Cyber Security Automation tool

Major Project (IT)

Submitted in partial fulfillment of the requirements
for the degree of

BACHELOR OF ENGINEERING
(Information Technology)

by

Pranav Darwai

0225IT181040

Under the guidance of
Prof. Vishal Pranjape
Department of Information Technology

Global Nature Care Sangathan Group of Institutions, Jabalpur (M.P.)

RAJIV GANDHI PRODYOGIKI VISHWAVIDYALAYA, BHOPAL
(M.P.)

DEC-2021

Global Nature Care Sangathan Group of Institutions, Jabalpur (M.P.)
Department of Computer Science & Engineering

Certificate

This is to certify that the Major Project report entitled Cyber Security Automation tools submitted by **Pranav Darwai** has been carried out under my guidance & supervision. The project report is approved for submission towards partial fulfillment of the requirement for the award of degree of **Bachelor of Engineering** in **Information Technology** from "**Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (M.P).**

Prof. Guide Name
Vishal Pranjape

Prof. Vishal Pranjape
HOD
Dept of Information Technology

Global Nature Care Sangthan Group of Institutions, Jabalpur (M.P.)
Department of Computer Science & Engineering

Certificate

This is to certify that the Major Project-I report entitled "**Cyber Security Automation Tools**" is submitted by **Pranav Darwai** for the partial fulfillment of the requirement for the award of degree of **Bachelor of Engineering** in **Information Technology** from **Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (M.P).**

Internal Examiner
Date :

External Examiner
Date :

Declaration

I hereby declare that the project entitled **"Cyber Security Automation tools"** which is being submitted in partial fulfillment of the requirement for award of the Degree of Bachelor of Engineering in Computer Science and Engineering to **"RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL (M.P.)"** is an authentic record of our own work done under the guidance of **Prof. Vishal Pranjape**, Department of Computer Science & Engineering, **GLOBAL ENGINEERING COLLEGE, JABALPUR**.

The matter reported in this Project has not been submitted earlier for the award of any other degree.

Dated :2 Dec 2021 **Pranav Darwai**
Place : Jabalpur **0225IT181040**

Acknowledgment

We sincerely express indebtedness to esteemed and revered guide “Prof. Vishal Pranjape”, Assistant Professor, for his invaluable guidance, supervision and encouragement throughout the work. Without his kind patronage and guidance the project would not have taken shape.

We take this opportunity to express a deep sense of gratitude to “Prof. Vishal Pranjape”, Head of “Department of Computer Science & Engineering” for his encouragement and kind approval. Also we thank him for providing the computer lab facility. We would like to express our sincere regards to him for advice and counseling from time to time.

We owe sincere thanks to all the lecturers in “Department of Computer Science & Engineering*”* for their advice and counseling from time to time.

Dated :2 Dec 2021 **Pranav Darwai**
Place : Jabalpur **0225IT181040**

1. Introduction

Keystroke logging, software also known as keylogging, is simply tracking the keys that are struck on a keyboard. This can be done in multiple ways using a wide variety of hardware devices or software. The reason for its large threat to networks and their security is due to its covertness 4 Chandigarh Polytechnic College nature. Most keyloggers show no signs of any intrusion within the system allowing for them to gain typed information without anyone having knowledge of its actions except for the user who installed it. With the proper keylogger installed on the correct machine a person could easily gain access to a company's entire network infrastructure. In terms of system critical data or extremely privileged information this could cause problems for a vast amount of people very quickly. Types of keyloggers There are two basic types of keyloggers, hardware and Software.

1.1. Hardware keyloggers These can be implemented via BIOS-level firmware or via a device that can be plugged in line between a wired computer keyboard and a computer. All of the information that is logged by a hardware-based keylogger is stored to its own internal memory leaving no trace of its existence on the machine itself. One of the main advantages to using a hardware key logger over a software based one is that it can begin recording keystrokes from the moment the computer is turned on. This gives it the ability to capture passwords related to the BIOS and system encryption. All hardware keyloggers must have both a microcontroller and nonvolatile memory. The microcontroller processes the data stream between the computer and the keyboard while the non-volatile memory stores the information collected even after power to the computer is lost. Hardware keyloggers non-volatile memory can range anywhere from a few kilobytes to several gigabytes. With each key stroke taking typically only one byte of space most hardware keyloggers can hold millions of character strings. Typical hardware keyloggers are designed to blend in with the rest of the computer cabling system. They either resemble a PS/2 connection or more recently a USB interface that simply plugs into the end of the keyboard cable and then into the computer, hence the inline description. The pictures below depict both a PS/2 (left) and a USB (right) inline keylogger. 5 Chandigarh Polytechnic College In the event a person would need to be even more covert with their hardware keylogger a circuit attachment installed inside of the keyboard is also available. With this type of modification to the naked eye nothing will appear to have changed with

the computer system while still given access to the data collected by the keylogger. The picture below is an example of a circuit keylogger that can be soldered within the keyboard's circuitry. To be even more inconspicuous the BIOS, which handles all of the events of the keyboard, could also be reprogrammed to retain keystrokes for later assessment. This type of modification would be done strictly to the computers firmware requiring no extra hardware since the collected data could be stored directly to the computer's hard drive. Another type of logger that is considered to be hardware based is an acoustic Keylogger. Every time a key is pressed on the keyboard it has a unique sound signature. With the proper frequency analyzer a person would be able to find a repetition frequency of similar acoustic keystroke signatures. A few things become necessary for this to work. The timing between the keystrokes and the language the user is typing in can be combined to create a so called map of sounds to letters. A fairly long string of about 1000 or more typed characters is required to ensure that a proper map is created. Lastly, in a world today where most every peripheral device such as keyboards and mice are becoming wireless, there are hardware keyloggers that can attempt to capture this information as well. Wireless keyloggers simply collect the data that is transmitted between the wireless keyboard and the receiver and attempt to crack the encryption between the two devices. With wireless keyloggers the information collected can be retrieved by the user from any computer with the supplied software within range of the wireless keyloggers transmitter. This is the best option when it comes to hardware keyloggers because it only requires the installer to gain access to the system once. With the ability to retrieve the logged information wirelessly the installer will have no need to recover the keylogger risking getting caught by someone in the process.

1.2. Software Keyloggers Software keyloggers fall into basically five main categories, hypervisor-based, API-based, Form grabbing based, Memory injected based, and Kernel based. Hypervisor- based loggers 6 Chandigarh Polytechnic College can be embedded in a malware hypervisor running behind the operating system. The essentially become a virtual machine that is undetected by the computer user. A good example of this is a program called Blue Pill. API-based loggers are simple programs that hook the keyboard's API allowing for

windows to notify the program each time a key is pressed. Even though these are the simplest to write they may be easily detected in the event there is a great amount of keystrokes to pull. The increased amount of key pulling will also increase the CPU usage which can be seen by the computer user via task manager or some other 3rd party software that displays CPU usage. A form grabbing based logger is confined only to web based forms. These loggers record data that is input into forms and captured when the user clicks the submit button. Because this is done on the host side of the machine it can bypass any security set up by a HTTPS website such as Bank account web pages and those alike. Memory injection based loggers do just as the name states; they inject directly into memory and alter memory tables to capture keystrokes in web forms and other system functions. This method is commonly used when the user wants to bypass Windows UAC (User Access Control). Finally, Kernel based loggers are the most difficult to program and implement but also allow for the greatest amount of discrepancy. These loggers can act as a keyboard driver giving it the ability to capture any and all information typed on the keyboard. They are typically implemented using rootkits that can bypass the operating system kernel and give the user unauthorized access to the system hardware.

2. Objective of the Project

2.1. Project Summary

There are a multitude of keyloggers from hardware based to software based. Each of them has their advantages and disadvantages. Keyloggers prose one of the largest threats to computer and network systems. Most everything that users protect on computers is protected by usernames and passwords. Keyloggers basically bypass these setup safety protocols making their data completely vulnerable. In order to prevent keyloggers from recording 7 Chandigarh Polytechnic College sensitive data such as passwords, usernames, bank account number, and others alike it is pertinent that administrators follow the steps of prevention 2.2. Project Description Keyloggers have a wide variety of uses and can be either hardware-based or software-based. The main purpose is to log everything that is typed on a keyboard and store it in text files for later assessment. Everything that is typed will be logged; this

includes sensitive information such as passwords, names, pin numbers, and even credit card numbers. While keyloggers have many acceptable uses they also have many malicious uses. Acceptable uses ¬ Parent monitoring child's computer usage. ¬ Boss monitoring employee's computer usage. ¬ Government retrieving information pertinent to a crime Malicious uses ¬ Cracking passwords. ¬ Gaining unauthorized information. ¬ Stealing credit card numbers. ¬ Reading sent emails or messages not intended for public viewing. ¬ Retrieving secret names. ¬ Stealing account numbers Most associations with keyloggers are much like those with hackers. Even though there are many beneficial uses to keyloggers the only ones the public seems to associate with them are the malicious ones.

3. Methodology

3.1. Keylogger Construction

The main idea behind keyloggers is to get in between any two links in the chain of events between when a key is pressed and when information about that keystroke is displayed on the monitor. This can be achieved using video surveillance, a bug in the keyboard, wiring or the computer itself, intercepting input/output, substituting the keyboard driver, the filter driver in the keyboard stack, intercepting kernel functions by any means possible (substituting 8 Chandigarh Polytechnic College addresses in system tables, splicing function code, etc.), intercepting DLL functions in user mode, and, finally, requesting information from the keyboard using standard documented methods. Experience shows that the more complex the approach, the less likely it is to be used in common Trojan programs and the more likely it is to be used in specially designed Trojan programs which are designed to steal financial data from a specific company. Keyloggers can be divided into two categories keylogging devices and keylogging software. Keyloggers which fall into the first category are usually small devices that can be fixed to the keyboard, or placed within a cable or the computer itself. The keylogging software category is made up of dedicated programs designed to track and log keystrokes. The most common methods used to construct keylogging software are as follows:

- A system hook which intercepts notification that a key has been pressed (installed using Windows API) for messages sent by the window procedure.
- A cyclical information keyboard request from the keyboard (using WinAPI Get(Async)KeyState or GetKeyboardState).
- Using a filter driver (requires specialized knowledge of coding language)

This project is a software based project and all we need as computer resources are just PCs with the tools (needed software) installed in. The number of computers will be as much as the team member working in this project. Also python and C++ IDE for testing in the implementation process. And a virtual box that help in testing and prevent our system from any error or failures.

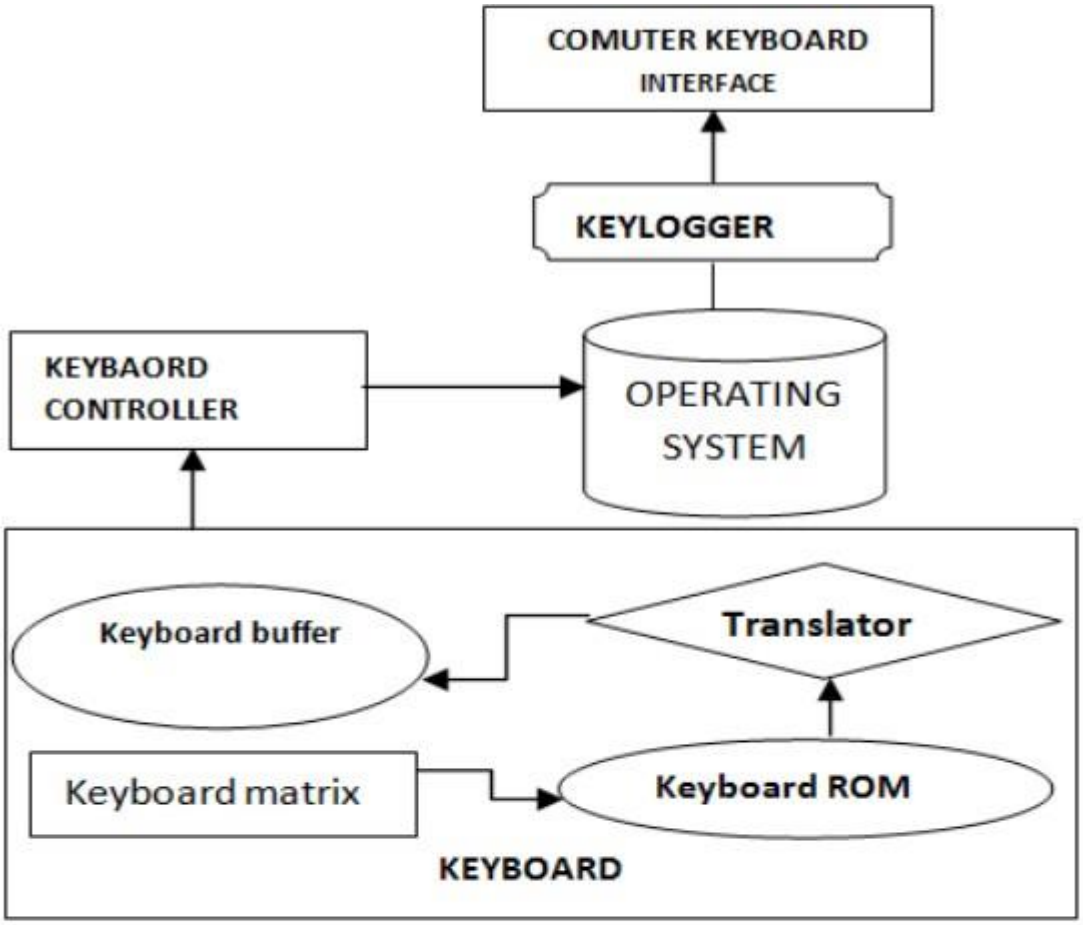
4.1. Hardware Requirements

We need computer resources with sufficient hardware and the tools installed in.

- Processor - Intel Core i3 @ 1.80 GHz
- RAM - 2 GB
- Hard Disk - 500 GB
- Monitor - 15” colour monitor
- Keyboard - 122 keys
- Mouse - Any two button optical mouse with standard 800 DPI
- Network card -10-100 MBPS of Network card 4.2. Software Requirements

This keylogger will be software based program where people can use this for their study purpose or monitoring there system use. Since it is a software application an IDE will be used in order to write code and to run them. Among these tools, we need to install latest version of python in our computers. With the help of these tools, it is possible to implement a keylogger to a system and maintain a log of pressed keys. In addition to these tools, the languages we will use is Python and C++. Some other required software are

- Operating System: Windows v10
- Virtual Box: Oracle VM Virtual Box
- Python Version: Python v3.7.2
- Python IDE: PyCharm
- C++ IDE: Code Blocks



Data Flow Diagram I