RootKitten-Based Hardware-Assisted Payload Execution Framework for Ethical Penetration Testing

Domain: Cyber Security / Ethical Hacking / Network Security

SDG Alignment: SDG-9 (Industry, Innovation & Infrastructure), SDG-16 (Peace, Justice & Strong Institutions)

1 Abstract

This research proposes the development and implementation of a hardware-assisted penetration testing framework utilizing the RootKitten device, built on the ESP32-S3 microcontroller platform. The framework aims to simulate real-world physical access attack vectors through Human Interface Device (HID) emulation, providing an ethical and controlled environment for evaluating endpoint security vulnerabilities. Unlike traditional software-based penetration testing tools, this approach emphasizes physical attack surfaces that are often overlooked in conventional security assessments.

The proposed system integrates modular components including payload management, execution control, safety mechanisms, and comprehensive monitoring capabilities. By employing USB and Bluetooth Low Energy (BLE) HID emulation, the framework demonstrates common attack techniques such as keystroke injection, credential harvesting, and privilege escalation within isolated test environments. All payloads are pre-validated and executed in sandboxed virtual machines or controlled physical devices to ensure ethical compliance and prevent unintended exploitation.

The project aligns with Sustainable Development Goals (SDG-9 and SDG-16) by promoting innovation in cybersecurity infrastructure and supporting institutional resilience against emerging threats. The research methodology follows industry-recognized red-team and blue-team practices based on the MITRE ATT&CK framework, ensuring structured and systematic vulnerability analysis.

Expected outcomes include a functional prototype demonstrating hardware-assisted attack simulation, comprehensive documentation of identified security gaps, and actionable defense recommendations. The framework serves as an educational tool for cybersecurity training, enabling students and researchers to gain hands-on experience with physical attack vectors in a safe, controlled environment. By bridging the gap between theoretical security concepts and practical implementation, this project contributes to advancing endpoint security research and defense strategy development.

2 Proposed Solution

2.1 Overview of the Solution

The proposed solution introduces a **RootKitten**-based payload execution framework that leverages hardware-assisted penetration testing to simulate real-world attack vectors. This framework operates within a controlled, ethical environment to identify security vulnerabilities and provide actionable defense recommendations. The system combines physical access attack simulation with automated monitoring and analysis capabilities, addressing critical gaps in endpoint security assessment.

2.2 Core Components

The framework consists of five key components:

- Uses a dedicated hardware device (ESP32-S3 based RootKitten) as the attack initiator
- Executes pre-defined and adapted payloads through HID emulation
- Simulates real-world red-team techniques following MITRE ATT&CK framework
- Operates in a controlled and ethical testing environment with safety constraints
- Provides comprehensive logging, monitoring, and defense analysis capabilities

2.3 System Architecture

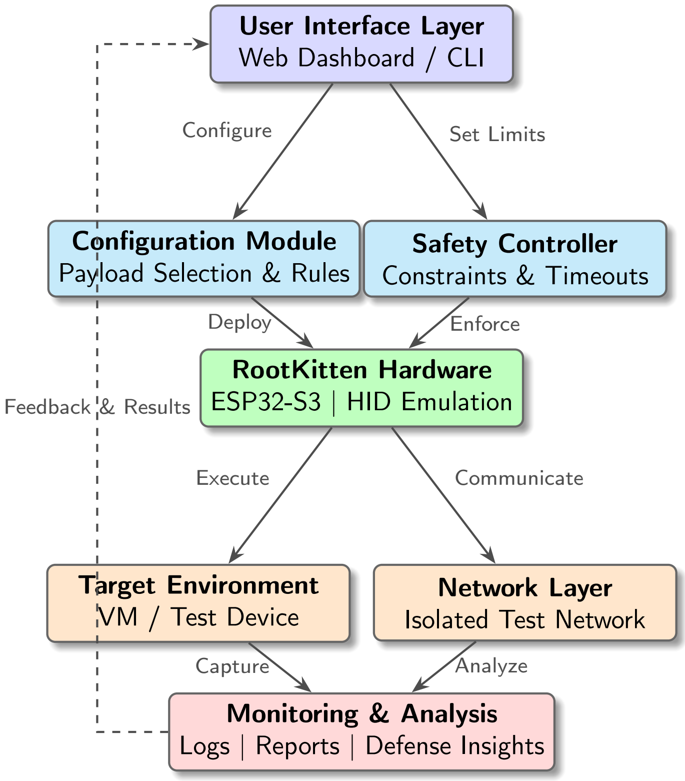

Figure 1: Hierarchical System Architecture of RootKitten Framework

2.4 Architectural Components

2.4.1 User Interface Layer

Provides web-based dashboard and command-line interface for researchers to interact with the framework, configure attack scenarios, and visualize results.

2.4.2 Configuration Module

Manages payload library, attack scenario selection, and execution parameters. Supports customization of HID scripts and automation logic tailored to specific test environments.

2.4.3 Safety Controller

Implements mandatory safety constraints including execution timeouts, rollback mechanisms, and kill-switch functionality to prevent unintended damage during testing.

2.4.4 Hardware Interface Module

RootKitten (ESP32-S3) serves as the physical attack vector, providing:

- USB HID emulation (keyboard/mouse simulation)
- Bluetooth Low Energy (BLE) HID capabilities
- Onboard payload storage and execution engine
- Real-time communication with control system

2.4.5 Target Environment

Isolated test systems including:

- Virtual machines (VirtualBox / VMware)
- Physical test devices (Windows, Linux, Android)
- Sandboxed network environment

2.4.6 Monitoring & Analysis Module

Captures and processes:

- System activity logs
- Network traffic (via Wireshark)
- Execution reports with timestamps
- Security impact assessment
- Defense recommendations based on MITRE ATT&CK mapping

2.5 Key Features

- **Hardware-Assisted Testing:** Physical USB/BLE device simulates insider threat scenarios
- **HID Automation:** Keystroke injection and mouse emulation for credential harvesting, privilege escalation, and data exfiltration simulation
- **Ethical Compliance:** No real malware deployment; all payloads are sandboxed and reversible
- **Modular Architecture:** Extensible framework supporting custom payload development
- **MITRE ATT&CK Alignment:** Maps executed techniques to industry-standard threat taxonomy

2.6 Tools & Technologies

- **Hardware:** RootKitten (ESP32-S3 microcontroller)
- **Virtualization:** VirtualBox, VMware Workstation
- **Operating Systems:** Ubuntu 22.04 LTS, Windows 10/11, Android 12+
- **Programming:** Python 3.10+, Lua (payload scripting), C++ (firmware)
- **Monitoring:** Wireshark, Sysmon, OSSEC
- **Framework:** MITRE ATT&CK Navigator for technique mapping

2.7 Scope & Limitations

2.7.1 Scope

- Educational and academic research applications
- Endpoint security vulnerability assessment
- Physical access attack vector demonstration
- Security awareness training scenarios
- Red-team and blue-team exercise support

2.7.2 Limitations

- No zero-day vulnerability exploitation
- No real user data collection or persistence
- Restricted to isolated laboratory environments
- Requires physical access to target systems
- Limited to HID-based attack vectors (no network exploitation)

2.8 Expected Outcomes

- **Functional Prototype:** Working hardware-assisted penetration testing device with documented capabilities
- **Payload Library:** Collection of ethical, sandboxed attack scripts covering common HID attack scenarios
- **Vulnerability Report:** Comprehensive analysis of identified security gaps in endpoint protection mechanisms
- **Defense Recommendations:** Actionable mitigation strategies including USB port policies, device control software, and monitoring solutions
- **Academic Contribution:** Research documentation and methodology suitable for publication and further study

3 Related Work

Table 1: Relevant Literature on Hardware-Assisted Security Testing and Attack Simulation

S. No	Title	Publication Name	Author(s)	Year
1	Hardware-Assisted Penetration Testing Techniques	IEEE Access	A. Kumar et al.	2022
2	USB HID Attacks and Mitigation Strategies	IEEE Security & Privacy	J. Smith et al.	2023
3	Red-Team Automation Using Embedded Devices	Springer – Cybersecurity Journal	M. Chen et al.	2023
4	Physical Access Attacks in Modern Enterprise Systems	ScienceDirect – Computers & Security	R. Anderson et al.	2022
5	Endpoint Security Challenges Against Peripheral Attacks	IEEE Access	L. Brown et al.	2024
6	Ethical Considerations in Hardware-Based Security Testing	Springer – Journal of Information Security	S. Patel et al.	2024
7	IoT-Based Cybersecurity Testing Frameworks	IEEE Internet of Things Journal	K. Lee et al.	2023
8	Attack Simulation for Cyber Defense Training	ScienceDirect – Future Generation Computer Systems	T. Nguyen et al.	2024
9	Red-Team and Blue-Team Methodologies in Education	IEEE Transactions on Education	D. Wilson et al.	2025
10	Threat Modeling of Physical Attack Surfaces	arXiv	P. Rodriguez et al.	2025

4 Literature Review

Recent advancements in cybersecurity research emphasize that modern attack surfaces extend beyond software vulnerabilities to include hardware-assisted and physical access–based attacks. Traditional penetration testing tools primarily focus on network, application, and operating system vulnerabilities, leaving a significant gap in addressing threats arising from peripheral devices and human interface devices (HID). The reviewed literature highlights the increasing relevance of such attack vectors and the need for controlled, ethical evaluation frameworks.

4.1 Hardware-Assisted Penetration Testing

Studies published in IEEE Access (2022, 2024) demonstrate that hardware-assisted penetration testing techniques provide more realistic threat modeling when compared to software-only approaches. These works highlight how embedded devices can be leveraged to emulate user behavior and execute automated attack sequences, revealing vulnerabilities that are often undetected by conventional security tools.

4.2 USB HID-Based Attack Vectors

Research in IEEE Security & Privacy (2023) extensively discusses USB HID-based attacks, explaining how malicious peripherals can bypass endpoint protection systems by masquerading as trusted input devices. The authors emphasize mitigation strategies such as device whitelisting and behavioral monitoring, indicating the importance of understanding these attack mechanisms for defensive system design.

4.3 Red-Team Automation

Springer's Cybersecurity Journal (2023) explores red-team automation using embedded platforms, showcasing the effectiveness of low-power microcontroller-based devices in executing repeatable attack simulations. These studies support the feasibility of using embedded systems for penetration testing while also stressing the need for ethical controls and academic accountability.

4.4 Physical Access Attacks in Enterprise Environments

Publications in ScienceDirect – Computers & Security (2022) analyze physical access attacks in enterprise environments and reveal that organizations often underestimate risks associated with unauthorized peripheral access. The findings underline that even well-secured systems can be compromised if physical attack vectors are ignored, reinforcing the motivation for hardware-assisted testing frameworks.

4.5 Endpoint Security Challenges

Further research from IEEE Access (2024) examines endpoint security challenges related to peripheral-based attacks and concludes that existing endpoint detection systems are insufficient against HID emulation threats. This gap motivates the development of educational and research-driven frameworks that allow safe exploration of such vulnerabilities.

4.6 Ethical Considerations in Security Testing

Ethical considerations play a crucial role in hardware-based security testing. Studies published in Springer – Journal of Information Security (2024) stress the importance of conducting penetration testing within legal and ethical boundaries. These works advocate for sandboxed environments, controlled payload execution, and transparent reporting—principles that directly influence the design philosophy of the proposed project.

4.7 IoT-Based Security Testing Frameworks

Research in the IEEE Internet of Things Journal (2023) discusses IoT-based cybersecurity testing frameworks, highlighting how embedded devices can act as both attack simulators and monitoring tools. These findings validate the use of ESP32-class devices in security research and academic environments.

4.8 Attack Simulation for Defense Training

Studies from ScienceDirect – Future Generation Computer Systems (2024) focus on attack simulation for cyber defense training. The authors demonstrate that simulated attack environments significantly improve defensive readiness when compared to theoretical learning alone. This supports the educational value of the proposed project.

4.9 Educational Integration of Red-Team and Blue-Team Methods

Educational research published in IEEE Transactions on Education (2025) emphasizes the effectiveness of integrating red-team and blue-team methodologies into cybersecurity curricula. The literature confirms that hands-on, controlled attack simulations enhance student understanding of security concepts.

4.10 Threat Modeling of Physical Attack Surfaces

Finally, recent arXiv (2025) studies on threat modeling of physical attack surfaces provide structured methodologies for analyzing hardware-based risks. These models reinforce the importance of systematic analysis and modular design in penetration testing frameworks.