Keyloggers: A Threat to Privacy

Suchit Reddi
Electronics and Communication Engineering
Shiv Nadar University
Tehsil Dadri, India
rs521@snu.edu.in

ABSTRACT

Keyloggers are a spyware which collects sensitive keystroke information from the device on which they were installed. There are many ethical uses along with malicious uses for keyloggers. The primary paper is about what a keylogger is and different types of them. It also shows some basic security measures against keyloggers and the damage that can be done if the user is careless. The base paper goes deep into the details of working of some famous types of keyloggers.

The basic methods of identification and elimination are discussed in the base paper. The next supporting papers show us even more sophisticated methods of preventing malicious usage of keyloggers on the user. There is a paper which goes even more into this topic from keyloggers to touchloggers.

The final output of these papers is to make the user able to protect himself from the threat of keyloggers and utilize them to improve their productivity.

Keywords: Keyloggers, Keystrokes, Keyboard State Table Method, Windows Keyboard Hook Method, Kernel-Based Keyboard Filter Driver Method, Driver Signing, Integrity Protection Driver (IPD), Jailbreak, Rooting, Personal Identification Number (PIN), Screen Lock Password (SLP).

I. INTRODUCTION

Keyloggers are gaining popularity as they are being used largely for data theft in the recent years. It is wrong to assume that keyloggers are evil just by the fact that they are being used as an unethical means to an end. There are many good uses for keyloggers that it has the potential to change our lives for good. But users should be able to protect themselves from the malicious usage of keyloggers against them before being able to use keyloggers for their benefit.

Hackers try to obtain sensitive information in any way possible by analyzing known vulnerabilities and exploiting them. They prefer to automate the process of extracting data, to happen even in their absence. Keyloggers provide exactly what they need to extract very crucial information and stay anonymous and undetected. Keyloggers relieves hackers from using traditional reconnaissance techniques like brute force, dictionary attacks etc by collecting the information needed to gain access into their target's accounts.

Keyloggers can be installed through many ways. Physical presence is a must in the case of physical or hardware keyloggers; but in the case of software keyloggers, installing it on the targeted device is easily done by sending it through phishing emails and links, and many other ways. But as hardware keyloggers don't use system resources, they are much harder to detect.

The base paper has so much numerical information collected from different sources about the effects of keyloggers in real world for corporate espionage, spying etc.

Keyloggers are different from other kinds of spyware and malware. They use system resources from legitimate programs and reside on the system invisibly and carry out their tasks without attracting attention towards themselves. These days, they are being used for more advanced purposes than just collecting keystrokes.

II. OBJECTIVE

The main objective for this research is:

- Different types of keyloggers
- Detection of keyloggers
- Uses and misuses of keyloggers
- Methods to counter keyloggers

III. BASE PAPER CONTRIBUTION

Base paper introduces us to what a keylogger is and what a keylogger is used for, what their capabilities are, whether they can be detected or not, and how to protect ourselves from the threat of keyloggers.

Types of Keyloggers

There are two main types of keyloggers: Hardware and Software. Hardware keyloggers are small electronic devices attached to the keyboard cable or inside the keyboard itself. Physical installation in the target's keyboard is required for these keyloggers. They are cheap and can't be detected by antivirus because they don't use system resources or store data on hard disk. Software keyloggers are installed easily compared to hardware keyloggers. They collect keystroke information by tracking system processes which collect the same within the operating system. They store collected data in their own local or remote storage and sends them to the attacker through mail or cloud.

Functions of Keyloggers

Modern keyloggers have even more functions than just collecting keystrokes. More sophisticated keyloggers can perform advanced operations like:

- keystrokes typed and clipboard content
- mouse clicks and movements
- periodic screenshots
- usage statics
- file system operations like create, rename, and delete
- page visits and duration per page visit

- modifications in system registry
- windows session times and login details
- sound recording and video recording
- MAC and IP addresses and many more.

Methods used for making keyloggers

The base paper talks about various methods of keylogging like Keyboard State Table Method, Windows Keyboard Hook Method, Kernel-Based Keyboard Filter Driver Method.

In Keyboard State Table Method, GetKeyboardState API attaches its thread to the top-level thread message loop using AttachThreadInput API.

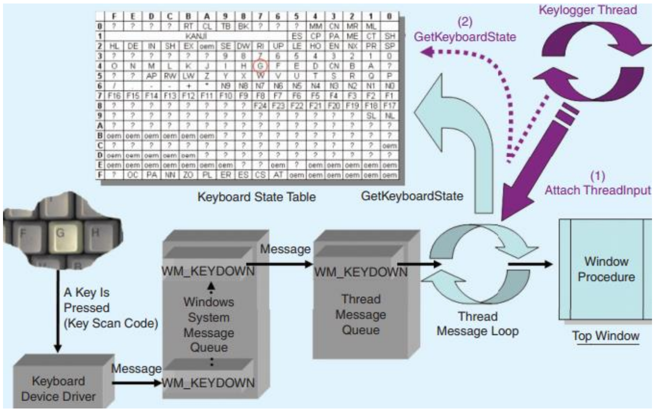


Fig1. Keyboard State Table Method

In Windows Keyboard Hook Method, the keylogger hooks itself to the message loop and by doing so, it can read, modify, and interrupt messages flowing through the hook procedure.

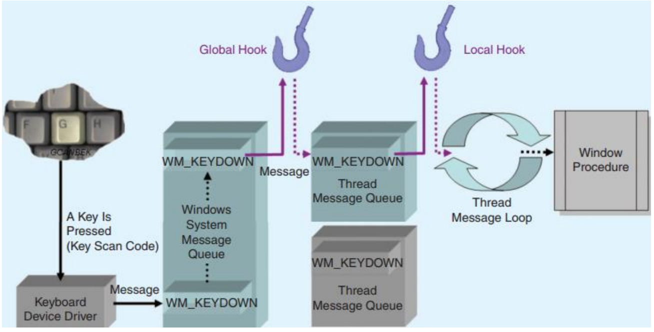


Fig2. Keyboard Hook Method

In Kernel-Based Keyboard Filter Driver Method, the keylogger resides at the kernel level and is nearly invisible. They are difficult to install, implement, and detect. It installs itself before the system's keyboard driver once administrator privileges are obtained and captures keystrokes even before the system does.

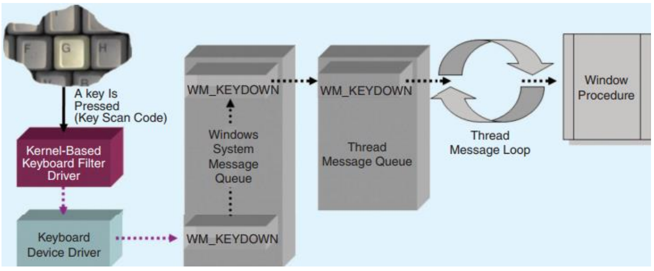


Fig3. Keyboard Filter Driver Method

Uses/Misuses of Keyloggers

Keyloggers are utilized in many fields by military, hackers, computer security experts, employers, parents, normal users etc. They are used for both ethical and unethical purposes. They are used for gathering sensitive information, identity theft which are unethical and illegal. They are also used for intrusion detection, computer forensics, surveillance, and disaster recovery which are ethical and legal. There are also controversial uses like parental monitoring by parents, workplace monitoring by employers which might be unethical but aren't considered illegal.

Going into details, keyloggers are used by hackers to swipe credit card information, and login details; they can also be used for corporate espionage by revealing trade secrets, costumer records, and business contacts. Hackers steal personal information like bank account information, online banking passwords, and identity information which can result in identity theft. Keyloggers keep logs of information which can be used in the case of intrusion, by law enforcement or cybersecurity operatives for computer forensics. A user can use keyloggers as a method to make backups of what is being done on the system. It allows the owner to recover information like forgotten passwords, lost information during unexpected shutdowns, detect intrusions and see what the intruder did.

Some controversial uses are parental & workplace monitoring. According to CERT-CC, in a workplace legitimate keystroke monitoring systems must show banners advising users that logging in and using their system includes giving consent to be monitored. Decisions about using keyloggers must be made only after analysing possible positive and negative effects. Some parents justify monitoring their children saying that there are risks in online environments like bullying, inappropriate content, financial scams targeting children etc. But continuous surveillance negatively impacts children by making them feel like they lost their freedom.

Counter measure to protect ourselves from keyloggers

Users should be able to detect the presence of keyloggers on their devices. Some common indicators for the same are: -

- Alerts from antivirus software
- Keys and mouse clicks do not work properly
- Delay in appearance of pressed key on screen
- Double clicks and drag-drop operations behave suspiciously.

When keyloggers are detected on the device, some basic procedures to protect our sensitive information are: -

- Install a good antivirus which has an anti keylogger.
- Use two factor authentication and strong passwords.
- Keep security patches updated and download programs only from trusted websites.
- Check for hardware keyloggers before using other's devices.
- BlueGem Security introduce in Computer News Briefs, October 2005; uses LocalSSL encryption to prevent hackers from using keyloggers to intercept and view user keystrokes. LocalSSL protects transmissions with a 128-key encryption by bypassing OS.

- Baig and Muhammad introduced a virtual keyboard application which could bypass system message queue and post the keyboard messages directly to a specific application message queue using an application-level hook. After receiving these keyboard messages, the application performs the appropriate actions as if it received the message through system message queue. As system-level message queue is bypassed through this, no knows software keylogger will be able to capture the strokes.
- Anti-keylogger software uses Application Programming Interface (API) monitoring techniques like proxy DLL and Import Address Table (IAT) patching. These methods can detect keyloggers which use Windows Hook and Keyboard State Table Methods. Driver Signing and Integrity Protection Driver (IPD) can detect Kernel-Based Keyboard Filter Driver keyloggers.

IV. RESULTS & FINDINGS

The potential of keyloggers to do good and bad equally is explained in this paper by the authors. The different types of keyloggers out there and how to detect them, and then protect ourselves from them is also discussed in the base paper. The vast range of functions of keyloggers is also researched by the authors. This paper gives a detailed working process of many types of keyloggers, which can't be found in many papers regarding this topic. It also says that even though keyloggers have many ethical uses, they are mostly used for illegal purposes by hackers.

V. QUESTIONS AND LACKING POINTS

1) This paper didn't discuss guaranteed methods for preventing data theft through keyloggers.

Answered by Paper [1]

2) This paper doesn't conduct practical testing on keyloggers.

Answered by Papers [2] [4] [5]

3) This paper doesn't discuss about touchloggers which are more deadlier, if not the same than keyloggers.

Answered by Papers [4] [5]

4) The base paper doesn't reveal how researchers collect keystroke data to analyse for research purposes.

Answered by Paper [4]

VI. FUTURE WORK

The authors of the basepaper have no intention of extending their paper on the same topic further for future work, as they most likely covered everything they know about the topic in the base paper.

VII. IMPACT OF SUPPORTING PAPERS

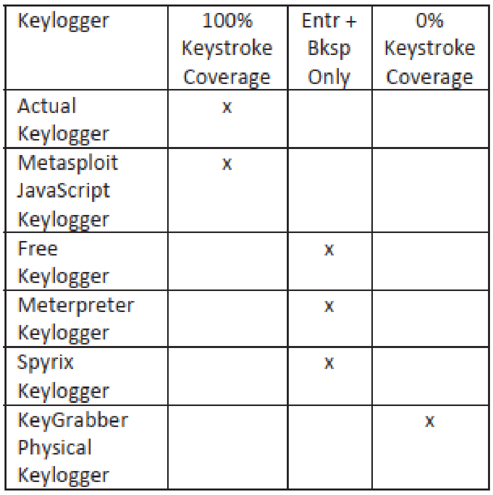
Supporting papers are selected such that they answer the questions arising from the base paper and fill in the lacking parts in the base paper.

Paper [1] has discussed some very good safety measures against keyloggers. Installing an antivirus which can detect keyloggers, Driver Signing, IPD are the main safety measure mentioned in the base paper, which is very much lacking in many ways. In paper [1], we can find many good methods. By feeding false keystroke information to system while safely delivering original keystrokes to the applications, we can bypass any keyloggers. Specific anti-screen capture techniques ensure that attempts to capture screen will result in a black screen display rather than the original screen. Containerization and using a secure, locked-down secure browser is another method to prevent any chances of infecting our device from malicious software. Combining all these by using a secure locked-down browser within a container and adding kernel-level keylogging protection with anti-screen capture measures will provide a very secure environment on any device.

Paper [2] has conducted practical testing of three keyloggers; Phrozen Keylogger Lite, Actual Keylogger, and Refog Free Keylogger by using SpyShelter and Malwarebytes. It explained what happens at the innermost procedure in keyloggers. Keyloggers have open circuits under each key. When a key is pressed, the circuit closes and makes a connection. The key's circuit location is mapped to a table in the keyboard ROM to identify which key is typed. This paper also pointed out that keyloggers have ground-breaking uses in security field. They can be used to identify typing pattern of the device owner and lock it when it finds the present typing pattern different. It can be used in incident response and forensics. Click tracking software is used alongside keyloggers by hackers. Even Google, Bing and Yahoo track user clicks automatically for marketing purposes which is unethical.

Paper [3] discusses about a transition in usage of touchloggers from keyloggers in the recent times. As times changed, everyone has a smartphone, and it became a very promising source of personal information for hackers. So, touchloggers are being used more and more each day. But, to collect information, touchloggers must gain root access to override internal OS methods which detect and manage touch events. It must be running constantly in the background to collect user's touch data. To do so, an android device should be rooted and an IOS device should be to jailbreak. This paper has detailed information on how to use touchloggers for user profiling based on touch patterns. It also consists of the ways how touchloggers can turn into malware. Some of the ways to overcome touchloggers is using custom made software keyboards that change the order of keys on the virtual keyboard which are mostly used in banking sites. This sophisticated software can be used either benignly or maliciously. The significance of the current study lies in the assessment of the potential of such software under two different views, by performing case studies.

Paper [4] goes more deeper into what keyloggers can do on a computer or laptop that also has touchscreen. This also discusses how researchers collect data from dropzones for research purposes. The attacker first infects the victim with keylogging malware. The malware then secretly logs critical information and sends the data to a dropzone which the hacker set prior to the infection. This data will be harvested from there by the hacker. Researchers use honeypots and spam traps to analyse and extract the location of the dropzone. They then access them and harvest the keylogger data just like the hackers. The authors performed tests on five keyloggers about working of keyloggers in touchscreen laptops in their paper whose results can be seen in figure 4.



Keylogger	100% Keystroke Coverage	Entr + Bksp Only	0% Keystroke Coverage
Actual Keylogger	x		
Metasploit JavaScript Keylogger	x		
Free Keylogger		x	
Meterpreter Keylogger		x	
Spyrix Keylogger		x	
KeyGrabber Physical Keylogger			x

Fig4. Percentage of Keystrokes captured

Paper [5] is completely based on practical experimenting of third-party keyboards available for free on the google play store and finding whether they can be made as keyloggers. The authors specifically pointed out that the keyboards asking for “internet” permission can be easily used as keyloggers, and it is the only permission needed for a keyboard to be used as a keylogger. The authors made a keylogger application for research purpose and submitted it to the review process of google play store, which surprisingly didn’t find anything malicious in their application and accepted it. Also, this is the first paper where I observed that the keylogger has the capability to collect only specific keystroke data like passwords etc. They tested 139 keyboard applications on 100 popular websites. 86 of 139 apps requested for the internet permission, which can be misused for keylogging. By analysing network traffic generated by them using Wireshark, the authors were able to find out that only 11 of them were generating network traffic while signing into Gmail, but that traffic was not having any password information. However, those 86 apps with internet permission can always be transformed into keyloggers. Out of 100 websites tested, login data was successfully captured from 81 sites, which was a concerning matter. Some ways are suggested by the authors to make sure that we are not using a keyboard which is a keylogger. Preventing data leakage by information flow tracking, where the user will be warned when a keyboard application delivers sensitive information to unknow servers. Enforcement of trustworthy keyboards by the websites themselves so that the users will be safe from data theft is a highly recommendable technique.

VIII.CONCLUSION

This paper is a collection of information from various research papers on the topic of keyloggers and touchloggers. The different types of keyloggers, various methods to make keyloggers, their effect in the outside world, how they can be used for both benign and malicious purposes, their functions, and capabilities, how they can be detected, different counter measures against them, practical experimentation on various keyloggers and keyboard applications, how researchers collect keystroke data etc are some of the important points discussed in this paper. People should be made aware of the impact keyloggers or touchloggers have on their personal lives if they are treated lightly. They can cause financial losses, private data leaks for both individuals and large corporate companies if used against them by hackers.

IX. REFERENCES

Format

[Number] Paper – Authors – Contact Info – Paper Link

[Base Paper]

Keyloggers: Increasing Threats to Computer Security and Privacy – Seref Sagiroglu, Gurol Canbek – Department of Computer Engineering, Faculty of Engineering and Architecture, Gazi University, Maltepe 06570, Ankara, Turkey;Email:ss@gazi.edu.tr– https://ieeexplore.ieee.org/document/5246998/

[1] How Keyloggers Work and How to Defeat Them – Dave Waterson, CEO at SentryBay and an expert in endpoint and application security- https://ieeexplore.ieee.org/document/9434212 This paper was not available on IEEExplore as pdf, the pdf is available at https://academic.oup.com/itnow/article/63/1/40/6139177?login=true

[2] KeyStroke Logs: Are Strong Passwords Enough? – Darshanie Sukhram, Thaier Hayajneh – Fordham Centre for Cybersecurity, Fordham University ,New York, United States Of America– https://ieeexplore.ieee.org/document/8249051

[3] From Keyloggers to Touchloggers: Take The Rough With The Smooth – Dimitrios Damopoulos, Georgios Kambourakis, Stefanos Gritzalis – University of Aegean, Greece – https://www.sciencedirect.com/science/article/pii/S0167404812001654

[4] Touch Interface And Keylogging Malware – Samuel Moses, Jon Mercado, Allie Larson, Dale Rowe – Brigham Young University, Cybersecurity Research Lab, Provo, Utah – https://ieeexplore.ieee.org/document/7381520

[5] Keyboard Or Keylogger? A Security Analysis Of Third-Party Keyboards On Android – Jungsung Cho, Geumhwan Cho, Hyoungshick Kim – Department of Computer Science and Engineering, Sungkyunkwan University, Republic of Korea – https://ieeexplore.ieee.org/document/7232970

Images –

Fig1,2,3 – From Base Paper https://ieeexplore.ieee.org/document/5246998/

Fig4 – From Paper [4] https://ieeexplore.ieee.org/document/7381520