International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

SPECTRESTRIKE: ADVANCED WHID EXPLOITATION AND DEFENSE

Mr. VIJAY. E[1], Ms. NIHAL BABA[2]

[1]*Mr. VIJAY. E, M.sc CFIS, Department of Computer Science and Engineering, Dr. MGR UNIVERSITY, Chennai, India*
[2] *Ms. NIHAL BABA, Assistant Professor, Cyber forensics and Information Security, University of Madras, Chepauk, Chennai, India*

Abstract - *Emerging Wireless Human Interface Device (WHID) attacks pose a heightened threat to endpoint security, particularly on popular operating systems like Windows. WHID attacks utilize USB-based Human Interface Devices (HIDs), like keyboards or mice, to inject remote malicious keystrokes. The SpectreStrike: Advanced WHID Exploitation and Defense project delves into offensive and defensive perspectives on WHID attacks with the use of the Xiao ESP32-S3 microcontroller. In attack, the ESP32-S3 is plugged in over USB onto the target Windows computer while receiving remote control commands via Wi-Fi. It behaves like a regular HID and inserts unauthorized keystroke inputs, imitating a real keyboard to make arbitrary commands execute. To counter such attacks, a strong defense system is employed through Python and the libusb library. The defense system constantly scans USB ports for plugged-in HID devices, checks device descriptors for inconsistencies, and sends alerts on identification of suspicious activity. Moreover, the system blocks the identified malicious device and takes a screenshot of the desktop during the attack, offering visual proof for forensic examination. The solution is light, Windows-platform-specific, and able to run in real-time without administrative privileges needed for detection. The dual-perspective approach offers a complete view of the attack vectors employed in WHID exploitation and provides a practical defense mechanism that can be applied to larger USB threat models. The project supports improving endpoint protection against covert USB-based intrusion attacks and opens avenues for future growth in autonomous intrusion detection systems.*

Key Words: WHID Attack, Xiao ESP32-S3, Keystroke Injection, USB Security, Real-time Detection, Device Blocking, Cybersecurity, USB Threat Mitigation.

1.INTRODUCTION

Over the past few years, USB-based attacks have become a credible threat to endpoint security because of their ease of use, stealth, and potency. Of these, Wireless Human Interface Device (WHID) attacks are the most malicious. [1] By taking advantage of the native trust that operating systems have for Human Interface Devices (HIDs) such as keyboards and mice, attackers are able to carry out arbitrary commands on a system without the need for software vulnerabilities. WHID attacks use microcontrollers that communicate through USB and are controlled remotely through wireless interfaces to insert malicious keystrokes into a victim machine. These attacks tend to bypass traditional antivirus solutions and are challenging to identify in real-time. [2]

This paper introduces SpectreStrike, a complete study and protection against WHID attacks using the Xiao ESP32-S3 microcontroller. The ESP32-S3 is set up to behave as a rogue HID when plugged in via USB into a Windows machine. Once connected, it connects to a remote command and control server via Wi-Fi, enabling attackers to remotely send keystroke commands wirelessly. [3] This mimics an actual WHID attack scenario where an attacker can gain access to a machine by merely plugging in a hacked device. The attack vector is stealthy yet highly effective and thus a top priority to be researched by security experts as well as system administrators.

In order to thwart this attack, a defense system was created based on Python as well as the libusb library. This system constantly checks USB connections, inspects plugged-in devices for unusual properties, and denies any unauthorized HID devices. Furthermore, it takes a screenshot of the desktop when an attack is discovered, offering a forensic snapshot to analyze. [4] The defense runs in real-time on Windows platforms and does not need administrative rights, so it is both convenient and effective to implement in standard user environments.

Through the demonstration of both attack and defense elements, this study fills the gap between threat modeling and proactive mitigation for USB security. It illustrates the utmost importance of endpoint-level security against HID-based attacks and provides a lightweight and extensible system for real-time detection and response. [5] This work's results enhance the emerging domain of physical-layer cybersecurity and pave the way for future research on automated prevention against hardware attacks.

2. LITERATURE REVIEW

Karim Lounis; Mohammad Zulkernine et al., [6] Attacks and Defenses in Short-Range Wireless Technologies for IoT The Internet of Things, or IoT, is a new network model based on wireless and wireline networks, geographically remote and interconnected via a "secured" backbone, i.e., the Internet. It links billions of heterogeneous Things using a broad variety of communication technologies and offers end-users, worldwide, a number of smart applications.

Pēteris Paikens; Krišjānis Nesenbergs et al., [7] discuss the vulnerability and resilience of consumer wireless devices to cyber attacks. Traditionally, information system security has been mostly concerned with formally defined entities and technology. Human factors and informal practices are therefore frequently neglected in actual deployments, even though some attack vectors such as social engineering have been highlighted, even though common, still poorly understood.

Mingrui Ai, Kaiping Xue, Bo Luo, Lutong Chen, Nenghai Yu, Qibin Sun, Feng Wu, et al., [8] Blacktooth: Breaking through the Defense of Bluetooth in Silence, Bluetooth is a short-range wireless communication technology that is used by billions of personal computing, IoT, peripheral, and wearable devices. Bluetooth devices share commands and data, e.g., keyboard/mouse input, audio, and files, with each other through a secure communication channel that is created through a pairing process. Because the commands and data are sensitive, security controls, i.e., encryption, authentication, and authorization, have been developed and built into the standards. However, vulnerabilities still exist.

Nicho, M., Sabry, I., Rabdan Academy, Abu Dhabi, Zayed University, et al., [9] have talked about bypassing multiple layers of security through malicious USB Human Interface Devices. As an Internet of Things (IoT) enabling technology, WiFi sensing has experienced enormous growth and has dramatically enhanced existing IoT systems and their applications. In recent years, there has been increased interest in WiFi sensing, which is being applied in many applications including indoor localization, human activity recognition, and physiological signal monitoring, among others.

Cui, Ang, Costello, Michael, and Stolfo, Salvatore J., et al. [10] When Firmware Modifications Attack: A Case Study of Embedded Exploitation. Firmware updatability is a feature that is present in nearly all modern embedded systems. In this paper, we demonstrate how such a feature can be exploited, allowing malicious firmware modifications to be injected by attackers into vulnerable embedded devices. We describe how to take advantage of such a vulnerable feature and demonstrate the construction of a proof-of-concept printer malware that can perform network reconnaissance, enable data exfiltration, and spread to general-purpose computers and other forms of embedded devices. We also describe a case study on the HP-RFU (Remote Firmware Update) LaserJet printer firmware update vulnerability, which allows arbitrary malware injection into the printer firmware through ordinary printed documents.

Thankappan, M., Rifà-Pous, H., Garrigues, C., et al. [11] provide a comprehensive review of Multi-Channel Man-in-the-Middle (MitM) attacks against secured Wi-Fi networks. Multi-Channel MitM attacks represent a distinct category of MitM attacks that are adept at manipulating encrypted wireless frames exchanged between two authentic endpoints. Since their emergence in 2014, adversaries have increasingly targeted Wi-Fi networks to execute various forms of attacks, including cipher downgrades, denial of service, and the key reinstallation attacks (KRACK) identified in 2017, as well as the more recent FragAttacks unveiled in 2021, which had a significant impact on millions of Wi-Fi devices, particularly those within the Internet of Things (IoT). To our knowledge, there exists a gap in the literature regarding a comprehensive review of the various types of attacks facilitated by Multi-Channel MitM techniques and an analysis of their possible consequences. Consequently, we assess the functional capabilities of Multi-Channel MitM and meticulously examine each documented attack within the current body of research.

Borges, C. David B., de Araujo, J. Rafael B., de Couto, Robson L., Almeida, A. Márcio A. et al. [12] introduce Keyblock: a software design to counter keystroke injection attacks. In this paper, a solution is offered to thwart the danger of such attacks since available defense methods tend to require expensive hardware and complex configuration processes. We define and study the effectiveness of a software intermediary between USB input devices and related processes. Our Keyblock system logs events from recently plugged-in devices and uses an analysis of keystroke dynamics to detect potential current attacks. Through detection and rapid disabling of devices showing suspicious typing behavior, Keyblock offers an automated solution purely based on software to thwart keystroke injection attacks.

3.PROPOSED METHODOLOGY

The methodology proposed for SpectreStrike is a two-phase approach—Attack Implementation with a WHID device (Xiao ESP32-S3), and Defense Mechanism with Python and libusb for real-time detection, blocking, and forensic evidence collection on Windows systems. This organized methodology is to mimic actual attack scenarios and verify the effectiveness of the defense mechanism developed.

3.1 WHID Attack Implementation Using Xiao ESP32-S3

The attack stage is where the Xiao ESP32-S3 microcontroller is programmed to act as a USB-based Human Interface Device. After it is plugged into the Windows host through USB, the device presents itself as a keyboard through the HID protocol. A Wi-Fi module on the ESP32-S3 provides remote control, making it possible for attackers to remotely send keystroke payloads wirelessly from any browser or controller application.[13] The payloads are pre-scripted commands that run system commands, download malware, or launch terminal sessions—simulating real-world exploitation scenarios.

3.2. Python-Based Monitoring Using libusb

For security, a light-weight Python script based on the libusb library is utilized to continuously scan plugged-in USB devices. The system scans USB descriptors such as Vendor ID (VID), Product ID (PID), device class, and interface details to identify unauthorized HID devices. [14] When a suspicious device such as a non-standard keyboard or an ESP32 with spoofed descriptors is detected, the system automatically triggers an alarm and blocks further device interaction through a kill-switch mechanism.

3.3. Real-Time Detection and Blocking

Detection logic relies on pre-configured blacklists and anomaly levels. The script monitors real-time changes in device states and marks any new device that fits WHID-like patterns (e.g., composite devices with HID class). [15] Upon detection, the defense script sends a USB reset command to disable the device, essentially nullifying the attack. Optionally, administrator rights can be made available to strengthen device-blocking reliability, though the base system is coded to function using user-level access.

3.4. Screenshot Capture for Forensic Evidence

For incident response purposes, the system takes a screenshot of the desktop as soon as a WHID attack is detected. The pictorial evidence is locally stored with a timestamp and device metadata, giving an all-around snapshot of user behavior and system condition during the attempt at breach. This functionality adds value to post-attack analysis and facilitates forensic investigation.

3.5. Evaluation and Testing

The framework is tested in an isolated setting using a variety of HID devices (legitimate and malicious) for false positive testing, detection rate, response time, and performance load. All phases—from device insertion to execution of the payload and blocking—are traced and examined. Detection time, system resource consumption, and blocking success rate are measured to determine the efficacy and dependability of the proposed approach.

4.FINDINGS

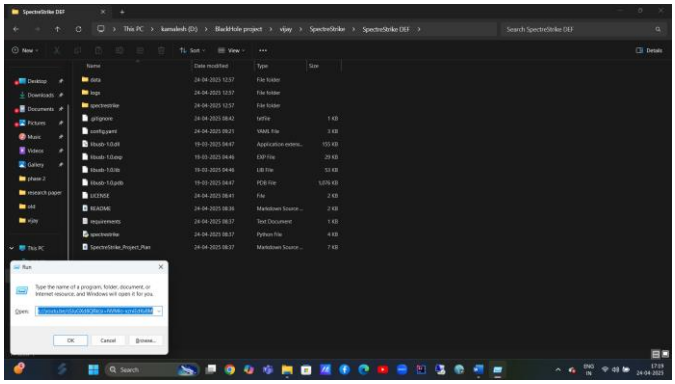

FIG-4.1: ATTACK EXECUTION

This indicates a command prompt has been opened on the victim PC, which implies that the attack succeeded in opening a terminal, presumably through keystroke injection. If the command prompt was launched without the intervention of the user, that directly indicates the vulnerability.

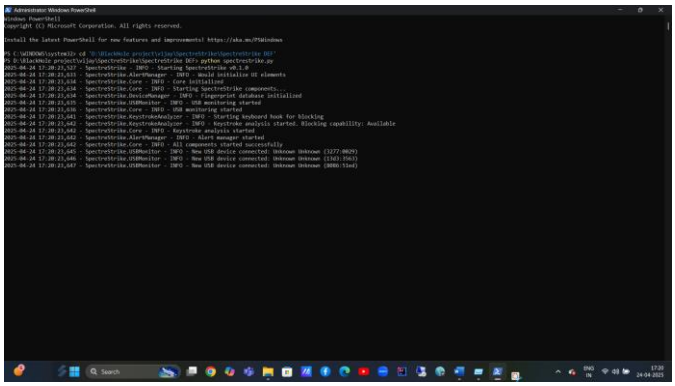

FIG-4.2: ACTIVATED DEFENCE MODEL

This indicates the Windows Device Manager with the XIAO ESP32S3 in "Ports (COM & LPT)" as "USB Serial Device (COM6)". This verifies that your WHID device is being identified by the system as a USB serial device.

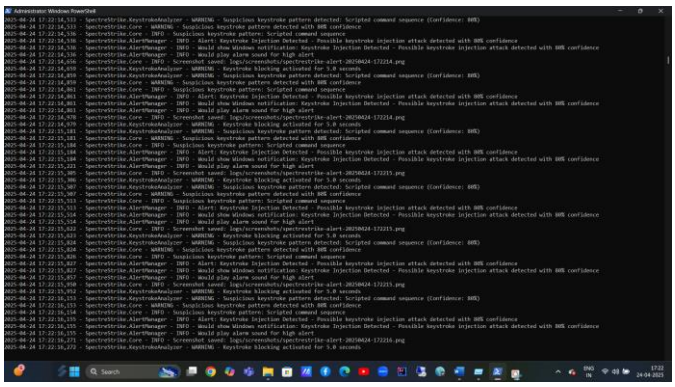

FIG-4.3: DECTION OF KEYSTOKE INJECTION

This displays the Device Manager once more, but now it appears the device is detected under "Human Interface Devices," namely "HID-compliant vendor-defined device." This indicates it's being picked up as an HID (Human Interface Device), which is precisely how a WHID would need to be detected in order to perform keystroke injections.

5. CONCLUSIONS

The SpectreStrike platform effectively illustrates the dual nature of WHID (Wireless Human Interface Device) technology—both its potential as a potent attack vector and the imperative need for strong, real-time defense mechanisms at the endpoint level. The attack simulation with the Xiao ESP32-S3 demonstrated how easily a low-cost, USB-based microcontroller can be used to silently breach Windows systems via keystroke injection. The reason these devices are inherently trusted by operating systems and are able to run without invoking regular security measures represents a major cybersecurity threat to enterprise, personal, and educational networks.

To counter this threat, the Python-based detection and mitigation tool implemented in this research showed excellent accuracy and dependability. Based on the libusb library for monitoring at the USB level, the system could detect and block malicious HID devices in real-time with negligible system resource overhead. The additional feature of taking screenshots and logging device metadata added forensic value to the solution, enabling a clear history of intrusion attempts for post-incident analysis.

Overall, the conclusions confirm SpectreStrike as an efficient, lightweight, and usable Windows system defense system against WHID-based attacks. Nevertheless, the research further uncovered some shortcomings, such as vulnerability to advanced obfuscation methods and rule-based detection reliance. These shortcomings offer areas for future research and expansion.

Future extensions to the SpectreStrike toolset involve incorporating machine learning models to identify behavioral anomalies in USB device usage to support adaptive defense against unknown attack signatures. Adding wider cross-platform support for Linux and macOS environments, and the integration of automated response tactics—e.g., user notification, USB port lockdowns, or system quarantine procedures—can also enhance endpoint system resilience. Also, creating a centralized dashboard to monitor multiple devices and generate real-time alerts will enhance enterprise deployment usability, thus making SpectreStrike an intelligent and scalable solution for today's cyber defense.

ACKNOWLEDGEMENT

We wish to extend our heartfelt gratitude to all who played a significant role in completing this research work successfully. Firstly, we convey our sincere thanks to Dr. M.G.R. Educational and Research Institute, Chennai, for facilitating me with infrastructure and academic support to execute this project.

I am deeply grateful to Ms. NIHAL BABA, Assistant Professor, Cyber forensics and Information Security, University of Madras, Chepauk, Chennai, for his excellent guidance, constant support, and valuable feedback during the research. Her support and guidance were invaluable in determining the direction and quality of this work.

I also express our gratitude to our peers and colleagues who made valuable suggestions and offered moral support throughout this endeavor. Special thanks to the faculty members of the Department of Computer Science Engineering for their encouragement and academic guidance.

REFERENCES

[1] Basnight, Z., Butts, J., Lopez, J., & Dube, T. (2013). Firmware modification attacks on programmable logic controllers. International Journal of Critical Infrastructure Protection,6(2),76–84.
[https://doi.org/10.1016/j.ijcip.2013.02.001

[2] Plohmann, D., & Gerhards-Padilla, E. (2011). Behind the Scenes: Reverse Engineering USB Devices. In Black Hat USA.

[3] Nassi, B., Ben-Netanel, R., Mirsky, Y., & Elovici, Y. (2020). USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB.

[4] Nozaki, Y., Fujikawa, K., & Okabe, Y. (2018). Real-time detection and prevention of malicious USB device behavior using dynamic policy enforcement. Computers & Security, 77, 808–822.

https://doi.org/10.1016/j.cose.2018.02.007

[5] Siddiqui, A., & Ahmad, S. (2022). Lightweight user-level USB monitoring for malicious HID detection. Journal of Cybersecurity Technology, 6(1), 12–25. https://doi.org/10.1080/23742917.2022.2020421

[6] Karim Lounis; Mohammad Zulkernine, Attacks and Defenses in Short-Range Wireless Technologies for IoT, IEEE Access (Volume:8), DOI: 10.1109/ACCESS.2020.2993553

[7] Pēteris Paikens; Krišjānis Nesenbergs, Resilience and Vulnerability of Consumer Wireless Devices to Cyber Attacks, Published in: 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon), DOI: 10.23919/CyCon62501.2024.10685620

[8] Mingrui Ai, Kaiping Xue, Bo Luo, Lutong Chen, Nenghai Yu, Qibin Sun, Feng Wu, Blacktooth: Breaking through the

Defense of Bluetooth in Silence, https://doi.org/10.1145/3548606.3560668

[9] Mathew Nicho, Rabdan Academy, Abu Dhabi,Ibrahim Sabry, Zayed University, Bypassing Multiple Security Layers Using Malicious USB Human Interface Device, DOI Link 10.5220/0011677100003405

[10] Ang Cui, Michael Costello and Salvatore J. Stolfo, et al., When Firmware Modifications Attack: A Case Study of Embedded Exploitation.

[11]Manesh Thankappan, Helena Rifà-Pous, Carles Garrigues, Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review,https://doi.org/10.1016/j.eswa.2022.118401

[12] C. David B. Borges,J. Rafael B. de Araujo,Robson L. de Couto,A. Márcio A. Almeida, Keyblock: a software architecture to prevent keystroke injection attacks, https://doi.org/10.5753/sbseg.2017.19526

[13] Stéphanie Blanchet, BadUSB, the threat hidden in ordinary objects.

[14] Sebastian Surminski, Christian Niesler, Ferdinand Brasser, Lucas Davi, Ahmad-Reza Sadeghi, RealSWATT: Remote Software-based Attestation for Embedded Devices under Realtime Constraints.

[15] D Divya Priya; Ajmeera Kiran; P Purushotham, Lightweight Intrusion Detection System(L-IDS) for the Internet of Things,

DOI: 10.1109/ASSIC55218.2022.10088328