 ISSN: **3107-6513**

USB Security Threats and Physical Access Vulnerabilities: A Comprehensive Review

Nachiket Sameer Patil[1],Yash bhoir[2], Sriniwas Narayanan Vengarai[3]

[1]M.S.(Cybersecurity),[2]M.S.(Cybersecurity)

University Department of Information Technology, University of Mumbai, Kalina, Maharashtra, India

[1]nachiket4748@gmail.com, [2] yashbhoir58@gmail.com, [3]Sriniwas.narayanan@mu.ac.in

***Abstract*—Universal Serial Bus (USB) devices are ubiquitous in modern computing, enabling convenient connectivity for data transfer, peripherals, and storage. However, USB devices also serve as effective gateways for cyber and cyber-physical attacks, including firmware manipulation, malware propagation, covert communication channels, and hardware-based exploits. Physical access vulnerabilities such as Direct Memory Access (DMA) attacks and peripheral manipulation further amplify these risks. This paper presents a comprehensive review of USB threats and physical access attacks, emphasizing techniques such as BadUSB, DMA exploitation, covert channels, and hardware Trojans. Mitigation strategies including device authentication, firmware verification, honeypots, access control policies, and employee awareness are discussed. Industry reports and real-world incidents demonstrate that an integrated technical and administrative security approach is essential to effectively securing modern computing and industrial systems.**

Keywords—USB Security; Physical Access Threats; BadUSB; DMA Attacks; Honeypots; Industrial Control Systems

I. INTRODUCTION

USB devices have become an essential component of modern computing environments, supporting tasks ranging from data storage to peripheral connectivity. Despite their operational convenience, USB devices introduce serious security risks due to their plug-and-play nature and deep integration with operating systems. Attackers can exploit USB firmware, peripheral interfaces, or power channels to compromise systems without relying on network access [4], [11].

Physical access threats further compound these risks. Even brief or indirect access to a system may allow adversaries to introduce malicious USB devices, exploit DMA-enabled ports, or manipulate hardware components to extract sensitive information [12], [13]. The convergence of cyber and physical attack vectors creates a complex and often underestimated threat landscape. This paper surveys USB-based attacks, physical access vulnerabilities, and mitigation techniques, providing a holistic view of USB security grounded in both academic research and industry experience.

II. RELATED WORK

USB security threats have been extensively explored in academic and industrial research. Behl and Behl [4] categorized USB attack vectors including firmware manipulation, malware delivery, and unauthorized peripheral impersonation. The BadUSB attack introduced by Nohl and Lell [11] demonstrated that USB firmware can be reprogrammed to execute malicious actions while remaining undetected by traditional security tools. Dumitru and Francillon [2] further revealed vulnerabilities in USB communication protocols through off-path injection attacks.

Covert communication channels using USB devices were demonstrated by Guri et al. [3] and Ibrahim et al. [1], proving that air-gapped systems can leak sensitive data through electromagnetic or magnetic emissions. Physical access threats such as DMA exploitation [12] and LED-based exfiltration [13] highlight how attackers bypass operating system protections entirely. Hardware-level attacks, including hardware Trojans embedded in USB flash drives, were analyzed by Skorobogatov [9], emphasizing the limitations of software-only defenses.

Industry reports corroborate these findings. Honeywell documented USB-borne malware incidents in industrial control systems [17], [18], often introduced through contractors or maintenance personnel. Kaspersky Lab [19] highlighted removable media risks in enterprise and healthcare environments. Collectively, these studies confirm that USB threats are both cyber and physical in nature and require comprehensive mitigation strategies.

III. USB THREAT ANALYSIS

A. Firmware-Based Attacks

Firmware manipulation represents one of the most dangerous USB threats. BadUSB attacks [11] allow a USB device to masquerade as a trusted peripheral such as a keyboard or network interface, enabling command execution or data exfiltration. Such attacks bypass traditional antivirus and endpoint protection mechanisms. Power analysis-based detection methods proposed by Conti and Pajola [7] offer promising techniques for identifying malicious firmware behavior.

B. Covert Channels

Covert channels exploit unconventional communication paths to bypass security controls. USB electromagnetic emission attacks such as USBee [3] and magnetic emission-based techniques like MAGNETO [1] demonstrate the feasibility of data exfiltration from air-gapped systems. Additionally, keyboard LED-based attacks [13] illustrate how seemingly benign peripherals can leak sensitive information without network connectivity.

C. Malware and Software Exploits

USB devices remain a significant vector for malware propagation. Prior studies [4]–[6] demonstrate how autorun features and backward compatibility across USB versions enable malware execution. DeSouza and Bailey [10] further highlighted systemic vulnerabilities in USB protocol evolution, increasing the attack surface across legacy and modern systems.

D. Physical Exploits

Physical access attacks such as DMA exploitation [12] bypass operating system security mechanisms entirely. Attacks like PoisonTap [16] can compromise locked systems via USB ports. Hardware Trojans embedded in USB devices [9] pose a persistent and stealthy threat. Social engineering techniques [14] often amplify these attacks by exploiting human trust and curiosity.

IV. COUNTERMEASURES AND MITIGATION

A. Technical Controls

Device authentication and fingerprinting techniques such as MAGNETO [1] help identify unauthorized USB devices. Firmware verification mechanisms prevent malicious reprogramming [11]. Strict access control and device usage policies reduce exposure, particularly in sensitive environments [19]. USB honeypots [8] and anomaly detection techniques using power analysis [7] enable early threat detection.

B. Administrative Controls

Employee awareness and training programs are critical in preventing social engineering-based USB attacks [8]. Physical access restrictions and controlled zones reduce opportunities for hardware manipulation [15]. Regular audits and monitoring of USB usage [17], [18] support compliance and early incident response. An integrated cyber-physical security framework is essential for holistic risk mitigation [15], [20].

V. CASE STUDIES AND INDUSTRY REPORTS

Honeywell reports [17], [18] document multiple incidents of USB-borne malware affecting industrial control systems, often introduced through third-party personnel. These cases highlight the importance of device monitoring and controlled media usage. Kaspersky Lab [19] reported similar risks across enterprise and healthcare sectors, emphasizing that technical controls alone are insufficient without strong policy enforcement and employee awareness.

VI. DISCUSSION

USB devices combine convenience with significant security risks. Firmware attacks, covert channels, malware, and physical exploits collectively expand the attack surface. While technical defenses such as detection and access control mitigate many threats, human behavior and physical security remain critical factors [3], [13], [17]. Even air-gapped systems are vulnerable, particularly to insider threats and covert communication channels. A layered defense strategy integrating technology, policy, and user awareness is essential.

VII. CONCLUSION

USB devices and physical access vulnerabilities pose serious threats to computing and industrial environments. Key risks include BadUSB attacks, covert channels, DMA exploitation, malware propagation, and hardware Trojans. Effective mitigation requires a combination of technical controls such as device authentication, firmware verification, and monitoring, along with administrative measures including employee training, physical access restrictions, and policy enforcement. Future research should focus on secure USB architectures, automated threat detection, and integrated cyber-physical security frameworks.

References

[1] O. A. Ibrahim, Y. Yona, and M. Guri, “MAGNETO: Fingerprinting USB Flash Drives via Unintentional Magnetic Emissions,” arXiv preprint, 2020.

[2] R. Dumitru and A. Francillon, “Off-Path Injection Attacks on USB Communications,” arXiv preprint, 2022.

[3] M. Guri, Y. Solewicz, and Y. Elovici, “USBee: Air-Gap Covert-Channel via Electromagnetic Emissions,” arXiv preprint, 2016.

[4] N. Behl and B. Behl, “USB-Based Attacks,” Computers & Security, vol. 70, pp. 675–688, 2017.

[5] R. Murugesan and R. Shanmugam, “Universal Serial Bus Based Software Attacks and Protection Solutions,” International Journal of Computer Applications, 2011.

[6] P. Patel and A. Shah, “A Literature Survey on USB Port Security Mechanisms and Malware,” International Journal of Innovative Research in Technology, 2019.

[7] M. Conti and L. Pajola, “Detecting Malicious USB Devices Using Power Analysis,” Electronics, 2023.

[8] K. Rieck and P. Laskov, “A Honeypot for Malware on USB Storage Devices,” in Proceedings of the RAID Conference, 2006.

[9] S. Skorobogatov, “Hardware Trojan Attacks on Secure USB Flash Drives,” IEEE Security & Privacy, vol. 17, no. 4, 2019.

[10] A. N. DeSouza and M. Bailey, “Understanding USB Insecurity Across Versions,” in Proceedings of the IEEE Symposium on Security and Privacy, 2018.

[11] S. Nohl and J. Lell, “BadUSB – On Accessories That Turn Evil,” Black Hat Conference, 2014.

ISSN: **3107-6513**

[12] J. Rutkowska, “DMA Attacks: Gaining Access Through Physical Ports,” Invisible Things Lab White Paper, 2012.

[13] M. Guri and D. Kedma, “Data Leakage from Air-Gapped Computers via Keyboard LEDs,” arXiv preprint, 2019.

[14] R. Heartfield and G. Loukas, “A Study of Social Engineering Attacks,” Information Security Journal, 2016.

[15] E. Cole and R. Krutz, Physical Security and Cybersecurity Convergence, Wiley, 2018.

[16] S. Gibson, “PoisonTap: Exploiting Locked Computers via USB,” Security Research Blog, 2016.

[17] Honeywell Cybersecurity Research Team, USB Threats in Industrial Control Systems, Honeywell Report, 2020.

[18] Honeywell Analytics, Industrial USB Cyber Threat Report, Honeywell, 2021.

[19] Kaspersky Lab Research Team, Cybersecurity Risks from Removable Media, Kaspersky Report, 2019.

[20] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Wiley, 2020.