Parental Monitoring Automation By Keylogger

A. Sunitha, Assistant professor
Department of Computer Science and Engineering
Vetrivel. E Student of Computer Science and Engineering
Vishwa. V Student of Computer Science and Engineering
St. Joseph College of Engineering, Sriperumbudur, Chennai.

Abstract:

The technique of recording all the pushed keys on a keyboard autonomously, so that the person using the keyboard is unaware that their actions on the computer are being observed, is known as keystroke logging. In the world of cybercrime, keyloggers are usually used for nefarious purposes including obtaining personal information and credit card numbers. However, a keylogger can be useful for monitoring user actions without being detected for ethical reasons. Parents, for example, can employ a keylogger to keep track of their children's online activities. The recorded keystrokes are saved in the log file. The current log files in the keylogger, on the other hand, are not encrypted and can easily be hacked for malevolent reasons. This study offers a novel software-based keylogger with encrypted log files to improve keylogging security in the Industrial Revolution. 4.0

Introduction:

As the name implies, a keylogger, also known as keystroke logging, is a tool that can log or record every single key that is triggered or pushed by a user on a keyboard. The keylogger system can also be programmed to capture clipboard logging, active windows session, mouse action, or screen recording in addition to keyboard key presses [1]. Keyloggers are available in both hardware and software formats, each with its own set of benefits and drawbacks. Since the 1970s, keylogger has been around for more than four decades. Early keylogger was used by spies to infect IBM Selectric electronic typewriters in the United States Embassy, and Consulate buildings in Moscow and St Petersburg [2][3].

Objectives:

- Keylogger steal the confidentials information and the completely run in stealth mode.
- Mostly data are captured by the keyloggers are stored in the same system.
- My approach is the data are send to the parent mail id with certain period of time the keyloggers datas are not stored in the system.

Literature Survey:

Muzammil Hussain, Ahmed Al-Haiqi, AA Zaidan, BB Zaidan, ML Mat Kiah, Nor Badrul Anuar, Hussain, Muzammil Hussain,25, 1–25, 2016 Pervasive and Mobile Computing Smartphone sensor capabilities have opened up new possibilities for creative UI and context-aware applications. They've also opened up new avenues for potential threats to user privacy and security breaches. Researchers recently investigated a novel attack vector that uses the built-in motion sensors in smartphones to infer user taps. Despite the lack of physical keyboards, this new side channel has introduced the threat of keylogging to cellphones. This study examines and surveys this form of attack.Jassim Happa, Hugo Sbai, Michael Goldsmith, Samy Meftali 18-32, 2018 International Symposium on Cyberspace Safety and Security

Because they can function in user space, easily be spread, and upload information to distant servers, keyloggers and screenloggers are one of the most active and growing dangers to user confidentiality. They employ a variety of strategies and can be executed in a variety of ways. Keyloggers and screenloggers have been diverted from their intended and legal use to be used for malevolent purposes, endangering the privacy of users, particularly bank customers. This paper provides an overview of keylogger and screenlogger assaults in order to raise awareness of the problem by covering basic topics linked to bank information systems and describing how they work, as well as presenting and discussing a wide range of viable solutions.

SYSTEM DESIGN:

The prototype keylogger will rely on the Windows API to capture all virtual key codes and translate each virtual key code back to the actual keyboard key value before it is recorded into a log file.

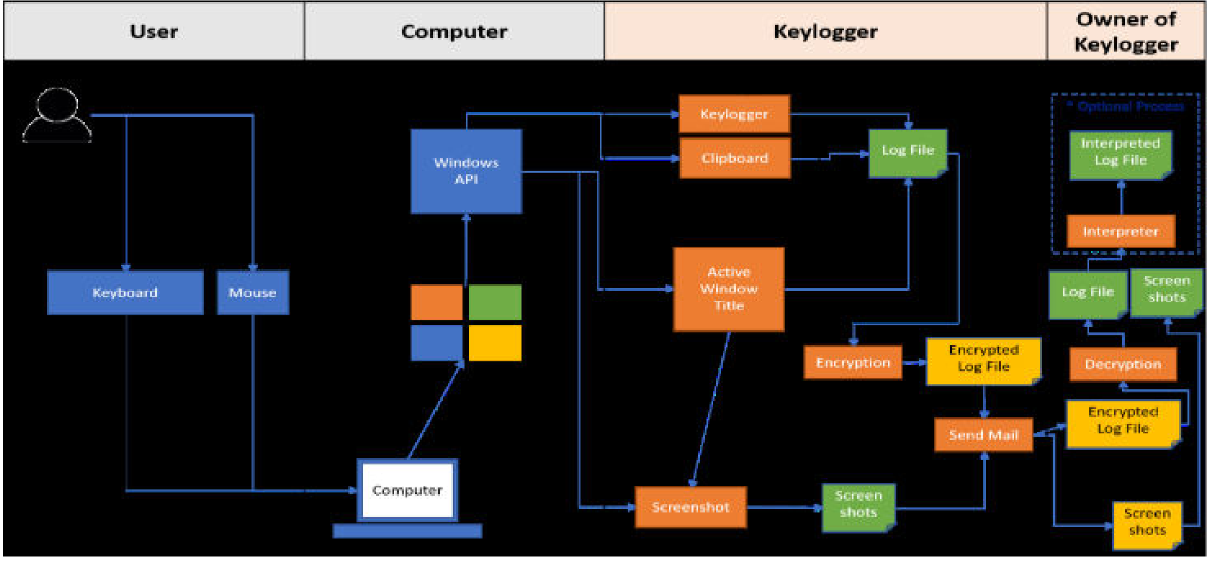


Fig1

In the meantime, the keylogger will record clipboard's data as well while recording the virtual key codes. But before it is logged into a log file, it will first check whether the current clipboard's data is the same as previously captured data, and if it is the same, the current clipboard's data will not be recorded into the log file to reduce the amount of redundant clipboard data being recorded into the log file. This process is required because the clipboard's data is captured continuously at a fixed time interval. Besides that, the prototype keylogger will record the active window's title name as well to provide more comprehensive information regarding what application is being used at the moment. Since the active window's title name is being captured continuously at a fixed interval, if a user remains on the exact same window, the keylogger will captured the exact same window's title as before. Hence, before the active window's title is logged into a log file, it will perform similar task as how clipboard data is being recorded, which is to perform a check on whether the current active window’s title name is the previous captured title to minimize the number of redundant active window’s title being captured. Once the active window’s title is logged into the log file, a screenshot will be tak- en by the key logger to provide better picture on how the applica- tion looks like.

All log files will be encrypted first on the target computer and all screenshot image files (in .jpg format) will have their file format changed to .slog format by the keylogger software before all files are being attached and sent to the owner of the keylogger software through e-mail or FTP. Once the owner has received the encrypted log file and screenshots, the owner can decrypt it using the decryp- tion tool to view the log file and screenshots. Optionally, the own- er can also use the interpreter tool to further translate all keyboard key values recorded in the log file to a more readable log file

Clipboard logging module

Clipboard Logging is required to ensure that the keylogger will record or log the Windows Clipboard data. In Operating System (OS), clipboard is a short-term data storage area used to store cop- ied information including text, files, folders, shortcuts, images, videos, and more [13]. Although clipboard can store various types of data, the clipboard logging module will only log ANSI string and store the data in a text log file. This module will capture the target machine’s clipboard data with the help of Windows API whenever it detects a new ANSI string or text is copied into the clipboard. A module called *clipboard.h* is developed using C++ to capture the Windows clipboard information. To use it, the user is required to include the *clipboard.h* header file to the C++ source file, and the *fstream* header in the source file to create an output log file using standard *ofstream*. Standard *ofstream* is an output stream class used to operate on a file.

Architecture Diagram:

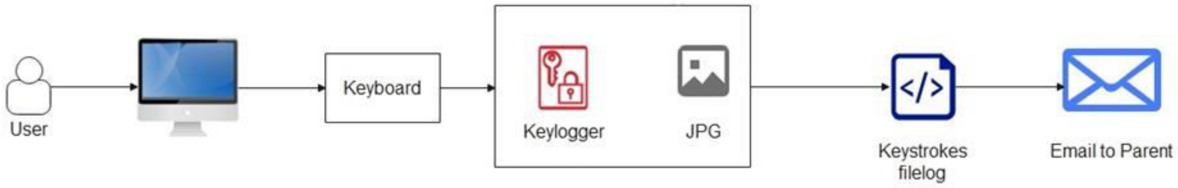


Fig.2

So the complete work flow can able to get the maximum accuracy level of values for the prediction project.

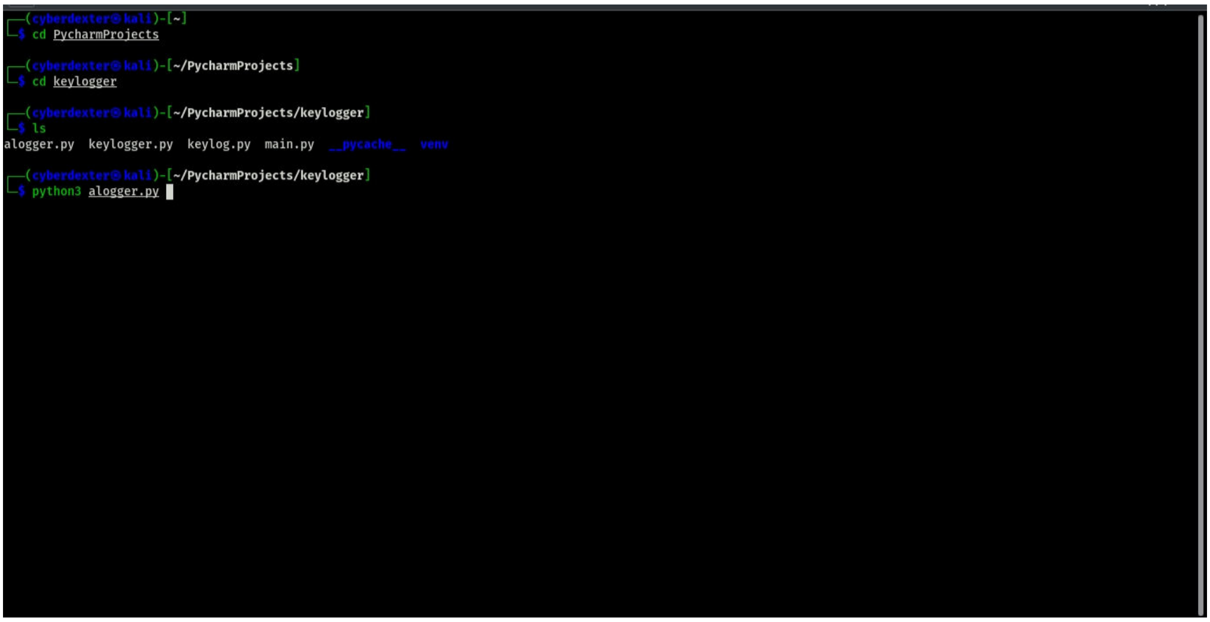
Implementation:

Algorithm Explanation:

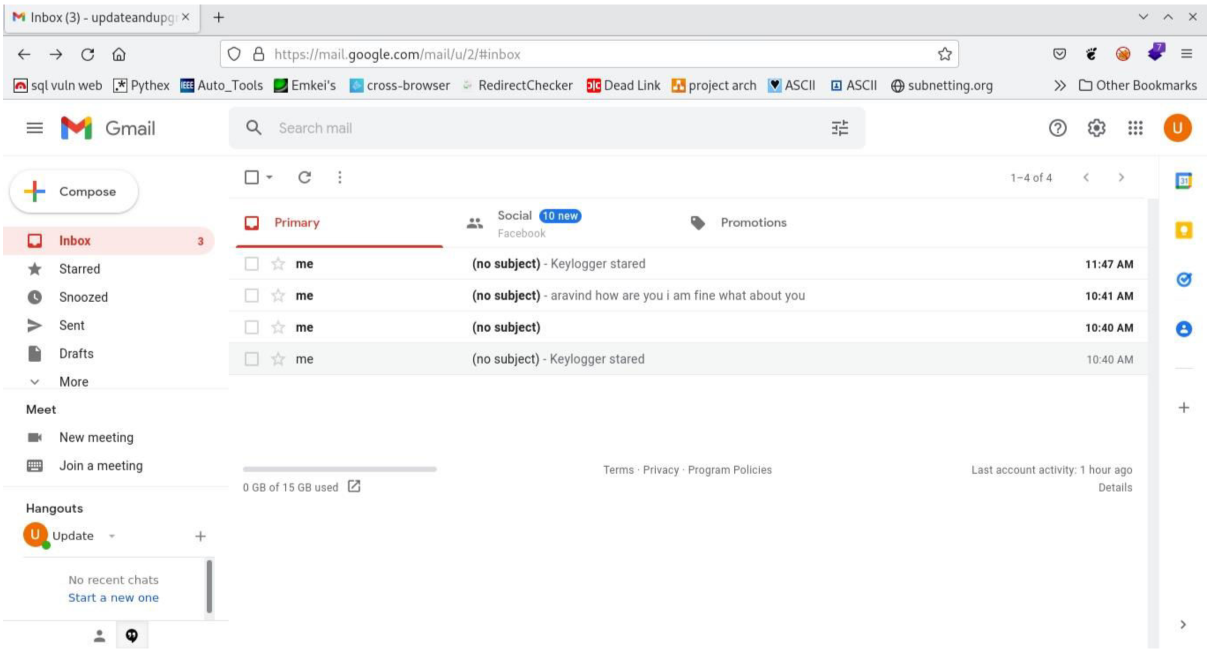
```
 import keylogger
import os
```

```
try:
    my_keylogger = keylogger.Keylogger(20, "updateandupgrade777@gmail.com",
"passwordennasollu36436")
    my_keylogger.start()
except KeyboardInterrupt:
    os.system("clear")
class Keylogger:
    def _init_(self, time, email, password):
        self.store_key = "Keylogger stared "
        self.time = time
        self.email = email
        self.password = password
    def log(self, string):
        self.store_key = self.store_key + string
    def key_press(self, key):
        try:
            current_key = str(key.char)
        except AttributeError:
            if key == key.space:
                current_key = " "
            else:
                current_key = " " + str(key) + " "
        self.log(current_key)
    def send_mail(self, email, password, message):
        server = smtplib.SMTP("smtp.gmail.com", 587)
        server.starttls()
        server.login(email, password)
        server.sendmail(email, email, message)
        server.quit()
```

Output:

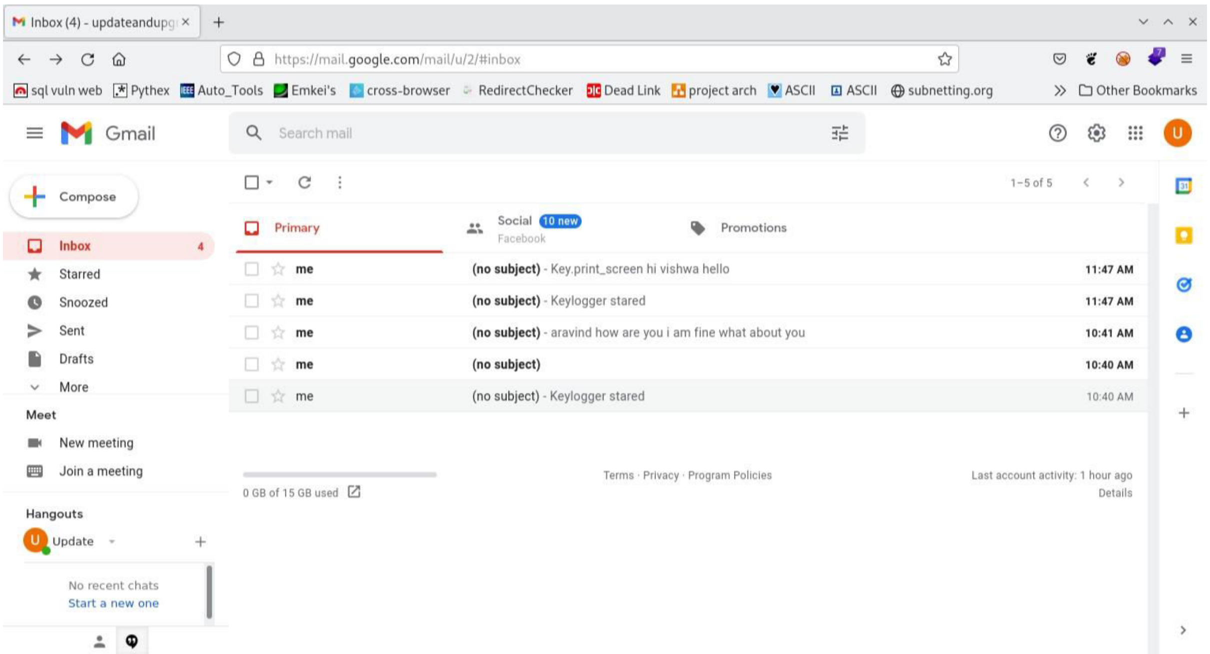


```
┌──(cyberdexter㉿kali)-[~]
└─$ cd PycharmProjects

┌──(cyberdexter㉿kali)-[~/PycharmProjects]
└─$ cd keylogger

┌──(cyberdexter㉿kali)-[~/PycharmProjects/keylogger]
└─$ ls
alogger.py  keylogger.py  keylog.py  main.py  __pycache__  venv

┌──(cyberdexter㉿kali)-[~/PycharmProjects/keylogger]
└─$ python3 alogger.py █
```



```
me   (no subject) - Keylogger stared                                 11:47 AM
me   (no subject) - aravind how are you i am fine what about you    10:41 AM
me   (no subject)                                                    10:40 AM
me   (no subject) - Keylogger stared                                 10:40 AM
```

0 GB of 15 GB used Terms · Privacy · Program Policies Last account activity: 1 hour ago
Details



me (no subject) - Key.print_screen hi vishwa hello 11:47 AM

me (no subject) - Keylogger stared 11:47 AM

me (no subject) - aravind how are you i am fine what about you 10:41 AM

me (no subject) 10:40 AM

me (no subject) - Keylogger stared 10:40 AM

Conclusion:

In some circumstances, like as monitoring a child's computer browsing behaviour, a keylogger programme is quite useful. For this reason, our study has created a novel Software-Based Keylogger Prototype that can monitor user activity without being detected for ethical reasons. The Windows API is a programming interface provided by Microsoft that allows programmers to obtain user inputs without knowing the actual hexadecimal encoding. Furthermore, this system and add capabilities to the keylogger prototype. Previous studies found that the lack of log file encryption limited the keylogger prototype that had been developed. Without log file encryption, the user of the computer is likely to be notified that his or her machine has been infected with a keylogger tool once he or she logs in. Alternatively, she may have gained access to the log files. Furthermore, the proposed keylogger proto-type can take snapshots whenever a new window or application is started, record clipboard data after the user has copied some text, and record the active window's title for a more thorough data gathering.

.

Mrs.A.Sunitha M.E., is an Assistant Professor in the Department of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai, Tamil Nadu. She has completed his M.E, CSE under Anna University Affiliation College in the year 2014. she has done his B.E, CSE under Anna University Affiliation College in the year 2012. Mrs.A.Sunitha has 07 years of teaching experience and 5 publications in International Journals and Conferences. Her area of interests includes Network Security, Computer Networks, Data Science and Machine Learning. She is an active member of CSI and IEANG. She has organized various International Conferences, workshops and Seminars in the area of Computer Networks, Cloud Computing & Machine Learning respectively.

Mr.E.Vetrivel B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering,Sriperumbudur,Chennai,TamilNadu. I had started a Ecommerce Start-up in my 3rd year College Days , Now the Start-up in the R&D Phase, Now I'm the Web Developer of the Start-up Company as Drawlead is owned by me

Mr.V.Vishwa B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering,Sriperumbudur,Chennai,TamilNadu. I had started a Ecommerce Start-up in my 3rd year College Days , Now the Start-up in the R&D Phase, Now I'm the Web Developer of the Start-up Company as Drawlead is owned by me