Keylogger with Encrypted Data Exfiltration

Introduction

The project 'Keylogger with Encrypted Data Exfiltration' was developed as part of the Elevate Labs internship program. The objective was to design a proof-of-concept (PoC) keylogger that demonstrates secure logging, encryption, and controlled data exfiltration mechanisms under ethical and educational guidelines. This project emphasizes the importance of cybersecurity awareness, data protection, and responsible development practices.

Abstract

This proof-of-concept project implements a safe, local keylogger using Python. It captures keystrokes via the pynput library, encrypts them using the cryptography.fernet module, and simulates encrypted data transmission to a localhost Flask server. The project operates ethically within user consent boundaries, serving as a learning model for understanding encryption, data protection, and system security.

Tools Used

• Python 3 — Core programming language
• pynput — To capture keystrokes
• cryptography.fernet — For encryption and decryption of keystroke data
• base64 — For encoding encrypted logs
• Flask — To simulate a localhost server for data exfiltration
• requests — For client-server communication

Steps Involved in Building the Project

1. Captured keystrokes using the pynput library.
2. Encrypted each log entry using cryptography.fernet.
3. Stored the encrypted logs locally with timestamps.
4. Created a Flask-based localhost server to simulate data exfiltration.
5. Implemented a GUI for user consent, start/stop control, and testing.
6. Added a kill switch and optional startup persistence for demonstration.

Conclusion

The Keylogger with Encrypted Data Exfiltration project successfully demonstrates how keystroke logging, encryption, and secure data handling can be integrated ethically. By simulating controlled data exfiltration to a local server, it highlights the importance of encryption and consent-based logging mechanisms. The project fulfills the objectives set by Elevate Labs and reinforces secure coding practices.