**UNIVERSITY OF PLYMOUTH & HKU SPACE**

**BSc (Hons) Computer and Information Security**

**PRCO304HK Computing Project**

**Develop an Anti-Keylogger Program (AKP) for Detection and Deletion of Keyloggers in Computer System**

**Student ID: 10072329**

Supervisor:

Second Marker:

# Acknowledgements

I would like to thank my project supervisor, Beta Yip, for his continued support throughout this project, as without his input, feedback and project guidance I would most certainly unable to complete this computing project within the period of time.

I’d also like to thank the developers at \_\_\_ ,\_\_\_\_, \_\_\_\_\_\_\_and \_\_\_\_\_\_ for developing the tools and platforms that consequently allowing me to develop the anti-keylogger program.

Finally, I’d like to extend my gratitude to my family, especially my wife, who have extensively supported me throughout this period and have kept me motivated to continue pushing forward in future.

# Abstract

This report describes the development of a program to detect and delete the Keyloggers within the computer system. IT security professionals would undertake when a cyber-security incident occurs in the aspect of Keyloggers as well as provide additional security for organizations through specific monitoring and response.

The report begins with introduction into the current state of cyber security issue related to Keyloggers and then progresses onto the aims, goals, objectives and deliverables of the project. Legal, social, ethical and professional issues that may arise because of this project are then highlighted before moving onto the main body of the report.

The main body of the report divided into four phases, followed by some evaluations which described my Anti-Keyloggers Program (AKP). This includes ………, ………. as well as the development of the Keyloggers detections and deletions that uses several technologies including program language C#, SQLite and \_\_\_\_ which Issued and challenged that arose throughout development are also discussed to highlight how they were overcome.

The report then progresses into the critical evaluation of the project and a full post-evaluation which highlights the overall state of the final product, a technology spectrum and personal review as well as future work that will further enhance the functionality of the Keyloggers detection and deletion.

Further information included in the form of appendices can be found at the end of this report which constitutes other materials generated over the course of the project such as highlight reports, project schedule and the project initiation document.

|  |  |
| --- | --- |
| Statement of Word Count………………………………………………………………….. | Page |
| Code Submission URL…………………………………………………………………………. | Page |
| Introduction………………………………………………………………………………………. | Page |
| Background………………………………………………………………………………………. | Page |
| Aim and Objectives…………………………………………………………………………… | Page |
| Project Approach and Methods…………………………………………………………. | Page |
| Project Management…………………………………………………………………………. | Page |
| Legal, Social, Ethical and Professional Issues……………………………………… | Page |
| Architecture & Design………………………………………………………………………… | Page |
| Project Development………………………………………………………………………… | Page |
|  | Page |
|  |  |
|  |  |
|  |  |

Content:

# Statement of Word Count

# Code Submission URL

# Introduction

As we know, key logger is a program that enable to monitor and records every activities of the computer user by their typing on specific keyboard of a computer or a mobile device. The software tracks or logs on the keys without the knowledge of the user. As the result, it may lead to a great threat to user to leak of the important data while they typing on the keypads. Most of the computer users are laymen users who will not realize the present of the Keylogger and its functions, also they will not have such behavior to remove the important Keylogger when they using of the computer.

The threat is not only to retrieve the data, but also intercept passwords and other confidential information entered through the keyboards. The hackers could steal the PIN codes, bank account numbers, passwords to emails and social networking account credentials. The final results to the loss of the users’ property and money from close relatives.

Although there have some paid or free anti-free Keylogger program, but we don’t know the program is safety or not if there is a back door of the program which will leading to lost the data security. Design of the program to detect and delete the Keyloggers found in the computer system would completely understand what the Keylogger done and how to avoid it in stealing the data.

# Background

In the recent decades, there were many criminal cases related to the use of the Keyloggers. In the year of 2016, there were a large scale cyber-attack by using the “Hawkeye Keyloggers”, until the 2018, the updated version of “HawEye Keyloggers” was sold to the criminals for invading the target computer systems. The Keyloggers functioned by injecting the malware into the programs likes MSBuild.exe、RegAsm.exe、VBC.exe in the computer OS, and execute the payload code as it wishes. Such cyber-attacks brought large amount of money and property lost as the results. Thus Anti-Keyloggers became important for preventing those attacks.

In the market, there were many Anti-Keyloggers products like\_\_\_,\_\_\_,\_\_\_and \_\_\_. However, we do not know if there were backdoor of those program resulted to the information leakage, and also the concerns of the license of the Anti-Keylogger with copyright of the authors. Therefore, the safest way to prevent the Anti-keylogger is to make our own one. It can prevent the backdoor of the program and no need to have copyright concern. Also, develop an Anti-Keyloggers program did raise the public concerns on cyber security control.

# Aim and Objectives

The aim of this report is through developing an Anti- Keylogger Program to understand its underlying mechanisms, and to raise the concerns by people to alert them in dealing with the keylogging activities, and to perform a good cyber security control to prevent the attack by hackers.

In this project, I would try to write up the software program by using the computer languages for Keylogger detection and deletion. The target OS of my project would be Microsoft Windows 10 & 11 64-bit system. The reason of choosing Windows as my target OS because it is a very common OS which mostly used by computer users and me. The second reason is Windows OS may easily attack by hackers by using Keyloggers when compare with other OS.

However, further research has provided influence resulting in altered and newly derived objectives:

* 1. To write up a Keylogger program to understand the mechanism of keylogger in the computer system.
  2. To write up an Anti-Keyloggers program to detect and delete the Keyloggers in the computer system.
  3. To analysis the Keyloggers characteristics and stored the data in the database
  4. To delete the Keyloggers detected by using the program
  5. To test the program and validate the program

In addition, the core deliverables would be listed as follows:

* 1. To have a client application
     + The application should be broken down into a collective set of modules that execute specific tasks: detection and deletion of Keyloggers functions
     + The application should aid the prevention data exfiltration
     + The application must use a strong encryption module
     + The application should have multiple monitoring modules
     + The application should have front-end modules
  2. To have a database
     + The database should have standard security controls and it must host a database in a secure manner.
     + The database should have a database management tool
     + In this project, SQLite3 was selected for the database development because of its easier to use and well known by users.

# Project Approach and Methods

In order to understand the functions of keylogger and develop the program focusing on it, it is needed to understand the background and the usage of the Keylogger in operation system.

* 1. How keylogger works in window OS

How does spyware keylogging work? It is the basic question when programmer try to develop the program. The easiest way for keylogging work is the Ring3 keyboard Hook. The Ring3 is the privilege level of the processor, it can describe the permissions of the system. The Ring3 and some privilege escalation performed by some software in Ring3 is called system. It would be done by changing the machine’s codes to implement the keyboard Hook. A more advanced way is the kernal-level ioapic/idt hook. It is real-time feedback of the keyboard stroke or information through Hook. The common types of Hook include Inline, IAT or SEH and the common way of Hook is the most basic HookEX, and the more difficult API Hook or HookSSDT. What I want to focus on the Keylogger program is the API Hook.

6.2 API Hook

The API Hook is provided by Microsoft under window, it was belonging to low-level operation function for window’s operations. There are four syntax in SetWindowsHookExA with different parameters. By using the parameters of these syntax in order to monitor the low-level keyboard inputs in order to write up the keylogger programme.

6.3 Program Language selection

As we all know that in the language C#, it is able to deletes a file by saying “File.Delete”, therefore, under Window OS, it corresponds to DeleteFileA, the Kernel32.dll which provided export function that we can use DeleteFileA to delete the desired file directly by using this code. But how about the function if the Window is not up to date? Is it unable to run the software if the OS is out - dated? Luckily, the programming languages provide a layer of encapsulation on top of this as long as File.Delete is normal no matter what platform or version of the system it is on just delete the file. That's the reason to use File.Delete instead of using the system function directly and the program language C# is selected to write the program.

6.4 Project Approach

In order to write up a program that prevents the deletion of files on the OS, I would like to Hook DeleteFileA to make a program that prevents the deletion of files on my computer. I would like to install the Hook and write a function with the same parameters and return value as DeleteFileA in my DLL (Dynamic-link library). Then I would like to inject to the target program that I want to Hook (DLL injection technique). As there are many API hooking methods, I prefer to use Write Process Memory function that directly writes the DLL to the target program memory to decompile the other party's DLL and insert it. That means I would like to use a piece of own codes and replace it that no matter what method to use to inject, the final goal is the same, i.e. replacing the original with a fake one well-understood term.

Then, when the program deletes the file, no matter what language it is written in, it will call DeleteFileA when being deletes it. Under normal circumstances, DeleteFileA is normally deleted and returned. Thus, if I replace DeleteFileA with mine, it will naturally execute mine. I can judge whether it is deleting through the path of FileName passed by and what's in our important folder if it doesn't delete what I don't want him to delete. I am calling the original DeleteFileA to execute it back so that it will not report an error, the purpose is to keep the system from crashing. But what it feels is that it deleted the file successfully but in fact, it did not execute DeleteFileA and was skipped by me.

* 1. Project Methods

In order to injecting the DLL’s in system, the most important to remind is that the DLL code is executed by the system itself, but not my program. That means the DLL injected is equivalent to the internal of others. So we just need to hook it off. SetWindowsPos will do, forbid it to create threads Hook off CreateThreadA. In my program, there are 3 methods to implement the objectives:

*Method 1*

The method 1 is the kernel-level Hook is directly hooked under the hardware layer and the driver layer. The disadvantage is several times better than method 2 and method 3, but if others are also kernel-level programs and they are loaded before me, they can still pass the hook kernel. Mount the driver entry Learn the driver I want to load and analyze what are doing.

*Method 2*

Method 2 is the more commonly used method. It is done by DLL Inject secretly into the specified program to read its memory or use the control UI Automation (non-hook to read information). The disadvantages for some high-level and high-level processes, memory injection may be failed. Only passive injection can solve the problem and the cost is very high.

*Method 3*

Method 3 or use the simplest method SetWindowsEx to install an Exhook hook on WH\_KeyBoard. The disadvantage is it is very, very easy to roll over.

In short conclude, for the method 1, it must be the most brilliant and the least easy to find, and the efficiency is also the best. Method 2 is also possible, but the automatic test control is based on the face, and some text boxes are special and cannot get the value. Method 3 is very simple, very effective and hassle-free, but the biggest problem of 3 is that SetWindowsEx can set multiple hooks at the same time. This means there may be hooks on yours... if method 1 and 2 are not easy to find then method 3 is the easiest to find because the intention is too obvious, and the system function SetWindowsEx is the easiest to roll over. That is to say, as long as we get the behavior of WH\_KeyBoard, we will immediately terminate its main program and notify the user, then we have to make sure our termination is 100% high intensity. It will terminate the process with PspTerminateProcessById at the kernel level instead of the KillProcess of Ring3 (The user layer). The kernel-level process protection mechanism ObRegisterCallbacks would be used when receiving any operation request or access request, i.e.,

OperationInformation->Parameters->CreateHandleInformation.DesiredAccess=0; which abusing our permissions in the kernel and resolve no one to access the program, then ending the program which needs the address of the process to end, but of course it can't even access us. It won't end us, but it will also be killed by the end of the kernel-level process. This is the same as Ring3 and Ring0 class relationship.

*Methods for hook detection*

*Method A*

The principle is to scan the DLL file called by the process and then compare the original DLL file. The behavior of hook is to rewrite the function, so when I change the system function, it will definitely be different from my own system function, so this is just to prevent DLL injection. In order to know which programs were violated. It could be done by time judgement. A queue would be made first and join all processes, and then keep traversing the process queue and keep comparing the changes of their system functions. Every time a new process is found, it will be added to the queue. Therefore, one of the process system functions of the original process has changed, and the changed function is related to keyboard input. Thus, it must be one of the newly added processes (there may be more than one in a short period of time and this situation is rare and mostly does not happen as long as the scan frequency is fast) which modified the program that was changed.

Then at this time, we will first judge whether these new processes already have digital signatures, add 10 to the score, and then judge the process which DLLs are loaded. After determine what language the process is written in by calling the DLLs deduct points for some special languages ​​such as easy Language, then we judge whether the software has a connection with the Internet, and if so, the score continues to decrease. If there are multiple or sort from low to high at the end, remind to record the user's operation to the database. The rating value showing to the user what software might be monitoring your keyboard for the end. If it is only one, that means 100% sure, end directly and enter the record to the database.

*Module B*

It will be done firstly by putting 64-bit SSDT Hook off this SetWindowsEx and add a springboard. Then DebugWinEx if hook action is WH\_KeyBoard in debugwinex like ring0 layer. That means, the software layer to write sends a message and then waits in a loop until a return is received. The software pops up a prompt box, the process name is calling the SetWindowsEx function, and the action of the keyboard hook is executed that blocking return a message to the driver after the operation is completed. The Kernel-level process protection Kernel-level process termination as the sharpest shield and spear of the program plus the mixed detection of the two modes. The security software to ensure privacy is developed using C# Wpf And C/C++ mixed development both at the bottom and on the interface must be different.

Then the keyboard monitoring of the driver layer is actually not enough for most anti-software main defenses. The reason why they can protect them is because they run before kernel-level virus software so they are hooked into loading drivers in advance.

Then analyze the behavior of the mounted driver through whitelisting and memory disassembly as well as behavior analysis and Trojan library signatures. But once when we put its driver in the past. It is not work, so the driver-level response is relatively low. Most of them may rely on passive scanning after file addition, memory scanning in process creation, and passive scanning of mounted drivers to judge whether the process is risky, but we certainly can't analyze the security of the software and find something wrong and kill it. This is the developmental status and the introduction of the functions to be implemented in the future and the explanation of the ideas.

# Project Management

The successful delivery of projects mainly relies on project management to ensure deadlines and objectives are constantly being monitored and upheld. The initial approach taken was the creation of Trello. The reason to use Trello as scrum master board because of its well organized with time frame and the events. And it also enables the function of backlog, the work-in-progress column, the validate and complete column which enable for clear understanding of the project progress and what were not done yet. The Trello timeline figure of my project as showed in the Figure 1.

*Figure 1. Trello Timeline Backlog*

*Figure 2. Trello Timeline Work-in-Progress*

*……*

# Legal, Social, Ethical and Professional Issues

Legal, social, ethical and professional issues were constantly being considered throughout the development of this project as Keylogger concept as well as the Anti-Keylogger program heavily relies on collection, storage, and analysis of the information (the Key logs).

8.1 Legal

One of the main legal aspects that must be considered is the General Data Protection Regulation. In UK, the Data Protection laws mainly stated in the Data Protection Act 2018, which is a well structural and organized law enforced in UK. The General Data Protection Regulation (GDPR) mentioned in the Data Protection Act 2018 applies to both data controller and data processors who process the data, and the data processor responsible for managing and directly handling the data specified by the controller. It applies to any piece of information that directly or indirectly relates to an identifiable person which could even be a reference to an identifier. The reason why this is particularly important and is directly related to this project is because the Anti-Keyloggers Program (AKP) would retrieve and assess one’s keystrokes and provide feedback and react to the next steps which is to delete the Keyloggers detected.

In this project, the main legal considerations would be ensured the data process within the program will not be leak to other third party. It would be achieved by create own keylogger program and Anti-keylogger program that prevents the backdoor from other open source.

In addition, another legal concern is the Copyrights of Keylogger program developer when I take some of the Keylogger products for reference during my product development. (The Copyright, Designs and Patents Act, mentioned by UK Government, 1988). In order to prevent the copy rights violation, I would like to write up my own program and the program development is only used for the study purpose.

8.2 Social

The main social concern of the project is mainly the risk of computer data misuse resulting to the risk of cyber security crimes incidents. The database of the Anti Keylogger Program may have the risk of data leakage when there are third party to assess the database without permission or acknowledgement. In my own opinion, the most social benefit by developing the Anti-keylogger program is to raise people concern on Keylogging activities, especially there are increasing online transactions and online banking which leading to the great risk.

8.3 Ethical

The main ethical concerns in this project was the utilization of the retrieved information by using Keylogger, i.e. the Keyloggers information. It is a serious ethical issue in relation to this project because there is risk of the programmer to sell the stored data in the database may lead to another cyber security hazard that criminals will make use of the information to steal the money from bank accounts or other important and personal data if the passwords were being sold by the programmer. This would not only be unethical, but also be the problem of legal aspect for data processing regarding to the Anti Keylogger Program which could include hefty fines as well as significant reputational damage.

8.4 Professional

The professional aspect of this project is the own development of the program with own database. The limited using of the Open source information also prevents the backdoor of the source’s program. In this project, I assume that all data processors were honest and user of the applications would use the program properly to prevent failed running of the program.

# Architecture & Design

# Project Development

**Phase 1 – Keyloggers Detection**

For the phase 1 of the product development, the Anti-Keyloggers Program (AKP) included several projects in the repository. The descriptions of the projects are as follow:

**PPLLProtect.sys**

This project aimed to protect the process of the program and to prevent to be re-write and end. It adapted ObRegisterCallbacks and PsCreateSystemThread to protect the particular program running (Microsoft, 2022).

By using the PsProcessType to command on call back types of ObRegisterCallbacks, i.e.,

|  |
| --- |
| OpOperAtion.ObjectType = PsProcessType  (To monitor for the target types of process) |
| OpOperAtion.Operations = OB\_OPERATION\_HANDLE\_CREATE | OB\_OPERATION\_HANDLE\_DUPLICATE (To monitor handle develop and updates) |
| OpOperAtion.PreOperation = (POB\_PRE\_OPERATION\_CALLBAC K)& OneProcessAction  (To monitor on the bound functions) |
| ObRegisterCallbacks(& CallBackReg, & ProcessListenThread)  (To monitor on the registered bound functions) |
| HANDLE CurrentPID = PsGetProcessId((PEPROCESS)pOperationInformation->Object)  (To retrieve the reference document of process’s ID of operating process) |

When the program received any process of the “DUPLICATE” or “CREATE” functions, it will run into the “OneProcessAction” method for monitoring and implement the “ObRegisterCallbacks”process.

*“OneProcessAction” Implementation*

Using of the function code “char szProcName[25] = { 0 }”to preserve the process name, and using “strcpy(szProcName, GetProcessImageNameByProcessID((ULONG)CurrentPID))”to copy the progress name copied from the ID to “szProcName”

“GetProcessImageNameByProcessID” *Implementation*

Using the function code “char\* GetProcessImageNameByProcessID(ULONG ulProcessID)” to implemented the getting process name by process ID, and carry out the protection:

char\* GetProcessImageNameByProcessID(ULONG ulProcessID)

{

NTSTATUS Status;

PEPROCESS EProcess = NULL;

Status = PsLookupProcessByProcessId((HANDLE)ulProcessID, &EProcess);//EPROCESS

//Get the EProcess via handle

if (!NT\_SUCCESS(Status))

{

return FALSE;

}

ObDereferenceObject(EProcess);

return (char\*)PsGetProcessImageFileName(EProcess);

}

Phase 2 – Keyloggers Deletion

# Security

# Project End Report

Project Objective Overview

--which objectives achieved,

Project changes

--any changes in mind while performing the project

--

# Project Evaluations

Project Objectives Evaluation

--which objectives did not achieve and difficulities

Development Process Evaluation

Technology Evaluation

Limitations -- limitations of the projects

Future Development

Personal Reflection – especial during the COVID-19 pandamic

# 14. Conclusions

# 15. References

# 16. Appendix

# Appendix I – Project Proposal

|  |
| --- |
| **Project Proposal : Detection and Deletion of Keyloggers in Computer System** |
| 1. **Project Vision**   Keylogger, which is a surveillance software installed on a system to record the keystroke made on that system. My project is planned to design a computer program to detect the keylogger software when the computer startup. The second step is deletion the keyloggers after the detection. Although there have some paid or free anti-free keylogger program, but we don’t know the program is safety or not. Design the program will make me to completely to understanding what the keylogger done and how to avoid it to steal my data. |
| 1. **Keywords**   Anti-keylogger/ Keyloggers/ Keystroking/ Capture/ Malicious/ Spyware/  Data leakage/ Remove Keyloggers/ |
| 1. **Risk Plan**   - Changing requirements and priorities.  Consult to the supervisor when facing the critical problems.  - Poor documentation.  Reference to the previous project.  - Failure to deliver on time.  Apply VL from company when the progress is obviously slow. |

# Appendix II – Report Highlights

|  |
| --- |
| **PRCO304HK – Report Highlights 1** |
| **Name:** Yau Chak Man, Winters |
| **Date:** 10th February, 2022 |
| **Review of work undertaken:**   * Set up the GitHub repository for project management * Create the Trello Boards account and update the project set up file * Past assignment review for better management |
| **Plan of work for the next week:**   * Research the mechanism of the Keylogger * Develop the Keylogger program for more understanding of the mechanism of keylogging activities * Research for the program language used in writing the program |
| **Brief notes from supervisory meeting(s) since last Highlight:**   * More research on the Big Keylogging events |

|  |
| --- |
| **PRCO304HK – Report Highlights 2** |
| **Name:** Yau Chak Man, Winters |
| **Date:**24th February, 2022 |
| **Review of work undertaken:**   * Research on Keylogging activities done * Decided to work on API hook when writing the program * Updated the Trello Board |
| **Plan of work for the next week:**   * Write up the Keylogger program for better understanding on the mechanisms of Keylogging activities |
| **Brief notes from supervisory meeting(s) since last Highlight:**   * Research for outside works on Keyloggers may save more time in better understanding of the Keylogging activites |

|  |
| --- |
| **PRCO304HK – Report Highlights 3** |
| **Name:** Yau Chak Man, Winters |
| **Date:** 17th March, 2022 |
| **Review of work undertaken:**   * Draft of the Project Objectives and Approach of the Program development * Develop the Keylogger Program for evaluation and understanding * Update the Trello Board with the Draft and the Keylogger Program |
| **Plan of work for the next week:**   * Draft of the Project Aims, Objectives, Approach and Methods in writing the Anti-Keylogger Program * Updated the Project Highlights for record * Write up the Keylogging Behavior Database for program development * Research on CVE on Keylogging for better learning |
| **Brief notes from supervisory meeting(s) since last Highlight:**   * Advised to use one more Keylogger for testing on the program, e.g., bestx software * Keep main lines of objectives terse * Research on more CVE on Keylogging |

# Appendix III – Code Reference

**Reference Sources of the Codes used in the Program:**

processhacker Github: <https://github.com/processhacker/processhacker/blob/master/phnt/include/ntexapi.h?msclkid=b6006000ced911ec9cc40ae535c790bf>

[gentilkiwi](https://github.com/gentilkiwi) Github:

<https://github.com/gentilkiwi/mimikatz/blob/master/mimidrv/ioctl.h>

Mattiwatti Github:

<https://github.com/Mattiwatti/PPLKiller/tree/master/PPLKiller>

**Reference Sources of the Libraries used in the Program:**

1. Dfad
2. Afd
3. Afdsa
4. Asfdad
5. Adfsa
6. Asfdd
7. Agdfsdg
8. Agdfagad
9. Asgdfgdf
10. Agdfgd
11. Agdfsg
12. Adgsdgd
13. Agrdfgr
14. Adgstrg
15. Adgts
16. Dargreg
17. Adgrtg
18. Ragerg
19. Drgertg
20. Rgerg
21. Drgtrh
22. Agtr
23. Sdrgtr
24. Sdgt
25. Sdrgrtg
26. srgtgh