International Journal of Applied Sciences: Current and Future Research Trends

(IJASCFRT)

ISSN: 2790-3990

https://ijascfrtjournal.isrra.org/index.php/Applied_Sciences_Journal

USB Threats

Sami Mehtonen[a]*, Mitha Jose[b], Seppo Koponen[c]

[b,c]Laurea University of Applied Sciences, Leppävaara Campus, Vanha maantie 9, 02650 Espoo, Finland.
[a]Email: sami_mehtonen_kvt@hotmail.com , [b]Email: mitha.jose@laurea.fi, [c]Email: seppo.koponen@laurea.fi

Abstract

This article aims to explore the evolution of USB attacks from their inception to the present day. By examining the equipment, history, and threat posed by USB hotplug attacks, this study builds on previous research and a comprehensive literature review of related technologies. This foundation has been utilized to understand the increasing prevalence of USB threats, their technological advancements, potential impacts, and prevention methods. The findings indicate that the trend of USB-targeted attacks has been on the rise, significantly impacting various societal functions and industries. The study underscores the need for further research on USB attacks and the development of protective measures to address vulnerabilities that have emerged alongside the evolution of USB technology.

Keywords: USB; Hotplug; USB Threats; Implant Attacks.

1. Introduction

USB, Universal Serial Bus, is a widely adopted standard for connecting various devices. Over the years, it has replaced most serial and parallel port applications. Compared to its predecessors, USB offers high transfer speeds, easy physical connectivity without the need for device reboots, plug-and-play functionality, and the ability to provide power to connected devices directly through the USB port [1:1]. As such, nine out of ten maintenance engineers in the industry sector use USB connections to connect to industrial equipment [2:3]. The world of information technology work is heavily dependent on the flexibility provided by USB for both data transfer and device connectivity.

Received: 6/15/2025
Accepted: 8/10/2025
Published: 8/25/2025

** Corresponding author.*

USB allows for the connecting various devices for data transfer and power delivery. It includes definitions for Human Interface Devices (HID), a class of device typically accepted by the operating system immediately on physical connection. This enables a series of USB-based hotplug attacks, commonly referred to as BadUSB. These attacks can target computers, tablets, smartphones, routers, smart refrigerators, and almost any other device with a USB port. [3:66] Almost any device can be adapted for attack purposes. Embedded systems chips' often hold reprogrammable firmware, allowing conversion of benign USB devices into advanced attack tools [4].

The United States Computer Emergency Readiness Team (US-CERT) has emphasized the threat posed by small portable devices for over a decade. These devices, include USB sticks, media players, tablets, and smartphones. They pose an increased risk of loss and exposure of data, and further attacks on the network. Data loss refers to the disappearance or destruction of data, either through intentional sabotage or the loss of a device. Data exposure refers to the unauthorized disclosure, leakage, or public release of information [5:1-2].

Dung and his colleagues have identified data theft using USB devices as the biggest concern for the corporate sector since the widespread adoption of the USB 2.0 standard in 2005. The prevalence of USB as an attack vector has not diminished [1:1]. Honeywell's executive summary "USB Security – Myths vs. Reality" provides four simple reasons for the commonality of USB attacks: USB devices are easy to carry, use, and are so common that most users do not consider them a risk. Many devices that charge via USB ports provide a plethora of functions beyond receiving power [2:4]. In 2021, 64% of international organizations reported USB-based attacks, up from 15% in 2020. These figures are based on Proofpoint's 2022 "State of the Phish" report [6:7]. Honeywell's "Industrial USB Threat Report" found that 44% of locations reported having detected and blocked at least one malicious or suspicious file representing a security threat [7:5]. Additionally, people who find USB sticks are likely to connect them to their computers, with 45-98% of USB sticks distributed on campuses being connected to a computer within a median time of 6.9 hours after being dropped [8:4-5].

2. Historical Attacks

Hacksaw was a project developed by the Hak5 community, where a configurable flash drive was created; the "Universal Serial Bus (USB) Hacksaw." The device aimed to produce a USB flash drive with a CD-ROM (compact-disc read-only memory) partition. This process required a flash drive compatible with SanDisk's U3 standard [9:6], which was configured using a modified version of the manufacturer's LaunchPad software. The U3 smart disk standard was developed in collaboration between SanDisk and M-Systems in 2005. This allowed a second partition recognized by the Windows system, from which an automatic strike could be launched from the autorun.inf file. [9:1,5] The same autorun.inf file's automatic launch was used in many installation programs of the era, as well as in the installation of USB modem drivers when connected to a computer via the USB bus.

Before the development of the Hacksaw device, the most common USB port attack was the direct copying of files to the flash drive by the attacker. The Hacksaw installed its malicious software directly among the native files of the computer, acting as a persistent internal threat that only required the connection of a new flash drive to the computer to trigger. During the USB device negotiation, the Hacksaw-infected terminal executes the

Hacksaw attack by running a malicious autorun.inf file (instead of, for example, the flash drive's drivers), potentially leading to a data breach [9:17].

"USB Switchblade" is, similarly to Hacksaw, a creation of the Hak.5 community. USB Switchblade can cause more damage to the system than Hacksaw. It needs administrative rights to function. Designed for collecting information from the Windows system or the surrounding network, the modular nature of the device allowed developers to add new tools. USB Switchblade can be considered more of a way to gather numerous administrator data collection tools into one practical package, rather than a completely novel invention [9:27] .The software of the device was originally used for system administration, protecting systems and their data. Its ability to retrieve and expose passwords, keys, and other critical system elements can be easily misused [9:31].

The Stuxnet worm was referred to as a "wake-up call" for the use of USB and embedded devices to compromise all systems, including air-gapped ones, in a 2015 Royal Holloway article on the BadUSB 2.0 tool [10:2]. Air-gapped networks and devices are isolated from the broader network; there is no direct connection from the isolated network to other surrounding networks and devices.

Like other methods of exposing a system to malware, the USB port provides a means to inject malicious code or malware directly into the target device – and thus the target network. The risks posed by malware affect data integrity, resource consumption, time usage, the trade secrecy, and privacy of personally identifiable data [9:88].

3. USB Technology and Specifications

The USB specification was developed in 1996, with USB 1.0 as the first version [9:5]. Since its inception, USB has evolved into four main versions: USB 1.0, USB 1.1, USB 2.0, and USB 3.0. USB 2.0, introduced in 2000, marked a significant turning point, enabling faster data transfer and more complex peripherals, which subsequently led to more sophisticated USB-based attacks. The USB 3.0 version, released in 2008, further increased speeds and allowed bidirectional data transfers, increasing the efficiency of activities. Below is a table comparison of these USB versions [11:11-14].

Table 1: Comparison of USB versions

USB Version	Release Date	Features
USB 1.0	January 1996	Limited support for peripherals
USB 1.1	September 1998	Added new transfer type (interrupt OUT)
USB 2.0	April 2000	Added high speed usb (480 Mbps transfer)
USB 3.0	November 2008	Added dual-bus architecture and SuperSpeed (5 Gbps transfer)

USB specifications define concepts that are crucial to understanding its vulnerabilities as an attack vector: functionality, devices, and ports. These specifications also outline processes like device enumeration, which attackers exploit to modify communication between USB devices and hosts. Device descriptors and their types dictate the data exchanged, presenting opportunities for attacks during enumeration. [10:18-20]

4. Human Interface Devices (HID) and Security Risks

Human Interface Devices (HID) are peripherals, such as keyboards, mice, and barcode scanners, that interact directly with the computer. The generality and support for specialized functions in HID devices have made them particularly vulnerable to manipulation. [11:180]. HID Devices allow humans to interact with technology, but also technological means of exploiting the device class allowing remote mimicry and malicious use as if a human was actively present.

Consumer Control Buttons (CCB), a subset of HID functionality, allow activation of software or functions with one press, such as media shortcuts. CCB has been exploited for kiosk attacks against ATMs and public information kiosks among other "closed" systems, demonstrating significant vulnerabilities in seemingly isolated setups. A team developed a proof-of-concept attack called “USB HID & Run” that demonstrated this vulnerable vector [12]

Preventing HID-based attacks can involve disabling the Human Interface Device service on Windows systems using commands like 'sc config hidserv start=disable,' which stops the service and prevents shortcut-based attack vectors [12]

5. Modern USB Threats

The evolution of USB vulnerabilities encompasses attack techniques such as HID & Run, which exploit HID and Consumer Control Button (CCB) functionalities to compromise devices. The original BadUSB-technique has evolved further into a proof of concept named BadUSB2.0, and USB-based attacks and devices keep evolving. Most techniques still exploit the inherent trust integrated in the HID class. BadUSB 2.0 devices are modified USB devices whose microcontroller firmware is changed to give them the ability to mimic other devices in implant usage. It can act as a keystroke logger, a device mimicking a keyboard, or a device similar to the original BadUSB. Combining these different techniques in real-time enables the analysis of multiple attack methods in chained attacks. Below is a table of BadUSB 2.0 techniques that have been successfully demonstrated in a laboratory environment during development. [10:3-4].

Table 2: Attack types proven in laboratory setting

Attack Type	Description
Eavesdropping	Keystroke logging
Sending Keystrokes	Sending keystrokes
Replaying Logon Credentials	Replaying login credentials
Character Substitution Attack	Real-time modification of messages between the keyboard and the host device
Data Exfiltration	Stealthy data exfiltration using HID protocol
Interactive Shell over USB-HID	Interactive command prompt
BadUSB	Re-registering the BadUSB device as a different device

Plentiful commercially available solutions to exploit these methods of attack exist. Keystroke injection attack devices, such as the USB Rubber Ducky by Hak5 are viable even today. It uses scripted text files on an SD-card to launch pre-scripted attacks from a disguised device. [13:1-2] A more mature solution with the same principle is MG’s O.MG-cable [14]. It functions in a similar fashion, but uses internal flash memory with different program slots, as well as advanced functions using a wireless hotspot and advanced geofencing features. Remotely controlled and capable of man-in-the-middle attacks and direct keystroke recording while still looking externally exactly like any other USB-cable, it is an elusive device to track down if in use [14] . There is a third device in “the same family”, available from the third vendor. The Bash Bunny can create reverse shell sessions, camouflage itself as a network adapter, and directly exfiltrate data into an internal SSD drive [15]. It also includes an entire Linux-system within itself, allowing an incredibly intrusive and complex variety of attacks based on having a system run “inside another system”, communication from the host and the Bash Bunny implant taking place over the SSH protocol [16] .

A quite recent entry to the field of BadUSB devices is the Flipper Zero, a signal hacking multi-tool, includes a variety of sensors but has some of its own extensibility for BadUSB attacks [17]. While slower than the Rubber Ducky “lineage” devices, it includes computing power and high degrees of extensibility through its exposed GPIO pins (General Purpose Input and Output). Its toylike appearance works as a light form of camouflage – it blends in as a pocket gaming device [18].

6. Conclusion

The evolution of USB technology has transformed it from a simple data transfer tool into a sophisticated attack vector. Initially designed for convenience and efficiency, USB devices have become ubiquitous in modern computing, connecting a wide range of peripherals and enabling seamless data exchange. However, this widespread adoption has also made USB devices a prime target for attackers.

Modern USB threats have evolved significantly from their early days, becoming more sophisticated, automated and pervasive. The increasing reliance on USB devices for data transfer and connectivity has made them a prime target for attackers. Devices like Flipper Zero [18] illustrate the ongoing development and application of USB-based attack mechanisms, showcasing the persistence of USB as a threat vector.

Historical attacks, such as Hacksaw and USB Switchblade, demonstrated the potential for USB devices to be used for malicious purposes. These early attacks exploited the autorun feature and the ability to install malware directly onto the host system, highlighting the vulnerabilities inherent in USB technology [9:27].

As USB technology advanced, so did the complexity of the attacks. The introduction of BadUSB and its variants showcased the ability to reprogram USB firmware to perform malicious actions, such as keystroke logging, data exfiltration, and command injection [4:21] [10:2]. These attacks leveraged the versatility of USB devices, making them a formidable threat to both individual users and organizations.

Mitigating these threats requires a comprehensive approach that includes strict policies for USB device usage, regular scanning for malware, and advanced security measures such as USB firewalls and device control software [1:2] [10:5-6] [19:506-507]. Organizations must remain vigilant and proactive in addressing USB-related vulnerabilities to protect their systems and data from evolving threats.

In conclusion, the transformation of USB technology into an advanced attack vector underscores the need for continuous research and development of protective measures. As USB devices become more integrated into our daily lives, understanding and mitigating the risks associated with their use is crucial for ensuring cybersecurity in the modern world.

References

[1] V. P. Dung, A. Syed, A. Mohammad and M. N. Halgamuge, "Threat analysis of portable hack tools from USB storage devices and protection solutions," Karachi, Pakistan, 2010.

[2] Honeywell, "USB SECURITY- MYTHS VS. REALITY.," Honeywell Process Solutions, Houston, TX, 2020.

[3] B. Cannols and A. Ghafarian, "Hacking Experiment by Using USB Rubber Ducky Scripting," 2017.

[4] K. Nohl, S. Krißler and J. Lell, "BadUSB — On accessories that turn evil," Tokyo, Japan, 2014.

[5] P. Walters, "The Risks of Using Portable Devices," 2012.

[6] Proofpoint, "State of the Phish 2022," DXC Technology, 2022.

[7] Honeywell, "HONEYWELL GARD USB THREAT REPORT 2024," Honeywell, 2024.

[8] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori and E. Bursztein, "Users Really Do Plug in USB Drives They Find," San Jose, CA, USA, 2016.

[9] B. Anderson and B. Anderson, Seven Deadliest USB Attacks, Burlington, USA: Syngress (an Imprint of Elsevier, Inc.), 2010.

[10] D. Kierznowski and K. Mayes, BADUSB 2.0: EXPLORING MAN-IN-THE-MIDDLE ATTACKS, Royal Holloway, 2015.

[11] J. Axelson, USB Complete: The Developer's Guide, Fourth Edition ed., Chinook Ln.: Lakeview Research LLC, 2009.

[12] E. Alm and A. Aaris-Larsen, "USB Hid-and-Run." Internet: https://github.com/piraija/usb-hid-and-run, 2023[Jan. 16, 2025].

[13] J. Queppet, "The Hardware Components of a USB Rubber Ducky," 2018.

[14] Hak5, "OMG-Cable." Internet: https://shop.hak5.org/products/omg-cable,2025 [Jan. 31, 2025].

[15] Blue Goat Cyber, "Hacking Tool: Bash Bunny."Internet: https://bluegoatcyber.com/blog/what-is-a-bash-bunny/, 2025 [Jan. 30, 2025].

[16] Hak5, "Bash Bunny by Hak5 Product Documentation." Internet: https://docs.hak5.org/bash-bunny, Jun. 2024 [Jan. 30, 2025].

[17] Flipper, "Flipper Zero Documentation, Bad USB." Internet: https://docs.flipper.net/bad-usb, 2025 [Jan. 30, 2025].

[18] Flipper, "Flipper Zero - Portable Multitool for Geeks." Internet: https://flipperzero.one/, 2025 [Jan. 30, 2025].

[19] M. Nicho and I. Sabry, "Bypassing Multiple Security Layers Using Malicious USB Human Interface Devices," Lisbon, Portugal, 2023.

[20] mg, "omg-cable." Internet: https://mg.lol/blog/omg-cable/, Feb. 11, 2019 [Jan. 31, 2025].

[21] Flipper. "BadUSB File Format." Internet: https://developer.flipper.net/flipperzero/doxygen/badusb_file_format.html, 2025 [Jan. 31, 2025]