and H.Lee, "Honeyid: Unveiling Hidden Spywares by Generating Bogus Events" 2008.
6. Y.Al-Hammadi and U.Aickelin, "Detecting Bots Based on Keylogging Activities", 2008
7. M.Aslam, R.Idrees, M.Baig and M.Arshad, "Anti-Hook Shield against the Software Key Loggers", 2004
8. S.Ortolani, C.Giuffrida and B.Crispo, "Klimax: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware", 2011
9. Moser, C. Kruegel, and E. Kirda, “Exploring Multiple Execution Paths for Malware Analysis,” Proc. IEEE 28th Symp. Security and Privacy, pp. 231-245, May 2007.