



Keylogger Detection and Termination System

Presented By:

Name: Bittu Kumar

Reg. No.: 222025109271

Department: B.Tech(CSE)

Semester: 7th

Presented To:

Guide: Mrs. Shiblya Swaroop

HOD: Dr. Naghma Khatoon

Date: 18 Nov 2025

Problem Statement

Challenge:

Keyloggers represent one of the most dangerous and stealthy types of malware, silently recording every keystroke and compromising sensitive data.

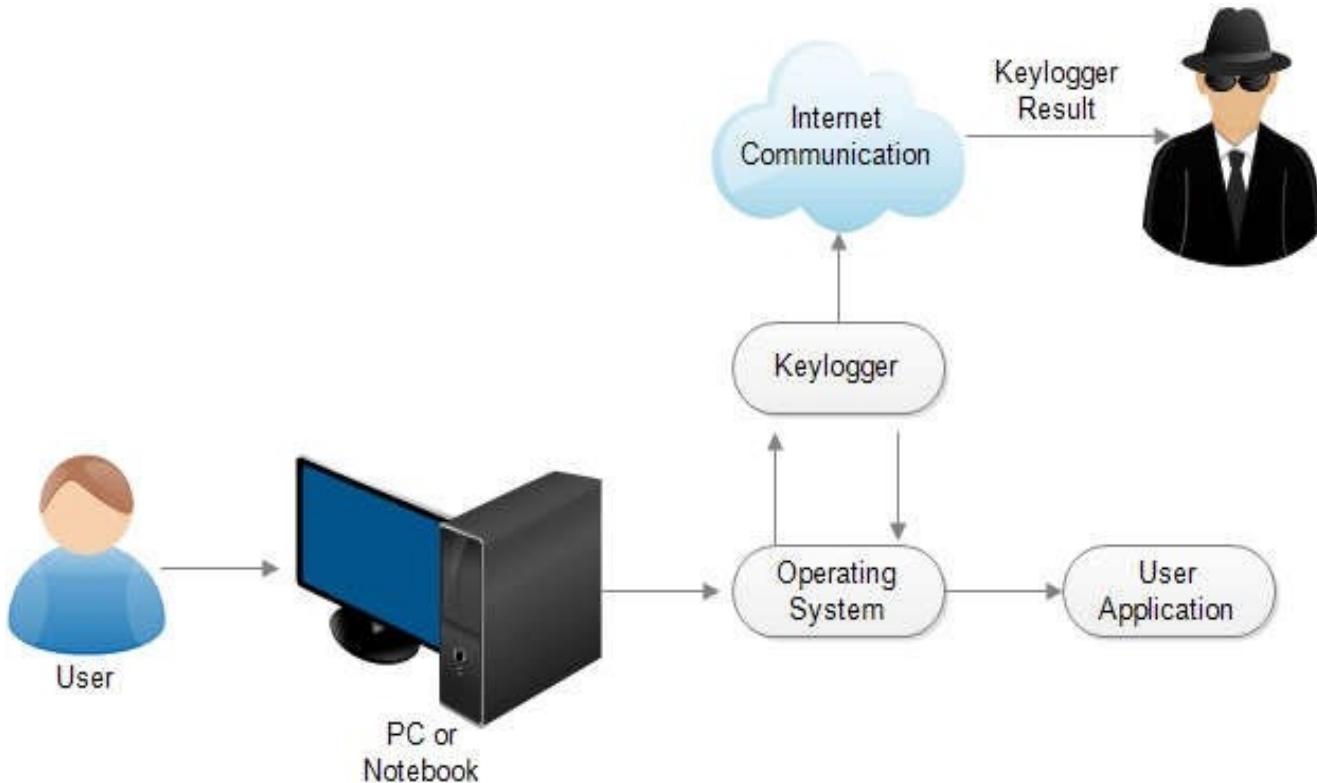
Key Issues:

- > Some keyloggers operate at kernel level, remaining undetected
- > Current systems lack behavioral and proactive defense mechanisms
- > Resource-heavy detection systems discourage continuous monitoring

Impact

Financial theft, identity fraud, unauthorized access, and data breaches affecting individuals and enterprises

Working of Keyloggers



Project Objectives

1) Intelligent Detection Framework

Develop behavioral and heuristic-based analysis to identify keyloggers through actions rather than code signatures

2) Decoy Input Injection

Implement proactive defense by injecting virtual keystrokes to trap hidden keyloggers

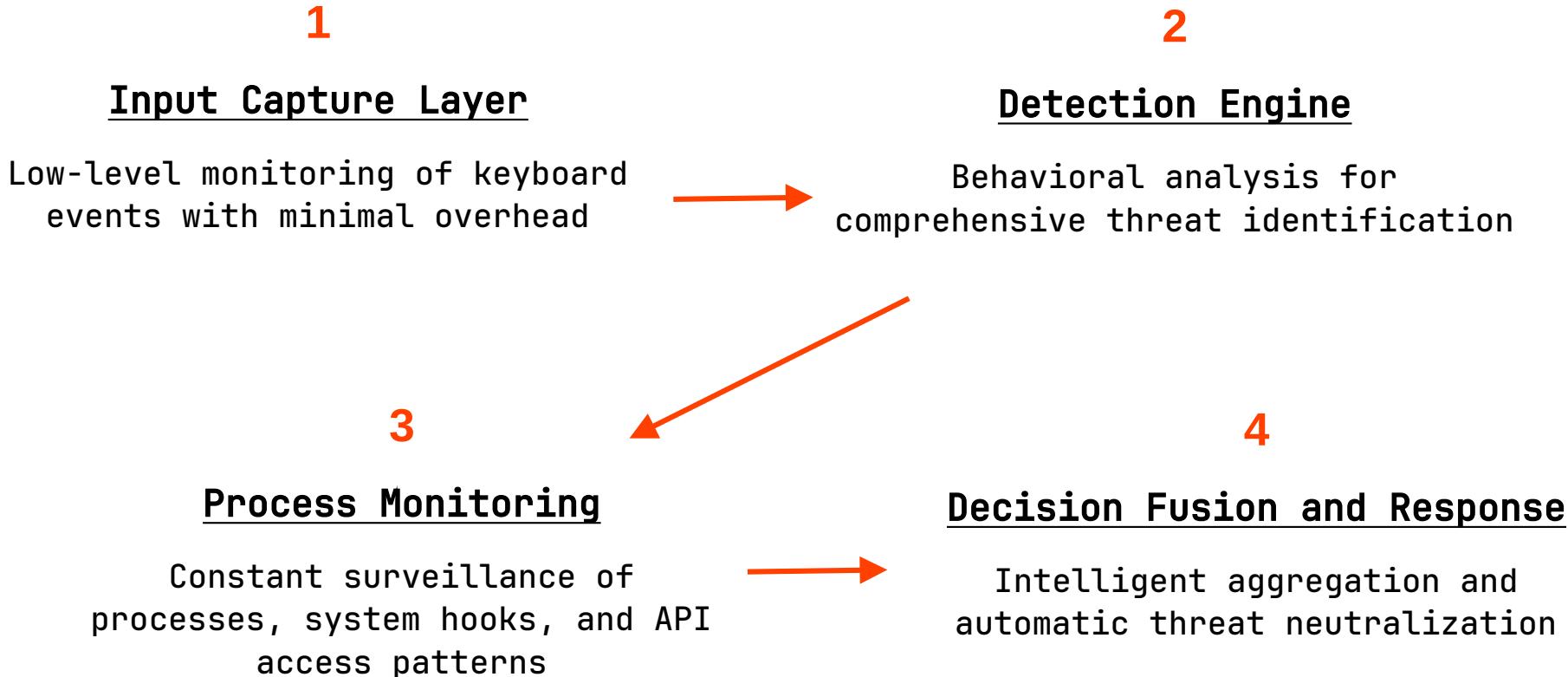
3) Minimize False Positives

Use decision fusion models to optimize detection accuracy with minimal false alarms

4) User-Friendly Interface

Create intuitive dashboard for monitoring, analysis, and forensic review

System Architecture



Detection Components

1) Suspicious Process Scanner

- > Multi-factor threat scoring based on naming, path, and resource usage
- > Categorization into **Medium**, **High**, and **Critical** levels

2) Startup & Persistence Monitor

- > Scans `~/.config/autostart/`, `systemd` services, and cron jobs
- > 80% detection rate of autostart configurations in testing

3) Network Activity Analyzer

- > Monitors external connections from suspicious processes
- > Flags potential data exfiltration attempts

4) Input Device Access Monitor

- > Tracks processes with open handles to `/dev/input/*` devices
- > Identifies both hardware and software-based keystroke capture

System Interface

Keylogger Detection and Termination System

Threats Detected!

Suspicious Processes Startup & Services Network Activity Real-Time Monitor

Detected processes with suspicious behavior patterns

PID	Process	User	Threat	Score	Command Line
3763	python	bittu	Critical	75%	/home/bittu/Desktop/keylogger-detection-system/keylogger
3816	uv	bittu	Critical	75%	uv run kelogger.py
3857	python	bittu	Critical	75%	/home/bittu/Desktop/keylogger-detection-system/.venv/bin/
3746	uv	bittu	Medium	45%	uv run light_main.3.py

Full System Scan **Terminate Process** Start Monitoring Save Report Threats: 5

This screenshot shows the main interface of the 'Keylogger Detection and Termination System'. At the top, there's a navigation bar with tabs for Suspicious Processes, Startup & Services, Network Activity, and Real-Time Monitor. A red banner at the top right indicates 'Threats Detected!'. Below the banner, a section titled 'Detected processes with suspicious behavior patterns' lists four processes. Each row includes the PID, process name, user, threat level (either Critical or Medium), score (75% or 45%), and command line. The 'Terminate Process' button is highlighted in red. At the bottom, there are buttons for Full System Scan, Start Monitoring, Save Report, and another 'Terminate Process' button. The overall theme is orange and grey.

1) Suspicious Process Detection

Keylogger Detection and Termination System

Threats Detected!

Suspicious Processes Startup & Services Network Activity Real-Time Monitor

Detected processes with suspicious behavior patterns

PID	Process	User	Threat	Score	Command Line
3763	python	bittu	Critical	75%	/home/bittu/Desktop/keylogger-detection-system/keylogger
3816	uv	bittu	Critical	75%	uv run kelogger.py
3857	python	bittu	Critical	75%	/home/bittu/Desktop/keylogger-detection-system/.venv/bin/
3746	uv	bittu	Medium	45%	uv run light_main.3.py

Confirm Termination

Terminate process 'uv' (PID: 3816)?

Warning: Only terminate if you're certain it's malicious. This may require sudo privileges.

Yes No

Full System Scan **Terminate Process** Start Monitoring Save Report Threats: 5

This screenshot shows the same system interface as the first one, but with a modal dialog box titled 'Confirm Termination' in the center. The dialog asks if the user wants to terminate the process 'uv' (PID: 3816). It includes a warning message about only terminating malicious processes and potentially requiring sudo privileges. There are 'Yes' and 'No' buttons at the bottom of the dialog. The rest of the interface remains the same, with the 'Terminate Process' button still highlighted in red.

2) Suspicious Process Termination

Limitations

Advanced Evasion

Sophisticated malware with polymorphic code and anti-debugging can bypass detection

Kernel-Level Threats

Rootkit-level keyloggers can hide from user-space detection

False Positives

Legitimate tools may trigger alerts

Resource Impact

May affect older hardware during continuous monitoring

Conclusion

The Keylogger Detection and Termination System successfully demonstrates that effective security monitoring is achievable through open-source solutions combining behavioral intelligence, proactive defense, and user-centric design.

Key Achievements:

- 1) Integrates behavioral analysis, process monitoring, and heuristic rules
- 2) 80%+ detection rate with 30% false positives in testing
- 3) Minimal resource consumption suitable for continuous monitoring
- 4) Easy threat neutralization with a single click
- 5) Intuitive interface making advanced security accessible to all users

Thank You!