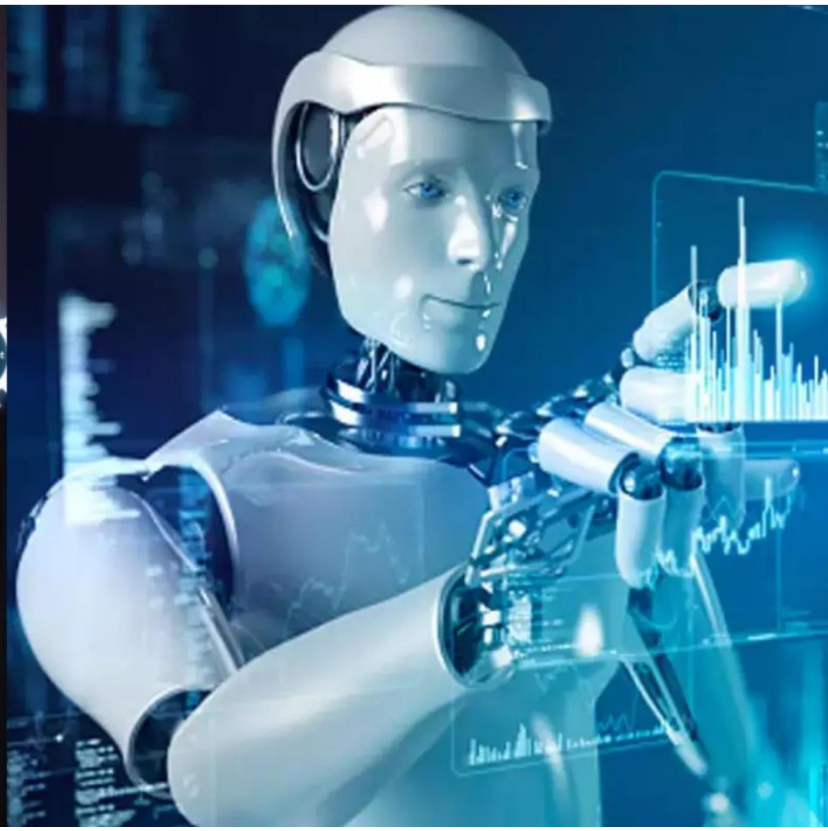
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 15, Issue 4, April 2026**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504043|

# Understanding USB-Based Hardware Attack Vectors: Security Risks and Defensive Mechanisms Against USB Rubber Ducky Attacks

**Keyur Kumbhani, . Dr. Himanshu Maniar**

Student, Bhagawan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

Asso. ProfBhagawan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, India

**ABSTRACT**: Universal Serial Bus (USB) devices have found widespread usage in today's computing systems [1]. However, despite the convenience and ease of usage, there is a high risk associated with the usage of these devices, owing to the implicit trust associated with the devices connected to the system [4]. The most commonly used device for carrying out cyber attacks is the USB Rubber Ducky, which was developed by Hak5 and works on the basis of emulating a Human Interface Device, such as a keyboard, and executing a set of pre-programmed keystrokes as soon as it is connected to the system [13]. As the system inherently trusts keyboard inputs, this device can carry out a range of malicious activities without being detected by the system's antivirus software [11].

This research paper focuses on hardware attack vectors through the use of USB devices. Specifically, it delves into HID-based keystroke injection attacks. The research paper discusses the architecture and operation of such attacks and their security risks. The security risks discussed include the deployment of malware, harvesting of credentials, and unauthorized access to systems [12]. The research paper also delves into the detection of such attacks and countermeasures such as endpoint monitoring and control policies and training users to be aware of such attacks [8]. The main aim of this research is to ensure that readers have a clear understanding of hardware-based USB attacks and how they can be prevented.

**KEYWORDS**: USB Security, HID Attacks, USB Rubber Ducky, Hardware-Based Attacks, Keystroke Injection, Cybersecurity

## I. INTRODUCTION

Moreover, due to the rapid development of digital technologies, there is a greater dependency on peripherals such as keyboards, storage devices, and network devices [1]. USB technology is a common interface for connecting computers and peripherals. Although USB technology facilitates greater productivity and ease of use, there are a number of security vulnerabilities that can be exploited by attackers [4].

Hardware-based cyber attacks have been identified as a significant threat in contemporary cybersecurity environments [11]. Unlike conventional software-based malware, which requires execution or installation, hardware-based cyber attacks utilize devices to penetrate systems. The attacks are normally hard to trace, as the operating system considers the hardware as a trusted device [8].

The USB Rubber Ducky resembles a normal flash drive, but it works as a keyboard, typing in the commands automatically [13]. The commands are executed at a lightning-fast speed, taking only seconds. This allows the attacker to run scripts to download malware, change system settings, or steal sensitive information [12].

## II. BACKGROUND OF USB-BASED HARDWARE ATTACKS

This is because USB devices are based on a plug-and-play approach, which means that when a device is plugged into a computer, the computer will automatically recognize and configure the device [1]. However, this approach to device management can lead to a number of security risks since the computer will assume that all devices plugged into it are genuine devices [4].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504043|

A USB device can represent itself as several different hardware devices, such as a storage device, a keyboard, a mouse, a network device, or a Human Interface Device. In most cases, attackers use this feature to design malicious devices that represent themselves as other devices[4].

The threat of HID-based attacks is high because keyboard inputs are trusted by the OS by default [8]. A malicious device, if it is configured to behave like a keyboard, can inject its commands into the system without the need for software installation or administrative privileges [8].

The USB Rubber Ducky makes use of a scripting language called Ducky Script, which is used for carrying out keystroke injection attacks [13]. The scripts allow attackers to carry out system operations, open terminals, download files, and create hidden user accounts [12].edges followed by thresholding and morphological dilation, erosion operation. Then, connected component labelling is performed to label each object separately. Finally, the set of selection criteria is applied to filter out non text regions. After text detection, text inpainting is accomplished by using exemplar based Inpainting algorithm.

## III. ARCHITECTURE OF USB RUBBER DUCKY

The USB Rubber Ducky is designed in the form of a common USB flash drive but is equipped with internal hardware that facilitates keyboard emulation [13].
The main components of the USB Rubber Ducky are as follows:
• Microcontroller: Executes the attack scripts
• MicroSD Storage: Stores the Ducky Script payloads
• USB Interface Controller: Allows communication with the target device
• Ducky Script Payload: Keyboard commands are automated [12]
When the device is plugged into a target device, the OS automatically identifies the device as a keyboard and waits for input [11]

**Fig. 1. USB HID Injection Attack Architecture**

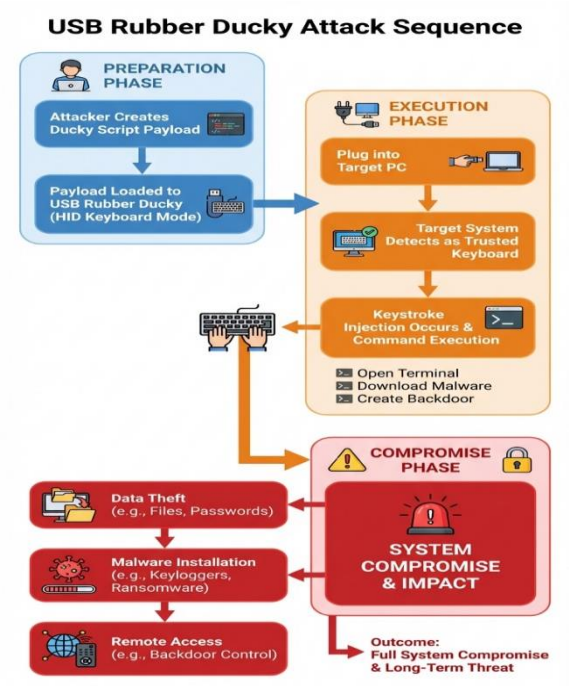



Fig. 1. Architecture of a keystroke injection attack using the USB Rubber Ducky.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504043|

## IV. WORKING MECHANISM OF HID INJECTION ATTACKS

HID injection attacks take advantage of the trusting relationship between operating systems and their input devices [11]. A standard HID-based attack utilizing devices such as the USB Rubber Ducky involves a series of steps. First and foremost, the attacker must develop and design their own script utilizing the Ducky Script language. The language is specifically designed to facilitate keystroke injection. Once the script is created, it is compiled into a binary format that can be executed on the device. The compiled script is then stored on the device. Once the attacker has gained access to the system and has connected the device to the compromised computer, the operating system recognizes the device as a standard keyboard because it is classified as a Human Interface Device. The device then proceeds to execute pre-programmed keystrokes rapidly and initiate attacks such as opening up command prompts, downloading malware, and creating backdoors within seconds of connection to the compromised computer system [12].Commands can involve opening up command prompts, downloading malware, disabling antivirus programs, creating hidden accounts, and extracting stored passwords [8].

## V. SECURITY RISKS

USB Rubber Ducky attacks introduce several serious cybersecurity risks that can significantly compromise system security [12]. One major risk is unauthorized system access, where attackers can create new administrative accounts or enable remote access services to gain control over a system without the user's knowledge [8]. In addition, these attacks can be used to install malware, as malicious scripts executed by the device may automatically download spyware, ransomware, or other harmful software onto the target computer. Another critical concern is credential theft, where sensitive information such as Wi-Fi passwords, browser-stored credentials, and login details can be extracted.
Furthermore, these attacks can lead to data exfiltration, where confidential files and information are secretly transferred to remote servers controlled by the attacker [14]. Insider threats also play a significant role, as individuals with temporary or authorized physical access to a system can easily plug in such devices and execute attacks. Finally, USB Rubber Ducky attacks are extremely fast, often completing within a few seconds, which makes them difficult to detect or stop in real time [13].

**Table 1. Comparison of Common USB-Based Attacks**

| Feature | USB Rubber Ducky | BadUSB Attack | USB Killer |
|---|---|---|---|
| Attack Type | Keystroke Injection | Firmware Manipulation | Electrical Hardware Attack |
| Working Principle | Emulates keyboard and types malicious commands | Reprograms USB firmware to act malicious | Sends high-voltage surge through USB |
| Main Target | Operating System | USB firmware controller | Computer hardware |
| Purpose | Malware execution and data theft | Persistent compromise | Destroy hardware |
| Detection Difficulty | Medium | Very High | Easy after damage |
| Physical Damage | No | No | Yes |
| Execution Speed | Seconds | Immediate after firmware activation | Instant |
| Risk Level | High | Very High | Critical |

Table 1. Comparison of major USB-based cyber attack techniques

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504043|

## VI. DETECTION TECHNIQUES

Detecting human interface device (HID) based attacks is difficult since the attackers behave like normal human interface devices like a keyboard or a mouse. The operating systems tend to trust the input devices, which enables the keystroke injection tools like the USB Rubber Ducky to perform the required operations without demanding any further permissions. Since the attackers behave like a keyboard, it is difficult for the antivirus programs to detect the attack [11].

Detection methods include:

### A. Behavioral Monitoring of Typing Speed

One of the approaches is to monitor the typing behavior of connected input devices. The typing speed of humans is normal, whereas the typing speed of automated devices is extremely high. Security monitoring tools can monitor typing speed and identify any abnormalities that may indicate automated keystroke injection attacks [8].

### B. Endpoint Detection and Response (EDR)

Endpoint Detection and Response systems continuously monitor activities on computers and detect suspicious behavior such as unexpected command execution, abnormal script activity, or unauthorized system changes.

### C. USB Device Monitoring

USB monitoring tools track newly connected devices and record details such as vendor ID and product ID. These tools help detect unauthorized or suspicious USB hardware connected to a system.

### D. Intrusion Detection Systems (IDS)

Intrusion Detection Systems analyze network traffic and system activities to detect suspicious behavior. If an injected script downloads malware or communicates with remote servers, IDS tools can identify this abnormal activity.

## VII. PREVENTION AND MITIGATION

Organizations can implement several defensive mechanisms to protect systems from USB-based attacks involving devices like the USB Rubber Ducky [11].

### A. USB Port Control

Administrators can disable unused USB ports or restrict device usage through system policies to prevent unauthorized devices from connecting to computers.

### B. Device Whitelisting

Device whitelisting allows only approved USB devices to connect to systems by verifying device identifiers such as vendor ID and product ID.

### C. Endpoint Security Software

Endpoint security solutions monitor system behavior and detect malicious activities triggered by automated scripts or unauthorized commands [8].

### D. User Awareness Training

Employees should be trained about the risks of connecting unknown USB devices to their computers.

## VIII. FUTURE RESEARCH DIRECTIONS AND CONCLUSION

Future research will be directed towards further advanced techniques for the detection and prevention of USB-related attacks. For example, machine learning techniques can be applied to the keyboard to recognize unusual typing patterns associated with USB devices. Other techniques include hardware authentication to allow trusted USB devices to access the computer. Furthermore, anomaly detection techniques can be applied to the system to recognize unusual activities. Other techniques include the development of advanced endpoint monitoring systems to enhance the accuracy of threat detection [9].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504043|

There is a major cybersecurity risk associated with USB-related hardware attacks. This is due to the fact that the attack is based on the trust between the computer and the USB device [12]. For example, the USB Rubber Ducky can be used to carry out malicious operations on a computer. This is due to the fact that the USB Rubber Ducky can emulate a keyboard. This can be used to carry out various malicious operations, including data theft and unauthorized access [8]. To prevent the risks associated with the USB Rubber Ducky and other similar devices, security measures must be implemented [13].

## REFERENCES

[1] N. Daswani et al., *Foundations of Security*, Apress, 2007.
[2] S. N. Checkoway et al., "Automotive Attack Surfaces," USENIX Security, 2011.
[3] S. Jana and V. Shmatikov, "Memento," IEEE Security and Privacy, 2012.
[4] K. Nohl and J. Lell, "BadUSB – On Accessories That Turn Evil," Black Hat USA, 2014.
[5] A. Costin et al., "Dynamic Firmware AnFalysis," USENIX Security, 2014.
[6] C. Miller and C. Valasek, "Remote Automotive Attack Surfaces," Black Hat USA, 2014.
[7] M. Guri et al., "USBee: Air-Gap Covert Channel via USB," arXiv, 2016.
[8] F. Griscioli and M. Pizzonia, "USBCaptchaIn: Preventing USB Device Attacks," Journal of Computer Security, 2020.
[9] O. A. Ibrahim et al., "MAGNETO: Fingerprinting USB Flash Drives," arXiv, 2020.
[10] R. Dumitru et al., "The Impostor Among US(B)," arXiv, 2022.
[11] M. A. Khan et al., "HID Attack Prevention and Mitigation," Asian Journal of Science and Technology, 2023.
[12] Z. R. Dönmez et al., "Leaking Network Devices with Rubber Ducky Attack," Journal of Innovative Science and Engineering, 2024.
[13] R. V. Reddy et al., "Unveiling the Power of USB Rubber Ducky," IJERT, 2024.
[14] D. Yadav et al., "Duck Hunter: Encountering USB Rubber Ducky Threat," IJRASET, 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details