Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 16, Issue, 02, pp. 13520-13523, February, 2025

RESEARCH ARTICLE

HID ATTACK PREVENTION & MITIGATION

***Mohd Avaish Khan, Aniket Gupta and Srivaramangai R**

University Department of Information Technology University of Mumbai, Vidya Nagari, Kalina, Santacruz East, Mumbai, Maharashtra 400098, India

ARTICLE INFO

Article History:
Received 10th December, 2024
Received in revised form
14th January, 2025
Accepted 26th January 2025
Published online 27th February, 2025

Keywords:

HID Attacks, Human Interface Device Security, Bad USB, Endpoint security, USB Authentication Mechanism, Malicious USB devices, Physical layer Attacks.

ABSTRACT

HID attacks have gradually made up as one of the major cyberspace threats that currently exist as far as current exploitations by decent operating systems are concerned, intended only for trusting USB devices. The attacks included the use of compromised USB devices for payload delivery using applications such as BadUSB and Rubber Ducky in commands to avoid security mechanisms and gain unauthorized access to the system's mechanisms. This survey paper reviews comprehensive literature related to HID attacks, covering various attack techniques, detection methods, and mitigation strategies proposed by different researchers. It has been found that most traditional security solutions such as antivirus applications and endpoint protection solutions fail to identify any HID-based threats as these execute at the hardware level. Many research efforts were made toward developing machine learning-based detection mechanisms, cryptographic authentication, and solutions to develop the hardware security subsystem to fight against such attacks. However, the attackers always change their tactics, so there must be a strategy of multi-layered defense consisting of appropriate real-time monitoring, enforcement of policies, and user awareness training. It also discusses several gaps that nations still have in HID attack mitigation and most importantly, future work in adaptive and proactive security measures research.

Citation: ***Mohd Avaish Khan, Aniket Gupta and Srivaramangai R.*** **2025.** "HID Attack Prevention & Mitigation", *Asian Journal of Science and Technology*, 16, (02), 13520-13523.

INTRODUCTION

Trained on data entirely up to October 2023. Some recent times are the emergence of Human Interface Device (HID) attacks which lead to much damage over the security of the country. This kind of attack uses the inherent trust of an operating system in USB devices and demonstrates how attackers can bypass security measures and take command of a system to run malicious payloads. There are many malicious peripherals atop physical devices such as keyboards or mice that will impersonate any one of them to deliver keystroke injection attacks, launch backdoors and exfiltrate sensitive data. Compared to traditional malware, they are quite different because traces of their actions do not consistently find themselves under popular antivirus systems: thus, a nightmare for people and organizations in general. The heavy reliance on USB peripherals all across critical infrastructures and enterprise environments, as well as across personal ends, deepens the growing risk of HID-based cyber threats. Social engineering, supply chain compromises, and rogue USB devices have become some of the means by which hackers could penetrate their target systems. Once connected, those devices can initiate self-execution for malicious script running, as well as change system settings, and grant permanent access to criminals on their own. This would be an extended literature survey on HID attacks providing different types of attack methods, detection mechanisms, and mitigation techniques. By reviewing existing research contributions, this study will be able to explain and analyze the rapidly changing scenario of HID-based cyber threats along with possible defense mechanisms such as machine learning-based anomaly detection, USB authorization frameworks, and hardware security enhancements. The research currently seeks to improve awareness about HID vulnerabilities and offer solutions toward stronger security systems to combat emerging USB-based attack vectors.

****Corresponding author: Mohd Avaish Khan***
University Department of Information Technology University of Mumbai, Vidya Nagari, Kalina, Santacruz East, Mumbai, Maharashtra 400098, India

LITERATURE SURVEY

The scope of literature survey looks at Bad USB attacks as HID and its mitigation techniques explored by Sankar E et al [1] (2023), which was published in the *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, Volume 11, Issue 4, in the year 2023. Bad USB exploits the firmware vulnerabilities of USB devices, so that a malicious payload gets executed without registering itself. Antivirus solutions are no longer able to detect this firmware-based attacks. They propose integrity verification with hashing and codesigning. Change system policies to require authentication from users for USB privilege escalation. Raspberry Pi Pico was used by them for a Bad USB simulation.Ali Hasan Munef et al.[2] (2020).introduced a system on Protection of Patient Information Records Monitoring System using USB-HID and PIC Microcontroller (PPIRMS).Published in *Test Engineering and Management* in 2020, their PPIRMS system uses USB-HID and a PIC microcontroller to authenticate and securely transfer patient data using the ID and password in order to avoid unauthorized access. The outcome of the simulation experiments shows great accuracy and security. They used USB-HID for the secure transfer of data and a PIC18F4550

microcontroller for processing and housing the data. José Oliveira et al[3] (2018) presented System Protection Agent against some Unauthorized Activities through USB Devices, which is detected-and-prevented-BadUSB-attack protective against Windows OS agents by blocking device installation on the registry and controlling driver installations. They had used many USB devices for detector and all attacks proven successful using HID keyboard and BadUSB Man-in-the-middle attacks. Registry manipulation was used to block the automatic installation of the driver while WMI was for managing device data. Kyle Denney et al[4] (2019) researched the concept of dynamic detection of USB attacks in hardware. Static typing dynamic analyses keystroke injection for detecting attack types. Their poster shows that may put feature-based machine-learning classifiers to detect malicious devices with decent effectiveness. Done with hardware-based USB data collection and machine-learning classification. Matthias Neugschwandtner et al[5]*UScramBle*, which is a transparent defense against USB eavesdropping attacks. As presented at *EUROSEC'16*, UScramBle is lightweight encryption solution, which is transparent to user, back-compatible with legacy devices and involves little overhead in terms of performance degradation. UScramBle is implemented with AES-CTR encryption. Ferdous A. Barbhuiya et al[6] (2015) proposed an anomaly-based approach for HID attack detection using keystroke dynamics. Their system is not tied to any particular platform and operates over any device while achieving a 0% false acceptance rate for attack detection.

They used keystroke dynamics based anomaly detection. Ferryansa et al[7](2025) appertained a study using an Arduino-based spying technique and the Metasploit Framework in a Windows Operating System. This paper demonstrated, in 2025, the fact that spying through USB could be achieved using the Arduino Pro Micro (Leonardo) and Metasploit Framework for Windows 10 systems at an 83% success ratio. They used a reverse shell backdoor planting and Powershell commands for security bypass. Novel payloads and novelties for detection mechanisms of USB Rubber Ducky payloads were investigated by Maaike Ellen van Vlietet et al[8](2024) in her Bachelor Thesis at the University of Zurich (2024). The thesis developed payloads for the O.MG cable and proposed an O.MG device's defense mechanism by their USB enumeration patterns in implementing a rate limiter to stop such attacks.overcoming the controls by the OS, group policy, and antivirus software harnessing simulation using a USB Rubber Ducky. PowerShell scripting was used for executing the malware and performing antivirus evasion techniques. Dave (Jing) Tian et al[10] (2015)*GoodUSB* is in fact a security framework that would mitigate the USB attack risk by enforcing permissions concerning what a user would expect to access. Presented at *ACSAC*, GoodUSB includes a security image component for user-friendly administration and a honeypot mechanism for profiling malicious USB devices. There used to be USB interface mediation and a user-driven device authentication concept. Koffi Anderson Koffi et al[11] (2024).

To (US)Be or Not to (US)Bethus presented a universal USB authentication system that detects and blots disgraced USB peripherals by figuring the pattern of power consumption. In *Electronics*, the system presents an Autoencoder model supported by CNN and LSTM for a perfect F1 score in ascertaining malicious USB devices from benign ones. Neural networks, Autoencoder, Long Short-Term Memory (LSTM), and Convolutional Neural Network (CNN) were involved.Rezky Aulia Efendy et al[12] (2019) researched the attack through a USB-based Fork Bomb against the Windows environment. The IEEE Conference Paper demonstrated how a Fork Bomb could be triggered through a USB flash drive, resulting in disproportionate memory consumption and crushing the system. They used Fork Bomb attack and USB Rubber Ducky.Isaac Yaw Fergusonet al[13] (2017) researched an aspect of social engineering as a cyber-attack channel. While at Halmstad University, he discovered that people tend to plug in USB drives that they find lying about or unknown drives, making organizations prone to cyber threats. They conducted Social Engineering (USB baiting) baiting. Federico Griscioliet al [14](2021) presented *USBCaptchaIn*, a hardware-based mechanism for security that protects ICS (Industrial Control Systems) from attacks that use USB malware and BadUSB. This system, published in the *Journal of Computer Security*, allowed the secure use of USB drives through a role of USB gatekeeper. They also employed Hardware-based USB authorization and Cryptographic integrity verification (Merkle Hash Trees).Stanford Open Virtual Assistant Labet al [15] investigated HID attack prevention using USBs below. Various attacks are discussed, and a multifaceted security approach is recommended, which includes education, endpoint security tools, device control policies, and machine-learning anomaly detection. They suggested Endpoint Security Solutions (EDR, antivirus) and USB Security Tools. Chia-Yu Huang et al [16] (2019) presented HIDTracker, a system that identifies HID-based attacks through the analysis of native host event logs using guilt-by-association analysis. Presented at ICCSP 2019, the approach achieves a 90% precision rate with a 2.33% false positive rate. They did Guilt-by-Association (GBA) Analysis for event correlation. Annisa Dwiayu et al [17] (2020) presented a research study in which they demonstrated USB keyboard Injection in Windows Operating Systems. The paper was published in the 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE).

Proceedings of ICOBI 2023: Various authors combined research together under the theme 'Accelerating Societal Change Through Digital Transformation'. This includes discussions about how technologies affect digitally reshaping industries and efficient operation processes through data-driven innovations. Use of AI in education, fintech, and sustainable tourism are some topics. Potocký et al [19] (2022): The authors analyze "The Human Interface Device Attack from the Perspective of the Attacker and the Forensic Analyst". They identify mitigations to bypass lock screen protections and explain very briefly possible forensic detection techniques which include HID attacks on Android devices. They use tools like Android Debug Bridge (ADB) and Metasploit framework for their analysis. Kharraz et al[20](2019). This work proposes USBESAFE, a machine learning-based system able to detect and mitigate BadUSB-style attacks with an impressive 95.7 percent true-positive rate besides just 0.21 percent false positives. Without changing USB protocols or needing users to perform any action, the system can analyze time and apply it to millions of USB packets. Mahboubi et al[21](2018): A lightweight authentication and delegation model has been designed based entirely on RFID technology to minimize threats from USB malware. Their model improves security in air-gapped networks by identifying USB devices infected with malware, which was done through simulation by utilizing Coloured Petri Nets (CPNs).Neuner et al [22] (2017): "Bad Things happen through USB" is a thesis basing its research upon reflashing attacks over USB that are basically related to the study of BadUSB. It provides detection mechanisms at both the levels of system as well as enterprise network, which are based upon large-scale data accumulations.Barankova et al[23] (2020): Their paper discusses methods of detecting passive hidden hardware USB-keyloggers and describes how to do that through the analysis of the electrical characteristics of keyboards with the help of a Raspberry Pi based detection device.

The study also shows that the measured power consumption patterns are quite drastically altered by keyloggers. Benadjila et a[24] (2018). This paper is a presentation of WooKey, an open-source designed device for USB mass storage that will counter USB-based security threats like BadUSB. It implements strong encryption, secure firmware updates, as well as two-factor authentication upon attack vectors. Bojović et al[25](2020). This study establishes an increasing threat from hardware edition attack through malicious USB devices that can carry out automated scripts and realize malware insertion. Hryhoruk N et al [26](2024) discusses USB drop attacks, a specific methodological means wherein the attackers drop USB drives in public places to deploy malware once connected by an unsuspecting user to his or her system. Pham et al [27] (2010) analyzes hack tools based on USB, including standard U3 applications, and identifies leading security threats introduced through these tools while suggesting countermeasures based on software restriction policy.

'HID Threat Vulnerability model' (HidTV) by Nicho and Sabryet al [28] (2022) maps malicious Human Interface Devices to categories of vulnerability according to their associated attack vectors, so that it can be used to formulate informed security policy recommendations. Arora and Thakur N et al [29].Their work is cryptic for "Ducky-Detector," which tries to prevent and detect malicious USB Rubber Ducky attacks through differentiating automated keystrokes from human keystrokes. Yang et al[30] (2018) demonstrates an attack on Tor via a malicious USB charging device, which will infer website visits purely based on power consumption patterns. Neuner et al [31] (2018) introduce "USBlock," a mechanism designed to detect and block injecting attacks on keypresses through USB by the examination of USB packet traffic for suspicious timing patterns. Denney K et al[32] (2020): This work recognizes USB-Watch, a hardware-assisted framework for detecting insider threats via USB devices, employing machine learning for anomaly detection with high accuracy. Kim et al[33] (2013) demonstrate how an attacker could avoid unique USB authentication by exploiting flaws in flash controllers of secure USB drives. Kumarage et al[34](2023).

Introduction of USB-Bouncer, a hardware-based solution to protect Windows PCs from different USB-based attacks as an intermediary between USB devices and the PC. A rate limiter is independent because it holds two modalities which measure Interarrival Time Analysis and Time Window Analysis. Bypassing multiple security layers using malicious USB Human Interface Device is shown by Mathew Nicho et al [9] (2023). This paper presented at *ICISSP 2023 - 9th International Conference on Information Systems Security and Privacy*, focused on the feasibility of USB-based attacks in Observations. In the context of a literature survey on HID (Human Interface Device) attacks, it presents some highlights about the methodologies of attack, detection techniques, and mitigation strategies. One of the major findings is that, in HID attacks, the implicit trust that operating systems on USB devices can be deeply exploited and therefore allow the attacking party to inject keystrokes, run malicious scripts, and compromise the system security without triggering the traditional antivirus defenses. Researchers have demonstrated that the tangible tools used like BadUSB, Rubber Ducky, and O.MG cables are weaponized to bypass security layers, thus lending more emphasis to the increasing sophistication of reckoning these attacks. Another major finding is that there exists a wide array of detection and mitigation techniques proposed against these attacks. Numerous studies were concentrated on machine learning-based detection mechanisms, which include analyses of keystroke dynamics, power consumption patterns, and device enumeration behaviors. Such approaches were found to increasingly give good results in separating legitimate HID devices from malicious ones. Other proposed solutions include hardware-based ones, like providing cryptographic authentication and USB gatekeeping mechanisms to avert unauthorized USB interaction.Despite some strides in HID-based attack detection, one of the fundamental challenges is the evolving nature of the attackers. This evolution in plans and techniques by the adversaries makes it increasingly impossible to propose an answer that fits all situations, where each and every answering mechanism would prove useful. The survey views it as quite essential for the defense against HID-based threats to have multi-layered security that would consist of endpoint security tools, user awareness training, and stricter USB access policy compliance.While many mitigation strategies exist, there is no single solution that guarantees full protection against HID attacks. Ongoing research needs to focus on quickly outpacing evolving threats, particularly through AI-driven anomaly detection, real-time monitoring, and tougher enforcement of USB security protocols.

CONCLUSION

HID, or Human Interface Device, attacks may very well be the most dangerous types of attacks on cybersecurity because such attacks could easily circumvent all security measurements by appearing as a legitimate input device. Such attacks are carried out through exploiting the embedded trust mechanism in USB devices to perform unauthorized commands on a computer, injecting harmful scripts, and compromising the integrity of the system. The final literature survey examined various methodologies on HDI attacks, BadUSB, and Rubber Ducky or O.MG cable exploits, as well as advanced detection and mitigation strategies.Although there have been numerous research efforts that proposed different solutions such as USB authorization frameworks, keystroke anomaly detection, and hardware-based authentication mechanisms, it has been seen that HID attacks are continuously evolving and pose a perpetual threat. Machine-learning techniques and solutions for real-time monitoring have proved to be promising in detecting and preventing unauthorized USB device activities. Still, it is essential that a comprehensive security approach integrating endpoint detection and response (EDR), user awareness, and policy enforcement should be enforced to thwart these threats effectively.Future work should delve into the development of more adaptable and proactive defense mechanisms that have AI-enabled threat detection and enforce stricter USB secure policies at both hardware and software levels. Since process techniques pertaining to HID attack are continually advanced, action monitoring, improved forensic analysis, and tighter regulations will be instrumental in averting sophisticated threats to digital environments.

REFERENCES

Ali Hasan Munef, Rosilah Hassan, Mohammed Dauwed, Azizah Ya'acob: "Protection of Patient Information Records Monitoring System through USB-HID and PIC Microcontroller (PPIRMS)," *Test Engineering and Management*, vol. 83, 2020, pp. 1725-1735[1].

Annisa Dwiayu Ramadhanty, Avon Budiono, Ahmad Almaarif: "Implementation and Analysis of Keyboard Injection Attack using USB Devices in Windows Operating System," *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, 2020, pp. 449-454[1].

Arora, L., Thakur, N., & Yadav, S. K. (2021). USB Rubber Ducky Detection by Using Heuristic Rules. *2021 International Conference on Computing, Communication, and Intelligent Systems* (ICCCIS).

Barankova, I. I., Mikhailova, U. V., & Lukyanov, G. I. (2020). Software Development and Hardware Means of Hidden USB-Keylogger Devices Identification. *Journal of Physics: Conference Series,* 1441(1), 6.

Benadjila, R., Renard, M., Trebuchet, P., Thierry, P., Michelizza, A., & Lefaure, J. (2018). WooKey: USB Devices Strike Back. SSTIC (Symposium sur la Sécurité des Technologies de l'Information et des Communications) 2018.

Bojović, P. D., Basicevic, I., et al. (2020). The Rising Threat of Hardware Attacks: USB Keyboard Attack Case Study.

Chia-Yu Huang, Hahn-Ming Lee, Jiunn-Chin Wang, Ching-Hao Mao: "Identifying HID-based Attacks through Process Event Graph Using Guilt-by-Association Analysis," *ICCSP 2019 (International Conference on Communication Software and Networks)*, 2019, pp. 273-278[1].

Dave (Jing) Tian, Adam Bates, Kevin Butler: "Defending Against Malicious USB Firmware with GoodUSB," *ACSAC (Annual Computer Security Applications Conference)*, 2015[1].

Denney K., Babun L., & Uluagac A.S.(2020). USB-Watch: A Generalized Hardware-Assisted Insider Threat Detection Framework.* Journal of Hardware and Systems Security*.

Federico Griscioli, Maurizio Pizzonia: "USBCaptchaIn: Preventing (un)conventional attacks from promiscuously used USB devices in industrial control systems," *Journal of Computer Security*, vol. 29, 2021[1].

Ferdous A. Barbhuiya, Tonmoy Saikia, Sukumar Nandi: "An Anomaly Based Approach for HID Attack Detection Using Keystroke Dynamics," 2015[1].

Ferryansa, Avon Budiono, Ahmad Almaarif: "Analysis of USB Based Spying Method Using Arduino and Metasploit Framework in Windows Operating System," 2025[1].

Hryhoruk, N. (2024). The USB Drop Attack's Threat to Security.

Isaac Yaw Ferguson:"The Effectiveness of Social Engineering as a Cyber-Attacking Vector: People Do Use Unknown USB Drive, They Find," Halmstad University - IT Forensic and Information Security Candidate Examination, 2017[1].

José Oliveira, Miguel Frade, Pedro Pinto: "System Protection Agent Against Unauthorized Activities via USB Devices," *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS)*, 2018[1].

Kharraz, A., Daley, B. L., Baker, G. Z., Robertson, W., & Kirda, E. (2019). USBESAFE: An End-Point Solution to Protect Against USB-Based Attacks. 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019), USENIX Association.

Kim J., Lee Y., Lee K., Jung T., Volokhov D., & Yim K.(2013). Vulnerability to Flash Controller for Secure USB Drives.* Journal of Internet Services and Information Security (JISIS)* 3(3/4), 136-145.

Koffi Anderson Koffi, Christos Smiliotopoulos, Constantinos Kolias, Georgios Kambourakis: "To (US)Be or Not to (US)Be: Discovering Malicious USB Peripherals through Neural Network-Driven Power Analysis," *Electronics*, vol. 13, no. 2117, 2024[1].

Kumarage T., Attanayake C., Bandara Nishshanka I.S.(2023). USB-Bouncer: A Hardware-Based Approach to Nullify Unknown USB Device-Based Attacks on Windows Machines.* Annual International Conference on Business Innovation (ICOBI) 2023*, 545-558

Kyle Denney, Enes Erdin, Leonardo Babun, A. Selcuk Uluagac: "POSTER: Dynamically Detecting USB Attacks in Hardware (Extended Abstract)," 2019[1].

Maaike Ellen van Vliet: "Novel USB Rubber Ducky Payloads and Detection Mechanisms," Bachelor Thesis, University of Zurich, 2024[1].

Mahboubi, A., Camtepe, S., & Morarji, H. (2018). Reducing USB Attack Surface: A Lightweight Authentication and Delegation Protocol. International Conference on Smart Computing and Electronic Enterprise (ICSCEE 2018), IEEE.

Mathew Nicho, Ibrahim Sabry: "Bypassing Multiple Security Layers Using Malicious USB Human Interface Device," *ICISSP 2023 - 9th International Conference on Information Systems Security and Privacy*, 2023[1].

Matthias Neugschwandtner, Anton Beitler, Anil Kurmus: "A Transparent Defense Against USB Eavesdropping Attacks," *EUROSEC'16*, 2016[1].

Neuner, S. (2017). Bad Things Happen through USB. Technische Universität Wien (Vienna University of Technology).

Neuner, S., Voyiatzis, A.G., Fotopoulos, S., Mulliner, C., & Weippl E.R.(2018). USBlock: Blocking USB-Based Keypress Injection Attacks.* DBSec 2018 (IFIP International Federation for Information Processing)*.

Nicho, M., & Sabry, I. (2022). Threat and Vulnerability Modelling of Malicious Human Interface Devices. The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 21, 241-247.

Pham, D. V., Syed, A., Mohammad, A., & Halgamuge, M. N. (2010). Threat Analysis of Portable Hack Tools from USB Storage Devices and Protection Solutions.

Potocký, S., & Stulrajter, J. (2022). The Human Interface Device Attack from the Perspective of the Attacker and the Forensic Analyst. NTSP 2022 Proceedings.

Rezky Aulia Efendy, Muhardi Saputra, Ahmad Almaarif, Warih Puspitasari, Avon Budiono, Edi Sutoyo: "Exploring the Possibility of USB-Based Fork Bomb Attack on Windows Environment," *IEEE Conference Paper*, 2019[1].

Sankar E, Megha Shyam Raju S, Sheshank Reddy K: "Bad USB as HID and Its Mitigations," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 11, no. 4, 2023, pp. 3685-3688[1].

Stanford University Open Virtual Assistant Lab: "HID Attack Prevention via USB," 2024[1].

Various authors (2023). ICOBI 2023 Proceedings - Volume I. NSBM Green University, Sri Lanka.

Yang, Q., Gasti, P., Balagani, K., Li, Y., & Zhou, G. (2018). USB Side-channel Attack on Tor.

****