International Journal of Engineering & Technology, 7 (2.28) (2017) 193-196

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Encrypted Log File Keylogger System for Parental Control

L.S. Li[1*], Z.M. Fauzee[2], N.Zamin[3], N.Kamarudin[4], N.A.Sabri[5], N.S.Nik Ab Aziz[6]

[1,2,3]University Malaysia of Computer Science and Engineering, Putrajaya, Malaysia.
[4]Universiti Pertahanan Nasional Malaysia, Kuala Lumpur, Malaysia
[5]Asia Pacific University, Kuala Lumpur, Malaysia
[6]Universiti Putra Malaysia, Serdang, Malaysia
**Corresponding author E-mail: limshengli@outlook.com*

Abstract

Keystroke logging, often referred to as keylogger, keylogging or keyboard capturing, is the process of recording all the pressed keys on a keyboard autonomously so that the person who is using the keyboard is unaware that their actions on the computer are being monitored. In the world of cyber-crime, keylogger tool has been used mostly for malicious purposes such as stealing personal information and credit card details. However, for ethical purposes, keylogger can be useful in terms of monitoring user's activities without being noticed. For instance, parents can use keylogger to monitor their child's activity on the web. The log file is used to store the recorded keystrokes. However, current log files in keylogger are not encrypted, which can be easily hacked for malicious purposes. This paper proposes a new software based keylogger with log file encryption to increase the keylogging security towards Industrial Revolution 4.0.

Keywords: *Keylogger; Keylogging; Keystroke Logging; Encryption; Cyber-Crime.*

1. Introduction

1.1. Keylogger

Keylogger, also known as keystroke logging, as the name suggests, it is a tool that can logs or records every single key that are activated or pressed by a user on a keyboard. Keylogger system also capable of capturing user information without relying solely on the keyboard key presses but also can be programmed to capture clipboard logging, active windows session, mouse action or screen logging [1]. Keylogger tools come in both hardware and software with their own advantages and disadvantages. Keylogger has been around for more than four decades since 1970s. 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].

1.2. Software-based keylogger API-based Keylogger

There are several categories of software-based keyloggers as described in **Table 1**. Almost all keyloggers have a major issue which they do not have encryption on the log files. Without encryption, the user might be alarm that his or her system being monitored, once the log files are discovered unintentionally. Hence, to prevent such situation from occurring, the prototype keylogger will encrypt all the log files being created before notification is sent to the owner of the keylogger software.

Table 1: Types of software-based keyloggers

Keylogger	Description	Example of case studies
Hypervisor-based	Keylogger that resides or infects the hypervisor to log all keystrokes sent to any virtual machines.	Blue Pill proof-of-concept developed by Joanna Rutkowska [4].
Kernel-based	Rootkit that intercepts key press or keystrokes that pass through the Operating System Kernel.	Refer to reference [5] for an example tool for kernel-based keylogger.
API-based	Keylogger that hook keyboard APIs inside an executed application to receive events every time the user pressed on a key so that the keylogger can records it.	Windows APIs such as GetAsyncKeyState() function is used to determine whether a key is up or down at the time [6].
Form grabbing based	Keylogger that records web form data before submitting it to the web server. It will record all the information on the web form once the user clicked on the submit button.	'Tiny Banker' malware [7].
JavaScript-based	Malicious JavaScript keylogger will be injected into a targeted webpage to listen for and record keyboard events.	Stealing credit card through web-based keylogger [8]. Zeus and SpyEye trojan [9].
Memory Injection based	Keylogger that perform logging function by modifying the memory tables linked with the browser and other system functions.	Zeus and SpyEye trojan [9].

One of the common type of software-based keylogger is the API-based keylogger, which relies on the OS's API that handle user's key inputs. OS's API has been used by all applications that will retrieve user keystrokes such as video games, word processing software, and many more. It can provide all the keystrokes for an application just by calling the API's own functions. A keylogger

can as well be coded to rely on this method to capture keystrokes. Thus, this project will focus on developing prototype API-based keylogger.

2. Proposed framework

The framework of the prototype API-based keylogger with data encryption is shown in **Figure 1**.

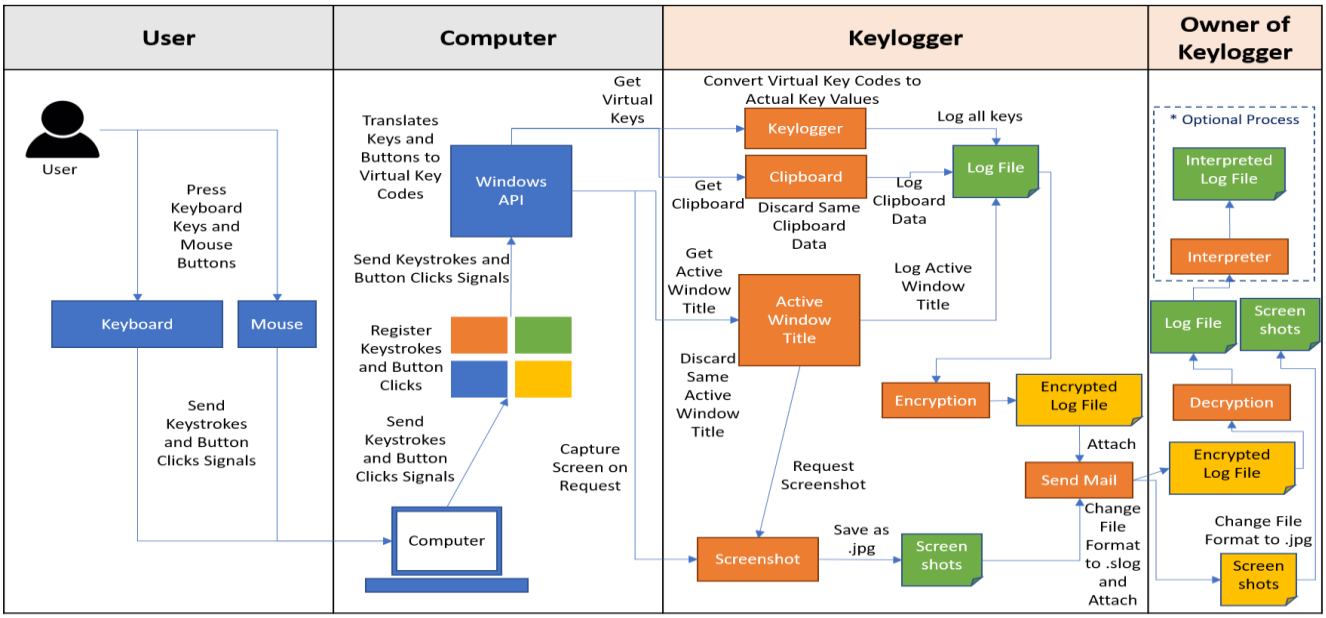
Fig. 1: API-based keylogger with data encryption framework

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. 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 taken by the key logger to provide better picture on how the application 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 decryption tool to view the log file and screenshots. Optionally, the owner can also use the interpreter tool to further translate all keyboard key values recorded in the log file to a more readable log file.

3. Result and Discussion

There are five (5) main modules which have been identified to be integrated into prototype API-based keylogger as shown in **Figure 2**. There are Clipboard Logging module, Screen Capture module, Active Window Title Logging module, Keystroke Logging module and Encryption module.



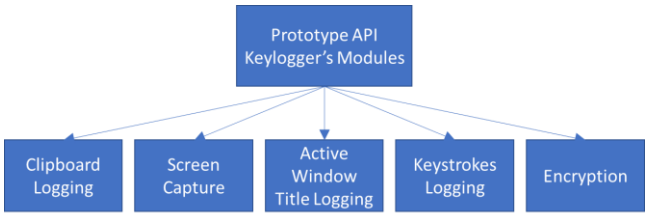


Fig. 2: Modules for the prototype keylogger

3.1. 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 copied 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. **Figure 3** shows the log file created by the module after the execution of the module.

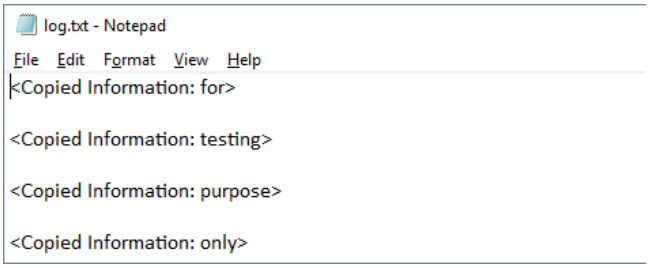


Fig. 3: Log file result after copied four (4) separate strings

3.2. Screen capture module

This is the module that will capture the window screen based on the interval time set by the system's admin. The screen capture module is embedded in the screenshot.h header file of a C++ source file. To view the image file, the user need to rename the output image file extension from .slog to .jpg and open it with any photo viewer or photo editing software to view the captured screen as shown in **Figure 4**.

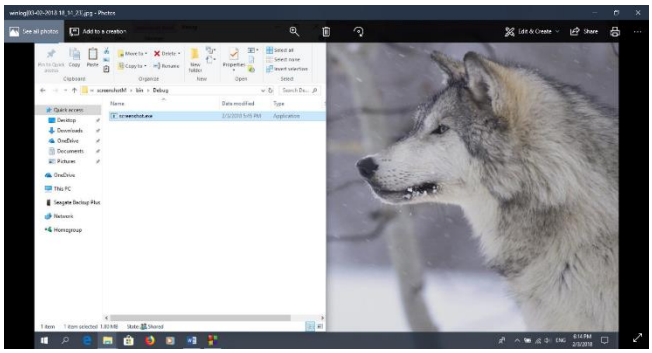


Fig. 4: Sample screen capture output image

3.3. Active window title logging module

This module captured the title of currently focused window in the current window manager. Active window title logging module will help in identifying any activities involves with other modules. The *activeWindow.h* header file is a module of active window title logging which will be included into a log file. Figure 5 shown the result of active window title logging captured by the prototype keylogger in a log file.

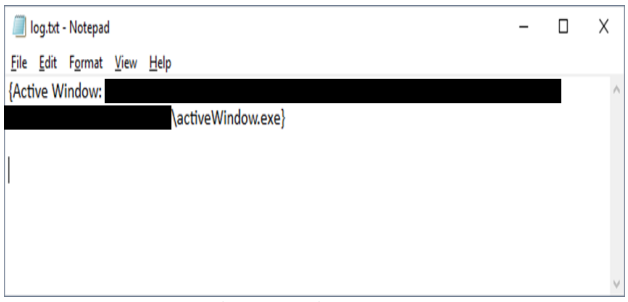


Fig. 5: Log file result after executing the module

3.4. Keystrokes logging module

Keystroke logging is the main module of prototype keylogger. This module will record all keystrokes on a standard keyboard and it also will record the mouse clicks activities on the target computer as can be shown in Figure 6. To enable this module, it requires the inclusion of keyboardHook.h header into C++ source file.

Fig. 6: Sample output for keystrokes logging module

3.5. Encryption module

This is the key module of this prototype keylogger tool. The encryption module is used to ensure that the keystroke's log file will be encrypted before been send to the system admin. One of the main purposes of this module is to make sure that the target computer will not be able to read the log file. A custom encryption module is developed for the prototype keylogger. This module relies on the Base 64 encoding method to encrypt the message to be stored in a keystrokes log file as shown in **Figure 7**. To enable this module, fstream header and Base64.h header need to be included in a C++ source file.

Fig. 7: Sample log file encrypted using encryptB64 module

4. Conclusion

Keylogger tool is extremely useful in certain cases such as monitoring child's browsing activities on a computer. For this particular reason, this research has developed a newly Software-Based Keylogger Prototype to monitor user's activities without being noticed for ethical purposes. Microsoft Windows Operating System provides an API known as Windows API for programmer to develop their program to retrieve user keystrokes without prior information on the exact keystroke hexadecimal code. Moreover, this program can also be a platform to utilize the Windows API to record keystrokes into a log file. Studies on existing open source keyloggers have been performed to allow improvements for the system and to add on some functionality to the keylogger prototype. In previous researches, the lack of log file encryption gave some limitations on the keylogger prototype that have been developed. Without log file encryption, there's a high chance that the user of the computer will be alerted that his or her computer is infected with a keylogger tool once he or she has managed to get access to the log files. Furthermore, the proposed keylogger prototype will not only capture the keystrokes, but can also screenshots whenever there's a new window or application being opened, record the clipboard data once the user has copied some text, and record the active window's title to have a more comprehensive data collection.

References

[1] S. Sagiroglu and G. Canbek, "Keyloggers: Increasing threats to computer security and privacy," IEEE Technol. Soc. Mag., vol. 28, no. 3, pp. 10–17, 2009.
[2] R. Creutzburg, "The strange world of keyloggers - an overview, Part I," Electron. Imaging, vol. 2017, no. 6, pp. 139–148, 2017.
[3] QCC Global, "'Soviet Spies Bugged World's First Electronic Typewriters,'" 2018. [Online]. Available:

https://www.qccglobal.com/soviet-spies-bugged-worlds-first-electronic-typewriters/. [Accessed: 14-Feb-2018].

[4] Joanna Rutkowska and Alexander Tereshkin, "bluepillproject.org." [Online]. Available: https://web.archive.org/web/20080418123748/http://www.bluepillproject.org/. [Accessed: 15-Feb-2018].

[5] "GitHub — fbocolowski/logger: A kernel-based keylogger for Windows." [Online]. Available: https://github.com/fbocolowski/logger. [Accessed: 15-Feb-2018].

[6] "GetAsyncKeyState function (Windows)." [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/ms646293(v=vs.85).aspx. [Accessed: 15-Feb-2018].

[7] D. Virgillito, "'Tiny Banker' Malware Attempted At Customers Of US Banks | Massive Alliance," 2014. [Online]. Available: https://www.massivealliance.com/2014/09/19/tiny-banker-malware-attempted-customers-us-banks/. [Accessed: 15-Feb-2018].

[8] T. Spring, "Web-Based Keylogger Used to Steal Credit Card Data from Popular Sites | Threatpost | The first stop for security news," 2016. [Online]. Available: https://threatpost.com/web-based-keylogger-used-to-steal-credit-card-data-from-popular-sites/121141/. [Accessed: 15-Feb-2018].

[9] Wladimir Palant, "SpyEye Targets Opera, Google Chrome Users — Krebs on Security," 2011. [Online]. Available: https://krebsonsecurity.com/2011/04/spyeye-targets-opera-google-chrome-users/. [Accessed: 15-Feb-2018].

[10] C. A. Rusen, "Simple Questions: What is the Clipboard in Windows & How to Manage It? | Digital Citizen," 2013. [Online]. Available: https://www.digitalcitizen.life/simple-questions-what-clipboard-windows-how-manage-it. [Accessed: 15-Feb-2018].