Clipboard Hijacking Simulation & Protection System

Project Name: Clipboard Hijacking Simulation (Shentinelix Sphere Internship Project)

Date: 2025-12-15
Version: 1.0.0

1. Executive Summary

The **Clipboard Hijacking Simulation** is an educational cybersecurity project designed to raise awareness about the risks of clipboard hijacking—a technique where malicious websites secretly modify the content of a user's clipboard. The project consists of a safe simulation environment and a defensive browser extension, bridging the gap between theory and real-world security awareness.

2. Project Objectives

- Educational awareness of clipboard hijacking techniques.
- Risk-free demonstration without executing malicious code.
- Proactive defense through a real-time browser extension.
- Ethical and responsible use of cybersecurity knowledge.

3. Technical Architecture

3.1 Web Application (Simulation)

The simulation is built using Node.js with Express.js for backend services, and a frontend composed of HTML5, CSS3, and Vanilla JavaScript. It integrates the Clipboard API to demonstrate command manipulation in a controlled environment.

3.2 Browser Extension (NoHijacking)

The NoHijacking browser extension is developed using Manifest V3 and includes content scripts, a background service worker, and a popup interface. It detects clipboard discrepancies and warns users in real time.

4. Key Features

- Split-view dashboard showing original and hijacked commands.
- Real-time visual alerts and safe terminal emulator.
- Live clipboard protection via browser extension.
- Local-only logging with strong privacy guarantees.

5. Safety & Ethical Guidelines

The project strictly avoids executing malicious code and is designed for localhost use only. Clear warnings, disclaimers, and an educational focus ensure responsible use of the demonstrated techniques.

6. Future Enhancements

- Advanced pattern detection using machine learning.
- Support for Firefox and Safari browsers.
- Enterprise-level reporting and analytics.
- Mobile-focused clipboard security demonstrations.

7. Conclusion

The Clipboard Hijacking Simulation project effectively demonstrates a subtle yet dangerous attack vector. By combining an interactive simulation with a real-world defensive solution, it significantly enhances cybersecurity awareness and promotes safer computing practices.