**HKU SPACE & UNIVERSITY OF PLYMOUTH**

**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 delves into four phases, followed by some evaluations which describe the This includes ………, ………. as well as the development of the \_\_\_\_ that uses several technologies including program language C#, \_\_\_ and ……. Issues and challenges 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 …………….

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.

|  |  |
| --- | --- |
|  | Page |
|  | Page |
|  | Page |
|  | Page |
|  | Page |
|  | 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

(Keylogger recent activities, famous events and its significance)

# 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
     1. The application should be broken down into a collective set of modules that execute specific tasks: detection and deletion of Keyloggers functions
     2. The application should aid the prevention data exfiltration
     3. The application must use a strong encryption module
     4. The application should have multiple monitoring modules
     5. The application should have front-end modules
  2. To have a database
     1. The database should have standard security controls and it must host a database in a secure manner.
     2. The database should have a database management tool
     3. 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

# 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

# Security

# Project End Report

Project Objective Overview

Project changes

# Project Evaluations

Project Objectives Evaluation

Development Process Evaluation

Technology Evaluation

Limitations

Future Development

Personal Reflection

# 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 – Project Planner

# Appendix IV – Initial Report