Keylogger — Project Report

This is an individual project made for educational purposes only. The author is **not responsible** for any misuse. Use this project at your own risk and always follow laws and ethical guidelines.

Author 1: Maruti Marathe
About Maruti: https://linktr.ee/ryuzakila

Author 2: Supriya Prajapati
About Supriya: https://www.linkedin.com/in/supriya-prajapati-b84126232

1. What is a Keylogger?

A **keylogger** (keystroke logger) is a tool that records what a user types on a keyboard. It can be either software or a small hardware device. While keyloggers are often used for malicious purposes (such as stealing passwords or private messages), they can also be studied safely to learn how to detect and defend against them.

2. Why I chose this project

I chose this project to learn how keyloggers behave and how defenders can detect and stop them. The goal is to understand the concept, the types of data keyloggers produce, and how to protect systems not to cause harm.

3. Main components (simple)

- **Capture:** The part that reads keystrokes.
- **Store:** Where the captured text is saved (for example, a file or memory).
- **Persistence:** How the program tries to stay active on the device.
- **(Optional) Exfiltration:** How captured data could be sent out if used maliciously.

Note: Component descriptions are intentionally high-level and non-actionable.

4. What a keylogger produces

- A chronological list of typed characters with timestamps.
- Which application or window was active while typing (e.g., browser, editor).
- Sometimes additional data such as clipboard contents or screenshots.

5. How to tell if something might be a keylogger (beginner signs)

- Unknown programs running in the background.
- New entries appearing in the list of startup applications.
- Unrecognized files appearing in user folders (e.g., AppData, Temp).

- Alerts from antivirus or endpoint protection software.

6. How to protect yourself (practical beginner tips)

- Use **strong, unique passwords** and a **password manager**.
- Enable **Multi-Factor Authentication (MFA)** on important accounts.
- Do not open unknown email attachments or click suspicious links.
- Keep your operating system and applications **up to date**.
- Install a reputable **antivirus** or endpoint protection product and scan regularly.
- Avoid using untrusted USB devices.

Conclusion

Learning about keyloggers helps you better protect accounts and devices. The best defenses are: using MFA, keeping systems updated, practicing safe habits, and using good endpoint protection.