International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 3, May-June 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Anti-Keylogger & Keylogger Using SVM

Pratibha Prasad*, Akash Kawale**, Gayatri Bankar***, Shriya Raut****

*(Information Technology, Bachelor of Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, India, Email: pratibha.prasad_19@sakec.ac.in)

** (Information Technology, Bachelor of Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, India, Email: akash.kawale_19@sakec.ac.in)

*** (Information Technology, Bachelor of Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, India, Email: gayatri.bankar@sakec.ac.in)

**** (Information Technology, Bachelor of Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, India, Email: shriya.raut_19@sakec.ac.in)

----------**********----------

Abstract:

Today, computers are used everywhere to perform everyday tasks. Input devices i.e. keyboard or mouse used to power the computer. Monitoring input devices is just as important as monitoring user logging. A keylogger, also known as a keyboard recorder, is a software or hardware device that tracks every keystroke a user makes. Keylogger runs in the background without the user being aware of its presence. It can be used as monitoring software for parents to monitor children's computer activity and owners to monitor their employees. A keylogger (be it spyware or software) is a type of surveillance software capable of storing every keystroke in a log file. This is very dangerous for systems that use their systems for day-to-day transactions, i.e. online banking systems. A keylogger is a tool designed to record all machine-generated keystrokes, which punishes hackers for stealing sensitive information without the user's intention. Privileged also relies on access for execution and placement by the Kernel keylogger, all messages are passed from the keyboard drivers, while the programmer simply relies on kernel-level facilities to interrupt. It certainly requires great strength and expertise for a realistic and error-free implementation. However, it has been observed that 90% of keyloggers today run in userspace, so they don't need any permissions to run. Our focus is on userspace keylogger detection. Our intention is to ban user space keyloggers from stealing confidential data and information. For this purpose, we are trying to create a mobile application which helps us to detect any keylogger present in the mobile device and if so, how to identify and remove it, for with the second feature we have added extra functions to our app which is battery performance check.

----------**********----------

I.INTRODUCTION

Keylogger programs, also known as keyloggers, are malicious software that maliciously monitors user input from the keyboard to steal sensitive data. Because it is the most common user interface for computers, the keyboard is the main place where the keylogger tries to collect user input. While there are both hardware and software keyloggers, software keyloggers pose the greatest threat to users whose valuable assets are stored on their computers. Accordingly, it is the main focus of this document. However, hardware keyloggers pose a significant privacy risk to computer users. Keylogger commonly known as keystroke recording software is a type of hardware or software that can effectively intercept various user input and activity provided by the user. It coordinates user activities on the computer, including keystrokes, web page visits, access to calculator applications, instant messaging, and several other computer tasks.

 ©IJSRED:All Rights are Reserved

Software keyloggers are one of the most serious types of malwares that stealthily record keyboard activity and, in most cases, transfer recorded data to third parties. Despite numerous research and marketing efforts, keyloggers can still pose a significant threat of theft of personal and financial information. Depending on the part of the computer they are integrated into and the operating system used, all keyloggers can be classified as either hardware-based or software-based. The latter is the most common and in turn is divided into several. Compared to other types of malwares, such as viruses and worms, the purpose of keyloggers is generally not to cause harm or spread to other systems. Instead, software keyloggers monitor user Behaviour and steal personal information, such as keystrokes and browsing patterns. This information is then sent back to the third party and can at best be used as the basis for targeted advertising or marketing analysis, while in the worst case, a malicious application Hackers can steal all your personal information, bank account passwords or any other confidential information.

Currently, different types of keyloggers work without location and/or deployment approval. A common user remains unaware of keyloggers and neglects to access meaningless software and keylogger implementations that can be fooled by intruders. Compared to Kernel keylogger, it definitely needs power and expertise to execute truly and without errors. It also depends on access for implementation and sorting by kernel keyboard recorders, the whole message is passed by the keyboard driver, and the programmer only needs to rely on kernel level facilities for interrupts. Keylogger a tool designed to record all machine-generated keystrokes and give hackers the ability to obtain large amounts of sensitive information without the owner's knowledge.

The general purpose of this simple keystroke detection software is to prevent the export of sensitive information. Keyloggers differentiate themselves using a black box strategy. The discovery method depends on behavioural properties that can be associated with all keyloggers and is independent of the keylogger's core qualities. This provides ways to frame mobile phone locations based on machine learning to identify keylogger applications.

Batteries are one of the most compact and reliable sustainable energy sources. The widespread use of nickel-cadmium and Li-ion batteries in mobile phones and smartphones plays an important role. To ensure its health and avoid possible problems with the battery, it is important to check its Health Zone correctly. So, it's important to monitor your battery health, how long will it last based on the percentage remaining? does the battery heat up? et cetera The battery performance monitor makes this task easier.

A computer virus is a program that can infect other computer programs by modifying them to include a (possibly evolved) copy of itself. They are not necessarily designed to cause harm, but often they are. Viruses are transmitted from one computer to another when a user runs infected programs or when opening a document infected with a virus. Viruses are a big threat to our devices, which is why anti-virus software has become essential.

I. METHODOLOGY

A. *Anti-keylogger feature:*

One of the most dangerous kinds of malware, software keyloggers secretly record keyboard activity and, in most instances, leak the information to outside parties. Keyloggers continue to pose a serious threat of stealing financial and personal information despite extensive study and commercial efforts. All keyloggers fall into one of two categories: hardware-based or software-based, depending on the area of the computer they are inserted into and the operating system being used. The latter is the most prevalent and is further broken down into various groups. Keyloggers typically do not aim to harm or propagate to other systems, in contrast to other forms of malware like viruses and worms. Instead, software keyloggers keep track of user activity and capture personal data like keystrokes and browsing habits. In the best-case scenario, this data can be used as a foundation for targeted advertising or marketing analysis, but

 ©IJSRED:All Rights are Reserved

in the worst-case scenario, malicious software can steal all of the private information, bank account passwords, or any other confidential information. This data is then sent back to third parties.

B. Keylogger:

It has been observed that 90% of keyloggers currently exist in userspace mode. Userspace keylogger does not require any authorization or authentication from the user for deployment. When you access the file, it will automatically run and hide in your machine and put in keystrokes and you will never know that your information is gathered from a source. A complete programmer with average skills can develop a userspace keylogger. There are several reasons why the userspace keylogger is the consumer version. Userspace keyloggers are based on documented APIs that are commonly available on modern operating systems, such as Windows 7, 8, Mac OS 10 or later, and more. Users can mistakenly run the keylogger as harmless software and be tricked into running the file. As a result, the intruder will receive all the keystrokes the user has pressed and easily get their personal information and any other data. On the other hand, kernel keylogger runs in kernel mode. It requires all permissions to run the deployment from the user. Under the system, small dongles are added between the keyboard and the motherboard to record a full log of which keystrokes are pressed by the operator (required for physical access). Meanwhile, keylogger software supports hardware devices to implement keylogger. These software are installed on the target machine whose task is to detect user actions by hiding and saving all key presses (made at that time) as well as some conditional statements. by forwarding them to third parties. Recently, all new operating systems have been designed to demonstrate familiarity with unprivileged Application Program Interface (API) groups that can be used by client space projects to invade. enter all client keys. Currently, different types of keyloggers work without location and/or deployment approval. A common user remains unaware of keyloggers and neglects to access meaningless software and keylogger implementations that can be fooled by intruders. Compared to Kernel keylogger, it definitely needs power and expertise to execute truly and without errors. It also depends on access for implementation and sorting by kernel keyboard recorders, the whole message is passed by the keyboard driver, and the programmer only needs to rely on kernel level facilities for interrupts.

C. Anti-keylogger:

To detect keyloggers on the system, a method is described. A personification description created; in the computer memory and hidden in the window creates a unique and unpredictable data pattern. The user analyses the execution of an unpredictable data pattern and performs secondary analysis of the suspicious process, the suspicious process has an associated cache containing a unique and unpredictable data pattern. Kernel malware often makes continuous control-flow adjustments, e.g. installing hooks, to gain and maintain control. Malware designers have begun targeting function pointers in kernel data structures due to fear of detection, especially for software that is strongly affected by memory and heap regions. The attack surface is huge and function pointer modification is stealthy, so the attack is attractive to malware developers. More than 18,000 function pointers exist in the Windows kernel. Additionally, to prove this threat is real to license-based operating systems, we applied two possible attacks to Windows by implementing two separate function pointers. The author then proposed a new technique to actively detect hooks and develop a prototype, called Hook Scout. In recent years, basic authentication frameworks based on secret words have been reasonably proven to be insufficient for some types of genuine devices. As a result, many exams are starting to work and focus their efforts on drafting biometric verification frameworks. This model has been further accelerated with a mobile approach, offering a significant number of sensors and the ability to apply a variety of wearable biometric verification frameworks. There is also a biometric verification route, but the attacks turned out to be more sophisticated and many other biometric

 ©IJSRED:All Rights are Reserved

methods eventually proved resistant to de facto advanced attackers.

D. Battery performance feature

A smartphone is a complex system consisting of various hardware components and software applications. Hardware and software components are responsible for the smartphone's power consumption. If the hardware is efficient and the software can't provide that efficiency, power consumption will be higher, and the same goes for inefficient hardware with optimized software. Therefore, it should be noted that hardware and software components must work equally efficiently to deliver maximum performance with less power consumption in smartphones. Therefore, to understand the power consumption of smartphones, a holistic approach is needed; In particular, knowledge of the following is necessary:

- A good understanding of each component of a smartphone
- The hardware and software relationship and coordination
- Where, how, how much, and in which condition the energy is used
  - o Energy consumption of each individual hardware
  - o Energy consumption of the OS and other system software
  - o Energy consumptionof the applications
  - o Energy consumption due to usage
- The external factors responsible for power consumption

However, as mentioned, smartphones are a complex system; Analysing and estimating the exact power consumption of each of the various components is not simple. It is further complicated by the fact that besides users and manufacturers, many other external entities participate directly or indirectly in the smartphone ecosystem and play an important role in consumption. its general energy. Therefore, in this section, we have taken a general approach to discuss the causes of smartphone power consumption and possible solutions to reduce it. Fig.1 summarizes the likely sources and reasons for power consumption in smartphones and possible ways to reduce them.

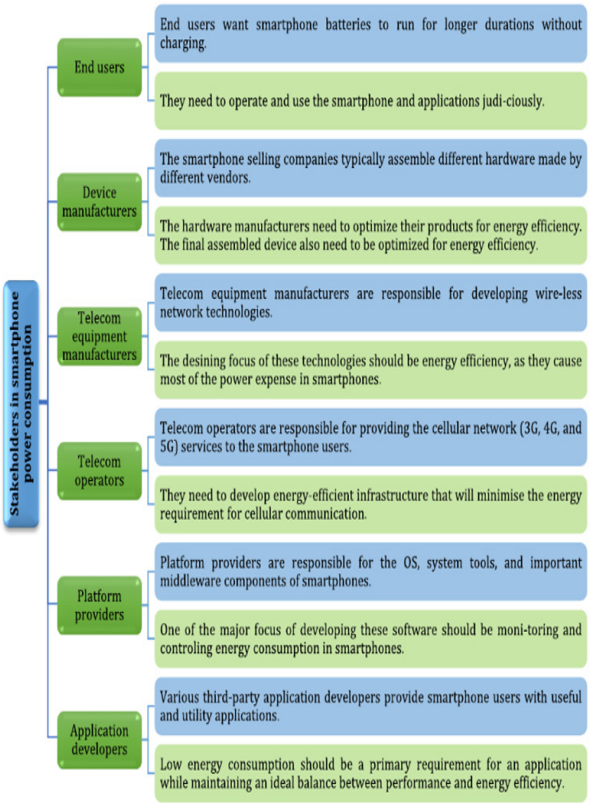

Fig.1. The probable sources and reasons for power consumption in a smartphone and probable ways to minimise

III.IMPLEMENTATION

A. Work-Flow of Project

The Order of action that takes place in the website contribute to the workflow of the website. Fig.2 Shows the flow of the entire website. It is further explained in detail.

 ©IJSRED:All Rights are Reserved

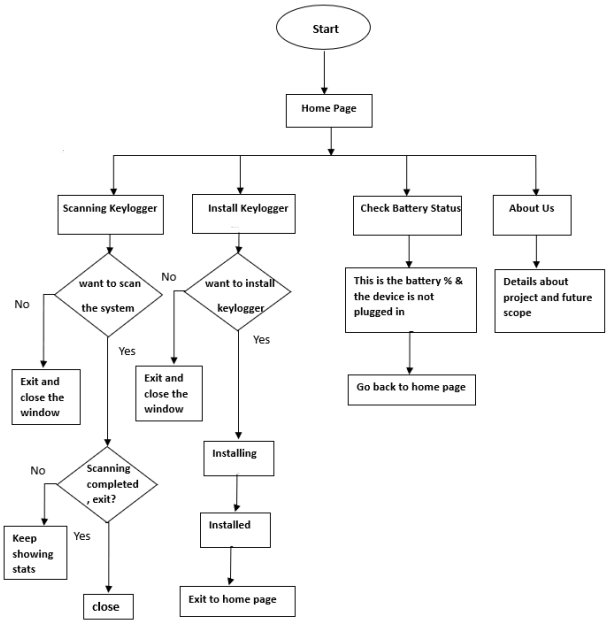

Fig.2 Flow of the project

*1) Home Page :*Start of the website begins with the home page. It displays the widgets and gives us the options to carry out the different tasks. Keylogger scanner, Install Keylogger, Check battery functions are the main features of the website.

Home page is built to give easy access to all the features of the website making it easy to navigate and operate.

*2) Keylogger Scanner:*Scanning of keylogger is a major feature of the website as it. This part operates on the basis of anti-keylogger and initiates the operation of the anti-keylogger.

Scanning is the first step of keylogger. After the scanning the stats are presented of whether any keylogger is present or not. Further action whether to kill the keylogger or not, if any present is done automatically.

*3) Keylogger Instalment:*The parental monitoring feature of the website is completely dependent on this process. The user has an option to install it or not.

With this process a website approved keylogger is embedded into the system for monitoring the actions that take place in the device. Once installed the keylogger will only be deleted when instructed to do so on the website.

This step will provide the user with files containing information on the history of the searches and tasks done by the device operator, which might be the users children.

3.1.4. Menu, about us, etc.

The menu section in the website gives us access to the different elements of the app.

Contact & Help section can help the user to put any complains about the website and clear doubts about the website.

The about us section gives the user more details of the website and its creators.

B. Working of Keylogger

The Keylogger installation mentioned earlier is used for parental monitoring. With the introduction of the internet in today's learning environment children have access to other fields and information as well, hence parental monitoring is considered important.

1) Library used

This feature uses the "pynput" library from the Python libraries to monitor the user actions. This library allows you to control and monitor input devices. Currently, mouse and keyboard input and monitoring are supported.

In our app, we have worked on the keyboard monitoring of the device. This helps in recording all the keys typed by the operator/user in a file. The file in which the keystrokes are recorded has restricted access and only the user a.k.a owner of the device can access the file.

*2) Challenges faced in the implementation of Keylogger:*The keylogger was designed in such a way that it stored strokes made on a physical keyboard only. Hence the website would not work on a smartphone, tablet, etc.

We redesigned the keylogger in such a way that it would record the strokes of a virtual keyboard. Hence now the keylogger does not care what kind of keyboard or device is used by the operator to type, and all the strokes are recorded.

 ©IJSRED:All Rights are Reserved

C. Working of Anti-Keylogger

Due to the growing networks connected to our devices, it is easy to get attacked by malicious malware and keyloggers are one of them. To protect the device from being monitored our website provides the anti-keylogger scanner and detector.

This process is done in three steps- scanning, detecting, killing

1) Scanning the keylogger:

In this step, the entire system is scanned for the presence of keyloggers. The keyloggers might be stored in any area of the device according to their convenience and such that they are not easily found. Scanning for keyloggers helps in the detection of the software keyloggers in all parts of the system so that none of them go undetected.

2) Detection of keyloggers:

The detection of keyloggers is the most important step as it tells us whether there are keyloggers present or not.

We have used the Support Vector Machine (SVM) detection technique in the detection of keyloggers. Here the SVM is a pre-trained Machine learning algorithm to detect the keyloggers present in the device. The time taken for the system to intake a command from the keyboard and the time when the key is physically typed is more in the presence of a keylogger than when it is absent. This time gap is exactly what the SVM targets.

After the scanning and detection of keylogger, the presence of it is shown to the user, and the further action to consider it as a threat or not is in the hands of the user. If the user, considers it a threat the keylogger is killed, if not the app exits the page.

The anti-keylogger is coded and designed in such a way that it does not consider the keylogger installed by the website as a threat, but another keylogger of similar features will still be considered a threat. The scanned and detection data will be deleted when the user leaves the website.

3) Killing of keylogger:

This step takes place if the user considers the detected keylogger as a threat.

In this step, the keylogger is completely eradicated so it does on take any further actions. And its connection to the malicious person is broken off completely.

4) Libraries used:

In our website, we have used the “pysimplegui” and “pyfiglet” libraries of Python.

The “pysimplegui” helps in the creative representation of the keyloggers detected during the detection phase. This makes it easier for the user to understand where the keylogger is and what it does.

The “pyfiglet” helps in the better explanation of the keylogger by highlighting the important parts using the creative fonts, so that the user only focuses on the parts that he needs to understand.

5) Challenges in the implementation of Anti-Keylogger:

The main challenge in anti-keylogger implementation was to not consider the keylogger installed by the website as a threat and kill it.

Allowing user control over the killing process of the keylogger was also a challenge as it killed the keylogger without the permission of the user.

Other challenges include proper scanning and detection of the keylogger as the software scanned some of the important docs and codes and considered them as threats.

D. Working of Battery performance feature

While checking the battery performance of a device it is necessary to understand the reasons for it before the means to improve the battery performance.

Our battery performance will keep the battery in check and if any issues are there in the device, it will notify the user of the cause of the issue and guide them thoroughly to eliminate it or seek professional help in case of major problems.

1) Library used:

We have used the psutil python library for the implementation of the Battery performance feature.

The “psutil” library is used to access system details and process utilities. It is used to keep track of various resource utilization in the system. Usage of resources like CPU, memory, disks, network, and sensors can be monitored using “psutil”.

2) Challenges in the implementation of Battery performance feature:

 ©IJSRED:All Rights are Reserved

The proper scanning of the battery which is essentially a hardware came as a challenge. The usage and consumption of the battery could be recorded but battery health is difficult to record as it may contain hardware requirements.

We stopped our focus on the battery performance, at its usage and small details like the percentage of battery and whether the device is charging or not. Additional features could be added in future.

IV.CONCLUSIONS

Keyloggers are powerful tools that cannot threaten the system itself but the user's confidential data such as usernames, passwords, PINs and bank cards. Although some keyloggers are legally applied, many keyloggers are used illegally by their creators. In This research working of a keylogger, the methods used to conceal while subverting the user's machine, the process to detect the keylogger and the process to kill if present any is been focused. And also looks at the current state of keyloggers and how they can spread. Finally, after analysing the existing detection techniques and highlighting some prevention techniques. Detecting keylogging technology in an organization is no different from controlling malware or other threats, requiring common sense, constant monitoring, and layered defence. The key point is to be aware of existing threats, recognize how they are used, and the appropriate ways to detect them. Therefore, keylogger detection and countermeasures should be part of an organization's incident response plan.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[1] [1] M. Wazid et al., "A framework for detection and prevention of novel keylogger spyware attacks," 2013 7th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2013, pp. 433-438, doi: 10.1109/ISCO.2013.6481194.

[2] [2] Wajahat, A., Imran, A., Latif, J., Nazir, A., & Bilal, A. (2019). A Novel Approach of Unprivileged Keylogger Detection. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). doi:10.1109/icomet.2019.8673404

[3] [3] R. U. Corporation. Passfaces. http://www.realuser.com Last accessed: September 1, 2016.

[4] [4] Shaikh Saubiya Ahmed S. and Narendra M. Shekokar, "Cued Click Authentication", 2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN), IEEE, 2017.

[5] [5] Somya Shrivastava, Bhupendra Panchal, "A Novel Method for Securing Password Transparency from Keylogger Recorder", International Journal of Emerging Technology and Advanced Engineering, Volume 8, Issue 5, May 2018.

[6] [6] S. Gunalakshmii1& P. Ezlunnalai2 "Mobile Key logger Detection Using Machine Learning Technique", International Conference on Computer Communication and Systems, Chennai, India, IEEE, 2014.

[7] [7] M Hossein Ahmadzadegan, Ali-Asghar Khorshidvand, Meherdad Pezeshki, "A Method for Securing Username and Password against the Key Logger Software using the Logistic Map Chaos Method", 2nd International Conference on Knowledge based Engineering and Innovation(KBEI), IEEE, 2015.

[8] [8] Junsung Cho, Geumhwan Cho and Hyoungshick Kim, "Keyboard or Key logger: a security analysis of third-party keyboards on Android", Thirteenth Annual Conference on Privacy, Security and Trust (PST),IEEE, 2015.Xiyang Liu, Jinhua Qiu, Licheng Ma, Haichang Gao, and Zhongjie Ren, "A Novel Cued-recall Graphical Password Scheme", Sixth International Conference on Image and Graphics, 978-0-7695-4541- 7/11, 2011 IEEE DOI 10.1109/ICIG.2011.16

[9] [9] A.Solairaj1, S.C.Prabanand2 , J.Mathalairaj3, C.Prathap4 And L.S.Vignesh5, "Key Loggers Software Detection Techniques" , Intelligent Systems and Control (ISCO), IEEE, 2016.

[10] [10] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and Paul C. van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE Transactions On Dependable And Secure Computing, VOL. 9, NO. 2, March/April 2012

[11] [11]L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," ACM Trans. On Information and System Security, vol. 13, no. 1, pp. 1–26, 2009.

 ©IJSRED:All Rights are Reserved