TUNIS BUSINESS SCHOOL
UNIVERSITY OF TUNIS

# IT360: Information Assurance and Security

Mariem Rejeb
Islem Jeridi
Malek Ben Hamed
Zakaria Ayadi

Submitted to Prof. Manel Abdelkader

March 2024

Tunis Business School
Ben Arous, TUNISIA

2023-2024

# 1 Introduction

As a response to the growing threat posed by keylogging attacks, outlined in Part 1 of our report, where key-loggers were identified as having significant privacy and security concerns, a comprehensive Key-logger Design framework is introduced in this document. Delving into the structural aspects of this program, the main purpose is to dissect the anatomy of keyloggers through various lenses, including user roles and use case scenarios. By scrutinizing these fundamental elements, a deeper understanding of how keyloggers function and interact within digital ecosystems is guaranteed.
Subsequent sections will detail the Key-logger's design and operational functionalities.

# 2 Key-logger Design

Outlining the structural elements of the Key-logger software, the system design provides a comprehensive overview of its architecture through UML diagrams.

## 2.1 Key-logger Users

There are 2 specific user roles essential to the operation of our Keylogger software.

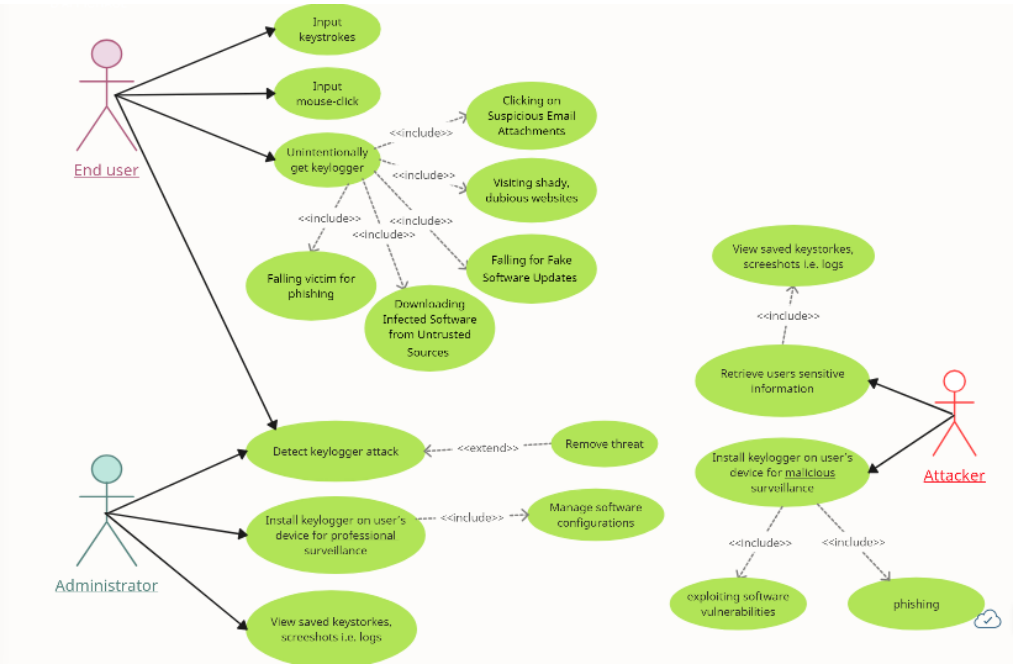
- End Users: Representing the **Victims**, they are typically individuals who rely on electronic devices for various purposes, ranging from personal to professional activities and who are unknowingly subjected to surveillance or monitoring through the use of keylogging software. These users unwittingly have their keystrokes and digital activities monitored by this malicious software. *For instance, a remote worker accessing company databases or an individual conducting online transactions would fall under the category of end users. They are exposing sensitive information like login credentials, personal data or financial details to potential surveillance.*

- Administrators: Serving as the backbone of system governance, administrators hold the critical responsibility of configuring and overseeing the entire keylogger software within organizational domains. With elevated access privileges and advanced features, administrators possess the authority to manage system configurations, orchestrate incident response protocols, and generate comprehensive reports to track system performance and potential security breaches. *For instance, an IT security manager or system administrator overseeing cybersecurity protocols within a corporate infrastructure embodies the essence of the administrator role. They act as the custodians of organizational data integrity and security, implementing they keylogging software on company devices or within a network for legitimate purposes, such as monitoring employee productivity, thwarting potential threats or ensuring compliance with regulatory standards and security policies.*

- Attackers: These malicious actors are individuals or entities who aim to compromise the security and privacy of end users and organizations by deploying keylogging software for nefarious purposes. Attackers may utilize various techniques such as phishing, social engineering, or exploiting software vulnerabilities to distribute keyloggers to unsuspecting victims. Once installed on a victim's device, the keylogger silently monitors and captures sensitive information, including login credentials, personal data, or financial details, which are then exploited for malicious activities such as identity theft, financial fraud, or espionage. Attackers often seek to evade detection and maintain persistence within the victim's system to continue their illicit activities undetected. They pose a significant threat to both end users and organizations, highlighting the importance of robust cybersecurity measures to defend against such malicious actors.

## 2.2 Key-logger Use Case Diagram

Illustrating the interactions between users and the software, depicting the functionalities this latter offers.




**In this keylogger use case diagram, three main actors interact within the system: the end user, the administrator, and the attacker,each playing distinct roles in either utilizing, managing, or exploiting the technology for various purposes.**

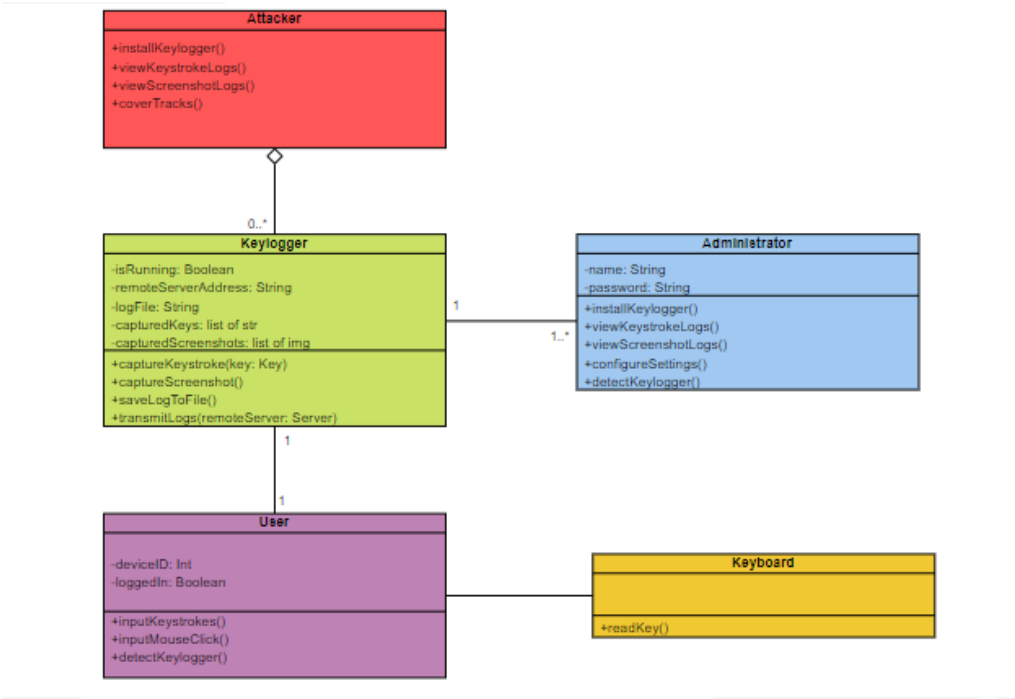
**Administrators hold the responsibility of managing keylogger installations, primarily for professional surveillance purposes i.e. to ensure compliance with the corporate policies. They install the keylogger software on user devices, configure software settings, and monitor saved keystrokes and screenshots for legitimate surveillance purposes. Additionally, they are equipped to detect keylogger attacks, enabling them to respond promptly and effectively to mitigate potential threats within their organizational domains.**

**Contrastingly, attackers aim to exploit keyloggers for malicious purposes. They install them on user devices through deceptive tactics like phishing or exploiting software vulnerabilities.. Once it is done, they can retrieve sensitive information captured by the keylogger, including saved keystrokes and screenshots, for nefarious intents such as identity theft or unauthorized access to confidential data.**

**Unfortunately, the end users unknowingly fall victim to keylogger installations through these actions.**

## 2.3 Key-logger Class Diagram

Showing the static structure of the program, including classes, attributes, methods, and relationships between them.




**This diagram is comprised of 4 classes:**

- The EndUser class: encapsulates actions related to user input, such as keystrokes and mouse clicks. It includes methods for inputting keystrokes and mouse clicks.
- The Administrator class: includes methods for installing the keylogger on user devices for professional surveillance, as well as viewing keystroke logs and screenshot logs.
- The Attacker class: includes methods for installing the keylogger on user devices for malicious purposes and retrieving sensitive information, such as keystroke logs and screenshots.
- The Keylogger class: represents the software responsible for capturing and logging keystrokes on the user's device. It includes methods for silently capturing keystrokes, saving them to logs, and potentially transmitting the logs to a remote location. This class is crucial for monitoring user activity surreptitiously and collecting sensitive information without the user's knowledge.

# 3 Key-logger Operations

A practical guide, detailing how keyloggers interact with and handle sensitive data, shedding light on the functions providing a detailed overview of the various actions performed by the software.

## 3.1 Key-logger exchanged data:

Keyloggers are designed to covertly capture various types of user interactions on a computing device, recording sensitive information without the user's knowledge or consent. The types of data captured can vary depending on their functionality and the specific features implemented by the attacker or administrator.

**In this report, there 3 types of data captured by the keylogger:**

- Keystrokes: recording every key pressed by the user on the keyboard whether it is virtual or not. This includes alphanumeric characters, special symbols, function keys, and even keyboard shortcuts. Keystroke logging enables to capture sensitive information such as passwords, usernames, credit card numbers, and other confidential data entered by the user.
- Mouse Clicks: In addition to keystrokes, the keylogger here also capture mouse clicks and movements. This data can provide insights into the user's interactions with graphical user interfaces (GUIs), including the selection of buttons, links, and menu options. Mouse click logging can be used to track user activity within applications and web browsers, enabling attackers or administrators to monitor navigation patterns and user behavior.
- Screenshots: the keylogger with its advanced features has the capability to capture screenshots of the user's desktop at regular intervals or in response to specific events. These screenshots can reveal sensitive information displayed on the screen, such as private messages, email contents, web pages, and documents. Screen capture functionality allows to visually monitor the user's activities and obtain visual representations of their digital environment.

## 3.2 Key-logger functions and steps:

### 3.2.1 Keystroke Logger:

**1st function: Capture Keystrokes**

- Step 1: Monitor keyboard input in real-time.
- Step 2: Capture each keystroke made by the user.

**2nd function: Record Keystrokes**

- Step 1: Store captured keystrokes in a log file or memory buffer.
- Step 2: Organize keystrokes by timestamp or sequence for later retrieval.

**3rd function: Concealment**

- Step 1: Operate stealthily to avoid detection by the user.
- Step 2: Hide its presence from antivirus software and system monitoring tools.

### 3.2.2 Screen Capture Module:

**1st function: Capture Screenshots**

- Step 1: Periodically capture screenshots of the user's desktop.
- Step 2: Save screenshots to a designated location or buffer.

**2nd function: Timestamping**

- Step 1: Associate each screenshot with a timestamp for chronological organization.
- Step 2: Ensure accurate timing to correlate screenshots with user activity.

### 3.2.3 Data Transmission Module:

**1st function: Data Packaging**

- Step 1: Package captured data, including keystrokes and screenshots.
- Step 2: Compress data to reduce transmission size and optimize bandwidth usage.

**2nd function: Transmission Protocol**

- Step 1: Establish a connection to a remote server or command-and-control (C2) infrastructure.
- Step 2: Transmit packaged data securely over the internet using protocols like HTTP, FTP, or encrypted channels.

**3rd function: Encryption**

- Step 1: Encrypt transmitted data to prevent interception or tampering by third parties.
- Step 2: Use strong cryptographic algorithms and secure communication protocols to ensure data confidentiality.

#### 3.2.4 Remote Control Module:

**1st function: Command Execution**

- Step 1: Receive commands from a remote attacker or control server.
- Step 2: Interpret commands to perform actions such as starting or stopping data capture, adjusting settings, or retrieving logs.

**2nd function: Response Handling**

- Step 1: Process responses or acknowledgments from the control server.
- Step 2: Handle errors or exceptions gracefully to maintain operational stability.

## 4 Conclusion

In summary, we delved into the intricate design and operational aspects of a keylogger, shedding light on its functionality and potential impact. Through the exploration of keylogger design, including user roles, use case diagrams, and class diagrams, a comprehensive understanding of how keyloggers interact within digital environments is gained. Additionally, the discussion on keylogger operations has elucidated the mechanisms by which these malicious tools capture data, their core functions, and the step-by-step processes involved in their operation. By examining them, we underscore the importance of cybersecurity vigilance and the need for robust defense mechanisms against such threats. In an era where digital privacy and security are paramount, it is imperative to remain informed and proactive in safeguarding sensitive information from potential breaches posed by keylogging activities.