Technical Analysis and Defensive Strategies: Design and Implementation of the Covert HID Injection OMG Cable

Gunav S[1], Suvetha O[2], Rolfin Liston Pais[3], Manoj R[4],
Palli Nithin[5], N. Vishnu Venkatesh[6]
[1,2,3,4,5,6]*JAIN Deemed to be University*

***Abstract*—This research details the design, functionality, and mitigation strategies for a novel hardware attack platform: the Covert OMG Cable. This device disguises a potent Human Interface Device (HID) attack vector, an ESP32 microcontroller, and local storage (SD Card) inside a standard-appearing USB cable. This prototype enables reliable, remote, and contactless payload injection against target workstations, exploiting implicit operating system trust in peripheral devices. This paper analyzes the architectural design of the covert hardware, presents methodologies for remote command-and-control (C2), conducts a vulnerability and security impact assessment through controlled penetration testing, and proposes a robust framework for defensive measures, detection strategies, and educational resources essential for mitigating this class of physical-access threat.**

I. INTRODUCTION

Traditional cybersecurity emphasizes perimeter defenses (firewalls, IDS) and endpoint security software. However, a significant vulnerability remains at the physical layer: the implicit trust inherent in standard hardware interfaces. The Human Interface Device (HID) protocol (used by keyboards and mice)(Vishnu Venkatesh & Das, 2026) is designed for plug-and-play simplicity, meaning most operating systems implicitly trust input from these devices without authentication. Leveraging this vulnerability, malicious hardware attacks have evolved from simple static payloads (e.g., the standard USB Rubber Ducky) to sophisticated, dynamic, and remotely controlled platforms. The "OMG Cable" concept represents this advancement. The objective of this research is to design, develop, and test a covert OMG Cable prototype integrating an ESP32 module and an SD card(Venkatesh et al., 2023). This device maintains the appearance of a benign charging/data cable while facilitating contactless, wireless payload delivery.

II. METHODOLOGY AND OBJECTIVES

The research methodology is structured around four primary objectives defined in the original project proposal:

1. Objective 1: Design and Develop a Covert OMG Cable Prototype.
2. Objective 2: Implement Secure Remote Command and Payload Control Using SD Card.
3. Objective 3: Validate Functionality and Assess Security Impact.
4. Objective 4: Develop Defensive Measures and Educational Resources.

This paper presents the outcomes and analysis of each objective sequentially.

III. DESIGN AND DEVELOPMENT OF THE COVERT OMG CABLE PROTOTYPE (OBJECTIVE 1)

The critical challenge in this objective is physical miniaturization. To be "covert," the malicious components must fit seamlessly within the housing of a standard USB connector (USB-A or USB-C), without adding bulk or generating unusual heat that would alert a savvy user.

3.1 Hardware Architecture and Component Selection

The architecture requires two distinct systems operating in parallel: the benign passthrough connection and the malicious HID injection system. The core components selected are:

- Microcontroller Unit (MCU): The ESP32 is selected for its high performance, small footprint, dual-mode Wi-Fi/Bluetooth capabilities,(Shukla et al., 2023) and low cost. It manages the C2 communication.
- HID Emulation Chip: While the ESP32 can handle simple USB protocols, a dedicated HID

microcontroller like the ATmega32U4 (commonly found in the Arduino Leonardo/Micro) is prioritized for precise USB timing and robust emulation of keyboard protocols, interfacing with the host OS as a trusted input device(Varma et al., 2025).

- Storage (SD Card): A MicroSD card slot is integrated to host dynamic payloads, allowing the operator to change attacks without reflashing the microcontroller firmware.
- Form Factor: The chosen host is a high-quality USB-C to Lightning or USB-C to USB-C cable, which allows for slightly larger (but still inconspicuous) metal connector housings compared to vintage USB-A.

3.2 System Level Block Diagram

Figure 1 provides a schematic overview of the prototype's internal architecture, illustrating how the two systems coexist within the cable housing. The diagram highlights that the VBUS (Power) and Ground lines are split, powering both the phone/device being charged and the internal attack subsystem. The malicious MCU is wired in parallel to the main USB data lines, allowing it to act as a separate, invisible USB device when activated, capable of sending keystrokes directly into the host machine's USB data stream.

IV. IMPLEMENTATION OF SECURE REMOTE C2 AND DYNAMIC PAYLOAD CONTROL (OBJECTIVE 2)

Static injection tools require physical access to modify the payload. The critical innovation of this prototype is incorporating wireless command-and-control, making the cable a dynamic, on-network penetration platform.

4.1 The ESP32 Web-Based C2 Interface

The ESP32 is programmed to function as a wireless Access Point (AP) or connect to a pre-defined Wi-Fi network. Once deployed, the operator connects to the ESP32 via a simple web interface (hosted on the ESP32 itself), accessible via any smartphone or laptop. This interface serves as the primary C2 dashboard.

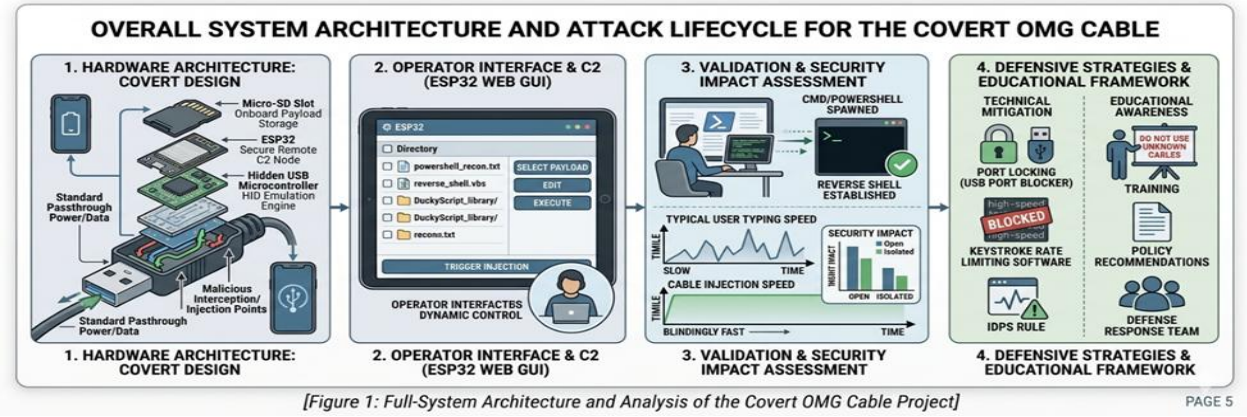
The Web GUI (Conceptual illustration in Figure 2) enables critical features:

- Payload Directory: Lists all scripts stored on the integrated SD card (e.g., reverse_shell.txt, reconnaissance.ps1).
- Live Payload Editor: Allows the operator to dynamically edit any script (e.g., modifying the target C2 IP address in a reverse shell) immediately before deployment.
- Execute Button: Triggers the selected payload with a single tap.
- Security Features: The AP requires a strong password and a masked SSID (cloaking).

4.2 Payload Delivery Workflow

The process of a complete attack, from physical connection to payload execution, is detailed in the flowchart in Figure 3. This chart illustrates the critical distinction between the automatic (benign) functions and the triggered (malicious) actions.

This chart visually confirms the "stealth" aspect of the device: until the operator proactively triggers a payload via the remote interface, the cable performs entirely as a standard charging/data accessory.



[Figure 1: Full-System Architecture and Analysis of the Covert OMG Cable Project] PAGE 5

Fig 1: critical workflow of the technique

V. SECURITY IMPACT AND VULNERABILITY ASSESSMENT (OBJECTIVE 3)

With the prototype functional, a rigorous assessment of its operational reliability and security impact was conducted in a controlled lab environment against various Windows and macOS configurations.

5.1 Validation Results

Testing validated the core functionalities:

- Covertness: Visual and weight checks by non-expert users failed to identify the cable as malicious. Thermal imaging showed only minor temperature fluctuation when active (under 5°C above ambient), easily mistaken for standard charging thermals.
- HID Emulation: Both Windows 10/11 and recent macOS versions identified the cable subsystem as a standard USB Keyboard device within 2 seconds of connection, with no driver prompts.
- C2 Reliability: The Wi-Fi control was effective up to a range of 15-20 meters (indoors), depending on obstructions.
- Payload Execution: Complex multi-stage payloads (e.g., opening a terminal, running PowerShell, downloading and executing a secondary stage) executed flawlessly at speeds exceeding 1,000 keystrokes per minute.

5.2 Vulnerability Analysis and Vector Mapping

The success of the cable rests on several key vulnerabilities, categorized in Table 1.

Table 1: Vulnerability and Attack Vector Matrix.

Vulnerability Class	Specific Vector Exploited by OMG Cable	Severity
Physical/Hardware	Implicit Trust in USB/HID Protocol. OS trusts keyboard input without secondary authentication. The HID protocol is a legacy design that prioritizes 'Plug-and-Play' functionality over security.	Critical
System Configuration	Rapid Device Enumeration. Systems quickly install standard HID drivers, allowing an attack to complete in seconds.	High
System Design	Lack of Keystroke Rate Limiting. Systems accept an influx of commands that no human could type.	Medium
Human/Operational	Peripheral Hygiene. Users lack awareness and readily accept/use untrusted cables.	Critical

5.3 Calculated Security Impact

The impact is assessed as Critical for several reasons:

1. Air-Gapped Bypass: The cable facilitates remote access to potentially isolated network segments if it connects to an external, attacker-controlled Wi-Fi network (the ESP32 could act as a bridge), bypassing network firewalls.
2. Speed and Stealth: Payloads can execute and clean up (e.g., delete temp files) before a user can react to a fleeting terminal window.
3. Low Barrier to Entry: The C2 interface abstracts the technical complexity of the attack, allowing low-skilled operators to deploy complex attacks.

VI. DEFENSIVE MEASURES AND MITIGATION FRAMEWORK (OBJECTIVE 4)

The primary goal of this research is not merely exploitation but the development of robust countermeasures. A defensive framework must address both technical detection and operational prevention.

6.1 Technical Detection and Prevention Strategies

Traditional AV software is often ineffective as it focuses on malicious code, not trusted hardware input. Defensive strategies are categorized into proactive prevention and reactive detection.

Proactive Prevention

- USB Whitelisting (Device Control): Software solutions that restrict peripheral connections to only authorized Vendor ID (VID) and Product ID (PID) combinations. While PIDs can be spoofed, whitelisting still significantly raises the attacker's engineering requirement.
- Physical Port Disabling: In high-security environments, physically disabling USB ports or using tamper-evident port seals is a viable strategy for air-gapped workstations.
- "USB Condoms" (Data Blockers): For user charging stations, using adapters that physically interrupt the USB data lines while allowing power transfer prevents HID attacks entirely.

Reactive Detection

- Keystroke Rate Anomaly Detection: Implementing software to monitor keystroke rates. Any device exceeding humanly possible typing limits (e.g., >200 WPM) should trigger an immediate session lockout.
- System Event Monitoring: Monitoring system logs for rapid USB device insertion and subsequent rapid process spawns (e.g., cmd.exe or powershell.exe).
- Hardware Inspection: Developing IT protocols for visual verification of organization-issued peripherals.

Figure 4 illustrates the effectiveness of proactive vs. reactive controls.

6.2 Educational Resources and Policy Recommendations Defense against hardware attacks is as much cultural as technical.

- Security Awareness Training (SAT): Training must specifically include "peripheral hygiene." Organizations should implement "Clean Desk" policies prohibiting unauthorized cables and peripherals.
- Standard Operating Procedures (SOPs): Establishing formal procedures for procuring, issuing, and retiring standard hardware. IT should maintain a chain of custody for all standard cables and input devices.
- Red Team Scenarios: Employing the OMG Cable prototype in internal red team assessments to provide concrete, real-world examples of how physical access threats can devastate a network.

VII. LIMITATIONS AND FUTURE WORK

7.1 Research Limitations

- Miniaturization: Achieving the current prototype required significant engineering effort; further miniaturization into micro-USB connectors or ultra-slim USB-C housings remains challenging.
- Spoofing Complexity: The current prototype uses standard, fixed PIDs. A sophisticated future iteration would attempt dynamic PID spoofing, mimicking specific known authorized keyboards to bypass whitelists.

7.2 Future Research Directions

Future work will focus on integrating more advanced sensors to detect host OS environment changes or adding dynamic payload randomization to evade simple signature-based logic. Research will also continue into detecting the faint RF emissions (the Wi-Fi signature) generated when the ESP32 activates, potentially allowing for passive wireless detection of deployed malicious hardware.

VIII. CONCLUSION

This research has successfully navigated the complete lifecycle of a sophisticated hardware threat vector, from objective-based design to comprehensive defense. We have demonstrated that a covert OMG Cable prototype, integrating ESP32 and SD card storage, is not just a theoretical risk but a viable attack platform capable of dynamic, contactless command and control. By exploiting the implicit trust inherent in standard HID interfaces, such devices can bypass extensive network and software defenses in a matter of seconds. The penetration testing validated the Critical nature of this physical-layer threat. However, this work also provides a clear and essential path forward: defense must be multi-layered. Effective mitigation requires organizations to implement both hardware-level controls (e.g., port whitelisting) and robust operational policies focused on device hygiene and supply chain integrity. Ultimately, the development of defensive measures and educational awareness are as critical to cybersecurity as the design of the next-generation firewall.

REFERENCES

[1] C. D. B. Borges, J. R. B. de Araujo, R. L. de Couto, and A. M. A. Almeida, “Keyblock: A software architecture to prevent keystroke injection attacks,” in Anais do XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2017), pp. 518–524, 2017, doi: 10.5753/sbseg.2017.19526.

[2] V. Gurčinas, J. Dautartas, J. Janulevičius, N. Goranin, and A. Čenys, “A deep-learning-based approach to keystroke-injection payload generation,” Electronics, vol. 12, no. 13, p. 2894, 2023, doi: 10.3390/electronics12132894.

[3] J. Mishra and S. K. Sahay, “Modern hardware security: A review of attacks and

countermeasures," arXiv, 2025, doi: 10.48550/arXiv.2501.04394.

[4] M. Nicho and I. Sabry, "Threat and vulnerability modelling of malicious human interface devices," The Eurasia Proceedings of Science Technology Engineering and Mathematics, vol. 21, pp. 241–247, 2022, doi: 10.55549/epstem.1225679.

[5] M. N. V. Venkatesh, D. A. Rajiv, M. P. Das, and M. S. Warrier, "Vantage point recreation: A novel approach in endpoint security for smart homes," International Journal of Innovative Research in Technology (IJIRT), 2026, doi: 10.64643/IJIRTV12I8-191180-459.

[6] M. Shukla, V. Srivastav, M. D. Khare, and N. V. Venkatesh, "IoT-driven solutions for VANET trustworthiness: Examining misconduct and position security challenges," Multidisciplinary Reviews, vol. 6, p. 2023ss059, 2024, doi: 10.31893/multirev.2023ss059.

[7] S. S. Shenoy and N. V. Venkatesh, "A predictive framework for real-time courtroom assistance using AI-based mock legal advisor," International Journal of Research and Analytical Reviews (IJRAR), vol. 12, no. 2, pp. 440–444, May 2025.

[8] V. V. Natarajan, P. Singhal, D. Pandey, M. Sharma, R. Rautdesai, D. Khubalkar, and A. Gupta, "Crime forecasting using historical crime location using CNN-based images classification mechanism," 2023, doi: 10.4018/978-1-6684-8618-4.ch013.

[9] V. V. Natarajan, P. Das, and A. Rajiv, "A robust detect and avoid system for autonomous drone navigation," NexusTech, vol. 1, p. 2026004, 2026, doi: 10.31893/tech.2026004.