**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, \_\_\_\_\_\_\_\_ for his/her 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 the ……. followed by a ……… which describe the ……... This includes ………, ………. as well as the development of the…….. that uses several technologies including Python, ……. 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

Word Count:

# 2. Code Submission URL

# 3. 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.

# 4. Background and Objectives

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:

4.1 To write up an Anti-Keyloggers program to detect and delete the Keyloggers in the computer system.

4.2 To analysis the Keyloggers characteristics and stored the data in the database

4.3 To delete the Keyloggers detected by using the program

4.4 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 server
     1. The database server should have standard security controls and it must host a database in a secure manner.
     2. The server should have a database management tool
     3. All inbound and outbound communications channels must be encrypted
     4. In this project, SQLite3 was selected for the database development because of its easier to use and well known by users.

# 5. Method of Approach

The method to develop an Anti-Keylogger Program (AKP) includes

# 6. 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*

*……*

# 7. 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).

7.1 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.

whilst the log management system developed for this process is subject to this legislation, it also

helps enforce and uphold the GDPR through the implemented Windows logs module that keeps

track of information being copied and read from removable storage devices, as well as through the

increase security that the system offers by holding a record of events which provides accountability

and enabling security professionals to investigate any developing security incidents.

It is also worth mentioned the Computer Misuse Act 1990. which is the main piece of legislation in

the UK used to persecute computer crime. The automatic investigation module has data-crawling

properties and whilst it was initially considered that an element of active scanning on an external IP

address to gather port service information would be integrated, this may fall into section 3

*“unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc”* (Computer Misuse Act 1990). It was therefore decided that Shodan will be used an alternative means of achieving this, which eliminates the active element of directly interfacing with the respective systems.

7.2 Social

The wide spectrum of information captured by the log management system is worth considering, mainly in relation to the rise of computer crime which the system aims to combat through monitoring and detection. Individuals committing computer crime do so for several reasons whether it being personal gain such as obtaining a type monetary currency or even for corporate espionage which can certainly be costly to prevent and difficult to persecute depending in which jurisdiction the person is located. Unfortunately, this widespread issue has continued to grow as mentioned earlier in the report, however with the right mitigations in place such as the increase in the monitoring and response capabilities of an organisation, it is a step in the right direction to combat this issue which could in turn could result in a downwards trend of cyber security incidents if the right measures are in place to continuously block intrusion attempts.

7.3 Ethical

The main ethical concerns in this project was the utilization of the captured information, 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 if the passwords were being sold by the programmer. This would not only be unethical, but also be out of the scope of lawful basis for processing with regards to the GDPR which could include hefty fines as well as significant reputational damage.

7.4 Professional

The primary method information stored on the log management system and the automated investigation module is accessed is through the developed web interfaces that can be accessed by anyone on the network (depending on the company’s configuration) through the fully qualified domain name or internet protocol address. This in turn provides no accountability and no access control which could in turn result in the compromise of the confidentiality and integrity principles of information security. To mitigate against this, certain security measures which will be discussed in the architecture section of the report were implemented to combat this including the addition of an access control function when access to the system is requested as well as the logging of any such requests be it successful or unsuccessful in order to provide a form of accountability if a dispute were to occur within the organisation.

# 8. Architecture & Design

# 9. Development

Phase 1

Phase 2

Phase 3

Phase 4

# 10. Security

# 11. Project End Report

* 1. Project Objective Overview
  2. Project changes

# 12. Project Evaluations

* 1. Project Objectives Evaluation
  2. Development Process Evaluation
  3. Technology Evaluation
  4. Limitations
  5. Future Development
  6. Personal Reflection

# 13. Conclusions

# 14. References

# 15. Appendix

Appendix I – Project Proposal

Appendix II – Report Highlights

Appendix II – Project Planner

Appendix III – Initial Report