INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 07 | JULY - 2023 SJIF RATING: 8.176 ISSN: 2582-3930

Analysis of Various Malicious Payload Deployment Cables

Anay Patharkar
Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur, India
anaypatharkar11@gmail.com

Anjali Udapurkar
Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur, India
udapurkaranjali25@gmail.com

Chinmayee Matte
Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur, India
chinmayeematte99@gmail.com

Nikita Kalmegh
Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur, India
nikitakalmegh1992@gmail.com

***Abstract*— Cybercriminals and hackers are always thinking of clever, new ways to exploit your devices and you must be perpetually vigilant. A malicious cable is any cable (electrical or optical) which performs an unexpected, and unwanted function. The most common malicious capabilities are found in USB cables. Data exfiltration, GPS tracking, and audio eavesdropping are the primary malicious functions. The worst malicious cables take control of a user's cell phone, laptop, or desktop. Usernames and passwords are the first bits to go. Next, the connected device's storage is emptied. Attacks through various computer ports such as Ethernet Port, if the targeted network contains faulty Ethernet (networking) cables on the attacker's path to their victim. This project gives a broad overview and a comparative study of the list of vulnerabilities in the hardware ports of a computer that can be exploited by the attackers using various malicious cables and payloads.**

Keywords*— *malicious, payloads, data infiltration, USB cables, ethernet cables, HDMI cables

I. INTRODUCTION

This project comes under the field of Cyber Security. In this emerging world of Cyber Warfare, Hackers are continuously looking for more creative, clever, and new ways of infiltration and exploitation of data. One of the easiest ways for an infiltrator to get access to users to confidential data is thru the Hardware Ports on the victim's computer with the use of a malicious cable connected to a remote controller or transmitter. This Project Compares different types of attacks performed on the hardware ports with the use of such apparatus and studies its effect on the users' data based on the CIA Triad model of Information Security.

A. Technology Background

This section outlines the tools or technologies used like USB cables, ethernet cables, HDMI cables, Digispark ATTiny85 Arduino board, Rubber Ducky, Shinolocker, Raspberry Pi Pico Micro-controller.

1. USB cables

   USB stands for Universal Serial Bus, used to connect computers to peripheral devices such as printers, cameras, scanners used for short distance digital data communications.

2. HDMI cables

   HDMI stands for High Definition Multimedia Interface used for transmitting digital audio and video from a display controller, to a compatible computer monitor, video projector, digital television, or digital audio device.

3. Ethernet cables

   Ethernet cables are a type of network cable used for high-speed wired network connections between two devices such as PCs, routers, and switches within a local area network.

4. Digispark ATTiny85 Arduino board

   Digispark ATTiny85 Arduino board is mini USB Development board.

5. Digistump's "Digikeyboard" library.

   Digistump's "Digikeyboard" library sends keyboard strokes to the computer and acts as a Human interface Device. [1]

6. Rubber Ducky

   USB Rubber Ducky is just like USB flash drive that injects keystrokes at phenomenal speed. USB Rubber Ducky was invented in 2010 and became the must-have pentest tool. [2]

7. Shinolocker

   Shinolocker is a ransomware simulator. In Shinolocker no ransom money is demanded for the decryption key.

8. Raspberry Pi Pico Micro-controller

   Raspberry Pi Pico is a microcontroller board. It's the primary microcontroller development board from Raspberry Pi.

II. ITERATURE SURVEY

1. Sumeet Kumar published a paper titled "*Simulating DDoS attacks on the us fiber-optics internet infrastructure*" in the 2017 Winter Simulation Conference. [3] In November 2017, a DDoS attack shut down Liberia's internet connection in an African country. The attack is reported to consume over 500 Gbps of bandwidth on ACE (African Coast to Europe) fiber optic cables that connect Europe and Africa to the Internet. This incident highlights a vulnerability in Internet infrastructure. You need a simulation testbed that can reflect the complexity of the Internet, but it still provides quick testing of attacks and insights that can be applied to real-world attack scenarios. This research attempts to identify such vulnerabilities using simulation. This work is a compilation of our original work on "Simulation of DDoS Attacks on US Fiber Optic Internet Infrastructure", which was accepted as a full paper at the 2017 Winter Simulation Conference.

2. Dave (Jing) Tian ,Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bate, Kevin R. B. Butler published a paper titled "SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions1 through C". in 2018 IEEE Symposium on Security and Privacy. [4] USB-based attacks have become more complex in recent years. Today's modern attacks span a wide variety of attack trajectory, from social engineering to signal injection. To acknowledge these challenges, the security community has retorted by increasing the set of fragmented countermeasures. This task examines and categorizes USB attacks and defenses and integrates peer-reviewed research with industry observations. Our systematization extracts offensive and defensive primitives that work across the communications layer within the USB ecosystem. Based on our classification, we found that USB attacks often abuse the default trusted nature of the ecosystem and bypass different layers in a software stack; No existing defense system provides a complete solution and multi-layer scaling solutions are the most effective. We then extended the first formal verification of the recently released USB Type C Credential and discovered fundamental flaws in the spec's design. Based on our systematization results, we found that while the specification succeeded in identifying the urgent need to address USB security, its flaws caused This goal cannot be achieved. We conclude by outlining future research directions to ensure a safer computing experience with USB.

I. RESEARCH METHODOLOGY

This section outlines 15 attacks that we performed to create a comparative study of it's effects on victims computer.

A. Block Diagram

The following figure depicts the broad view of the analysis process:

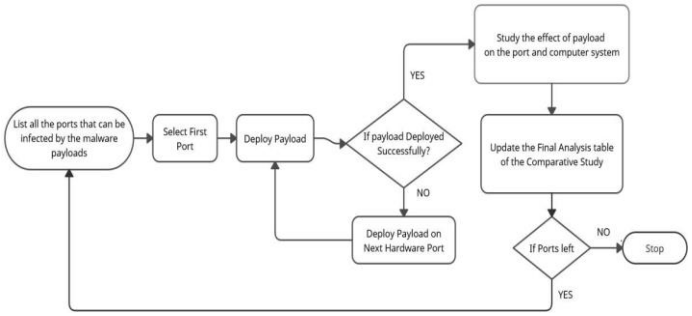

Fig. 1. Block diagram of the analysis process

B. Implementation of the proposed solution:

1. Attacks using USB cables on USB ports

The USB port is the standard cable connection interface for personal computers and consumer electronics. USB (Universal Serial Bus) is an industry standard for short distance digital data communications. The USB port allows connecting USB devices to each other and transferring digital data via a USB cable.

1.1. Attack 1 - Fork Bombing using a USB Cable and Digispark ATTiny85 Arduino board

The fork bomb (also known as the "rabbit virus") is a denial of service (DoS) attack in which the fork system call is used recursively until all system resources execute a Comeinand. The system will be overloaded and unable to respond to any input.

The Arduino library used in this attack is Digistump's "Digikeyboard". Digikeyboard sends keystrokes to the computer via a USB data cable and is therefore not detected by any installed anti-virus applications. The script written in C++ with the help of Digikeyboard library achieves the purpose of impeding the availability of data to the victim, thus making the DoS attack successful.

1.2. Attack 2 - Reverse Shell using Digispark ATTiny85 Arduino board

A reverse shell is a shell session started on a connection initiated by a distant machine rather than the attacker's host. After successfully exploiting a remote command execution vulnerability, attackers can employ a reverse shell to gain an interactive shell session on the target machine and continue their attack. Reverse shells can also work through a firewall or NAT.

An attacker may try to breach a server by exploiting a command injection vulnerability on the server system. The injected code is usually a reverse shell script that serves as a command shell for further malicious activity. Digistump's "Digikeyboard" Arduino library used in this attack. Digikeyboard delivers keyboard strokes to the computer via USB data cable, and is thus undetectable by any anti-virus software. The script, written in C++ and using the Digikeyboard Library, aids in the establishment of a remote access connection between the attacker's and victim's computers.

1.3. Attack 3 - Data Infiltration Attack using Rucky

By posing as a keyboard, the USB Rubber Ducky injects keystrokes at superhuman speeds, breaking computers' natural confidence in people. The USB Rubber Ducky became the must-have pentest tool after inventing keystroke injection in 2010. This rogue USB infiltrates systems and imaginations all over the world with its deceptive design and simple "Ducky Script" language. Rubber Ducky is essentially the next step in the evolution of BadUSB, embedding and executing the attack via a cable or a USB stick. Rucky is a modern-looking USB Rubber Ducky Editor and Attack Launcher that delivers keyboard strokes to the computer through USB data cable and is thus undetectable by any anti-virus software. The script helps achieve the goal of Infiltrating the browser and exfiltrating the Credentials by storing them in the form of .png files and emailing them to attackers' email-id.

1.4. Attack 4 - Ransomware attack using Rucky

Ransomware encrypts a victim's whole hard drive and prevents them from accessing their files until they pay a ransom to the attacker in exchange for the decryption key. We utilised the USB Rubber Ducky-like programme RUCKY to transmit the malware to a target PC. In a nutshell, the USB Rubber Ducky is a rogue device that uses keystroke injection to fool your target computer into thinking it's a keyboard, then types the key sequence set into its payload automatically. The only difference between RUCKY and a USB Rubber Ducky is that RUCKY is an android software, whereas the USB Rubber Ducky is a tangible object. These technologies take advantage of operating systems' innate confidence in humans. These tools reap the benefits of operating systems' fundamental trust in human interface devices (HIDs).

Because ransomware attacks are too risky and unlawful to try on your own or any computer, we used a preliminary ransomware simulator application called shinlocker. The shinlocker tool is downloaded and installed using the rubber ducky script in this attack, and then the victims' files are encrypted.

1.5. Attack 5 – Disable Windows firewall (WIN-7) using Raspberry Pi Pico Micro-controller

Windows Firewall is a network security system that monitors and controls incoming and outgoing network traffic on a computer based on pre-defined and custom rules to prevent harmful activity from infecting the operating system or computer system. This exploit makes advantage of the Raspberry Pi Pico Micro-Controller to simulate and send keystrokes in order to run a malicious script that disables Windows Defender and Firewall, making the computer open to a variety of cyber-attacks. The script for this payload is written in Ducky.

1.6. Attack 6 – Net Disabler attack (WIN-7) using Raspberry Pi Pico

The Net Disabler attack prevents the user from accessing the internet. When a web page is loading, the web browser generates a process request; this attack destroys that request, denying the user service. This exploit leverages the Raspberry Pi Pico Micro-Controller to simulate and send keystrokes to run a malicious script that executes the task kill command, which terminates a specific process.

1.7. Attack 7 – Drive Wiper attack using Raspberry Pi Pico

The Drive Wiper attack deletes all content on all discs on the victim's PC, making the information inaccessible to the user. The 'C' drive is kept alone since it houses the Operating System files, which if destroyed can cause the entire operating system to crash. The Raspberry Pi Pico Micro-Controller is used in this attack to simulate and deliver keystrokes to run a malicious software.

The following are the steps that were taken during the attack:

•The Ducky Script injects keystrokes into a.bat file to programme it.
•Scripted instructions to wipe all available drives.
•The attack is started by running the.bat file.

Circuit Python and the Adafruit HID library were used.

1.8. Attack 8 – Reverse Shell attack in Linux using Raspberry Pi Pico

A reverse shell is a shell session started on a session initiated by a distant machine rather than the attacker's host. After successfully exploiting a remote command execution hole, attackers can employ a reverse shell to gain an interactive shell session on the target machine and continue their attack. Reverse shells can also work through a firewall or NAT.

An attacker may try to breach a server by exploiting a command injection vulnerability on the server system. The injected code is usually a reverse shell script that serves as a command shell for further malicious activity.

The Raspberry Pi Pico Micro-Controller is used in this attack to simulate and deliver keystrokes to run a malicious software.

2. Attacks Using HDMI cables on HDMI ports

The High-Definition Multimedia Interface (HDMI) is a patented technology audio/video interface that allows an HDMI-compliant source device, such as a display controller, to send lossless video data and compact or decompress digital audio data to a compatible computer monitor, video projector, digital television, or digital audio device. HDMI is a digital video protocol that replaces analogue video standard.

The threat model for HDMI-Walk includes the following five threats. [5]

Threat 1: Malicious CEC Scanning: This threat involves the malicious use of scanning features such as CEC and open HDMI ports to obtain information about connected devices. Felicity, for example, can develop a topology of accessible HDMI devices to control and use this information to launch other attacks.

Threat 2: Eavesdropping: Mallory is not present in this threat but is actively listening in on CEC communication through an implanted device.

Threat 3: Facilitation of attacks: In wired and wireless attacks, this threat removes temporal and physical access limits. Many of these attacks are facilitated by HDMI-Walk, making them more viable or difficult to detect. Mallory, for example, installs a device that passively captures WPA handshakes, avoids detection, and can be controlled remotely via CEC.

Threat 4: Information Theft is a type of data transfer that Criminals may find valuable. For example, data about available HDMI devices or wireless handshake capture that could be used in future attacks.

Threat 5: Denial of Service: Mallory uses an HDMI connection to impair the availability of a system, resulting in a Denial-of-Service attack. These attacks can be directed at a single device or broadcast to a large number of them. Mallory, for example, blocks the use of a television by broadcasting HDMI control commands repeatedly.

2.1. Attack 1 - Topology Inference Attack

This attack demonstrates Threat 1 (Malicious CEC Scanning), which is achievable in both online and offline environments using CEC. With malicious intent, we leverage the HDMI-Walk architecture to move through the distribution and obtain information about every device available. This attack can be carried out either locally or remotely.

Step 1 - Activation: The listener immediately connects and begins the information gathering process using remote and local HDMI-Walk scans upon initial installation into the HDMI distribution.

Step 2 - Information Gathering: Using the CEC scanner module, the listener begins a "walk" over all of the devices. From available devices in the distribution, information about HDMI device type, device, logical address, physical address, active source, vendor, CEC version, device name, and power status may be easily obtained. The data is then stored locally by the listener after it has been processed.

Step 3 - Leakage: If a local client request it, the data is ready to be obtained through the File I/O module. The listener sends all of the collected information to POST: /cec/webclient for the remote client. The data is sent to the remote server as a JSON object, which a remote attacker can retrieve.

2.2. Attack 2 - CEC-Based Eavesdropping

This attack is used to illustrate Threat 2 (eavesdropping) and Threat 4 (Information Theft). An intruder has just access to the HDMI port for communication with the listener device in this local attack. The attacker walks the HDMI distribution and sends messages to the listener using the Microphone Access Module to activate and record audio. The listening device stores this audio data locally. The audio data is subsequently sent to the client via the File I/O module at a later time.

2.3. Attack 3 - WPA/WPA2 (wifi protected access) Handshake Theft

This attack was created to highlight Threat 3 (Facilitation of attacks) and Threat 4 (Information Resistance) (Information Theft). The

attacker in this local attack leverages HDMI-Walk to capture WPA/WPA2 handshakes and avoid detection by the security system in place. An attacker must wait for a handshake to occur in typical handshake theft attacks, which can take an endless amount of time because the WPA handshake is only delivered in specified conditions. If the hacker is pressed for time, he or she must attempt forceful de-authentication. This raises the possibility that forced de-authentication could be discovered using a network scanner like Wireshark or a more sophisticated IDS. We assist such a danger in this attack by removing temporal limits.

2.4. Attack 4 - Targeted Device Attack

This attack was intended to show Threat 5 (Denial of Service) using arbitrary sniffer and device control. The attacker uses the Python-based listener service to target a specific device in the HDMI distribution in this attack. She also uses the nature of CEC to smell and detect when a gadget has been switched on. There are three basic steps to this attack.

Step 1 :Activation: Attack activation is awaited by the listener. It waits for commands to activate the intended attack from either a local client (through a walk) or a remote client. The listener starts the attack after receiving a command.

Step 2 - Sniffing: The listener is placed within an HDMI distribution and watches for CEC packets to pass through. From any receiving source, we pay special attention to the data commands "84:00:00:00", "87:1f:00:08", and "80:00:00:30:00". These numbers usually indicate that a device's power state has changed and that it has been turned on by broadcasting to HDMI distribution devices. Specifically, 84 indicates a physical location, 87 indicates a vendor ID, and 80 indicates a routing change. The Sharp television is the target of this attack, which uses a CEC capable display.

Step 3 - DoS attack: Once the DoS attack is active, the listener waits for commands related to changing the power state of the HDMI distribution.

2.5. Attack 5 - Display Broadcast DoS

Threat 5 (Denial of Service) was shown using broadcast functionality in this attack. This technique takes advantage of CEC's broadcast function to generate a DoS in any display within a particular HDMI distribution. This attack targets displays explicitly, generating typical CEC directives for source and input control.

This attack is broken down into three parts.

Step 1: Install the Attacker Listener: The listener device is installed in any HDMI distribution point. The device then waits for instructions to start the attack from a client service. The listener's Remote Access Module becomes active if a wireless connection is available.

Step 2 - Activation Phase: The listener can activate in one of two ways:

(1) The listener receives a direct command to start the attack from a client service.

(2) The DOS1 command is received by the listener via a remote client.

Step 3 -DoS Attack phase: After the activation conditions are met, the listener device begins broadcasting various display input change commands. These are standard CEC commands for adjusting the active source on a display device that are accepted by equipped televisions. Power on ("20:04"), input 1 ("82:10:00"), input 2 ("82:20:00"), input 3 ("82:30:00"), and input 4 ("82:40:00") are all saturated with a broadcast loop in the CEC distribution. This basically disables the user's ability to use the displays, resulting in a DoS attack.

3. Attacks Using Ethernet cables on Ethernet ports

Ethernet is a group of wired computer networking technologies that are extensively used in LANs, MANs, and wide area networks (WAN). It was originally commercially available in 1980 and was standardised as IEEE 802.3 in 1983. Ethernet has since been improved to allow faster bit rates, a larger number of nodes, and longer network distances, while yet maintaining a high level of backward compatibility. Ethernet has essentially supplanted competing wired LAN technologies including Token Ring, FDDI, and ARCNET over time.

3.1 Attack 1 – Packet-in-Packet Attack

EtherOops is another name for the packet-in-packet attack. [6] When bit-errors occur randomly in transmissions, an attacker can leverage and manipulate them to insert completely controlled packets when they occur in a certain fashion.

The following are the steps to carry out this attack:

Step 1 - In Wi-Fi monitor mode, the attacker obtains the plaintext MAC addresses of possible target wireless devices and their nearest router.

Step 2 - The attacker iterates over all available 16-bit source ports, sending faked DNS answer packets from the Internet to the target network's external Internet IP address.

Step 3 - At this stage, the attacker can transmit acceptable UDP packets to a device behind the Wi-Fi AP with controlled payloads. These packets will carry the packet-in-packet payload from the Internet at high throughput.
Step 4 - Parallel to this, the attacker activates the EMP device and watches for bit flips on the unshielded wire. The EMP is constantly emitting high-frequency pulses. The packet-in-packet situation is attained once the correct bit flip happens, and a fully controlled packet is injected.

3.2 Attack 2 - LANtenna Attack

LANTENNA is an electromagnetic attack that uses Ethernet networking cables to leak data from air-gapped networks wirelessly. [7] Malware installed on a hacked computer or server can control the electromagnetic waves sent by an Ethernet cable, effectively turning it into a broadcasting antenna.
There are two essential steps in the adversarial attack model:

1. Infection and Reconnaissance

Lockheed Martin created the APT Kill Chain concept, which categorises seven stages of targeted cyber-attacks. Reconnaissance, weaponization, delivery, exploitation, installation, Command & Control, and data exfiltration are the seven common phases of APT incursions. Reconnaissance, delivery, and exfiltration are the relevant phases to consider in the context of our job. During the reconnaissance phase, the attackers use numerous tools and strategies to gather as much information as possible about their target. After determining the first target, attackers may use a variety of infection vectors to infiltrate the network, including supply chain attacks, tainted USB drives, social engineering tactics, stolen credentials, and malevolent insiders or mislead employees.

2. Data Exfiltration

The attacker may collect data from the compromised systems as part of the APT exfiltration phase. Documents, databases, access passwords, encryption keys, and other types of data can all be stolen.
Data transmission: Once the data has been gathered, the virus uses the covert channel to exfiltrate it. In the case of a LANTENNA attack, it modulates the data and sends it wirelessly across the Ethernet cables' radio waves.
Data reception: The covert communication can be received by a nearby radio receiver, which decodes it and sends it to an attacker. The receiving gear could be carried or disguised by a malevolent insider.

C. Comparative Analysis in tabular format

Ports	**Attacks**	**Component hampered (according to CIA triad model)**
USB	Fork Bombing using a USB cable and Digispark ATTIny85 Arduino board	Availability
USB	Reverse shell using Digispark ATTIny85 Arduino board	Confidentiality, Integrity, Availability
USB	Data Infiltration Attack using Rucky.	Confidentiality
USB	Ransomware attack using Rucky.	Availability
USB	Disable Windows Firewall using Raspberry Pi Pico.	Confidentiality, Integrity, Availability
USB	Net Disabler using Raspberry Pi Pico	Availability
USB	Disk wiper using Raspberry Pi Pico	Availibility
USB	Gaining Reverse shell in Linux using Raspberry Pi Pico	Confidentiality, Integrity, Availability
HDMI	Topology Inference Attack	Confidentiality
HDMI	CEC-Based Eavesdropping	Confidentiality
HDMI	WPA/WPA2 (wifi protected access Handshake theft)	Confidentiality, Integrity, Availability
HDMI	Targeted Device Attack	Availability
HDMI	Display Broadcast DoS	Availability
Ethernet (RJ45)	EtherOops	Confidentiality, Integrity, Availability

Ethernet ((RJ45))	LANtenna Attack	Confidential

Table 1. Comparative Analysis of various Attacks performed.

III. CONCLUSION AND FUTURE SCOPE

A. *Scope*

The current version of the project covers only a limited range of attacks on three ports. Following list contains a set of possibilities for improvement and further expansion of the research:

1. The Comparative study can be further expanded to cover more advanced ports including the thunderbolt ports and lightening ports.
2. More complicated and sophisticated attacks like power hammering and mosquito attack can also be performed and its effects can be monitored on the Power port and 3.5 mm audio jack respectively.
3. More parameters other than the C.I.A. Triad can also be taken in consideration for attacks on future hardware ports involving new technologies.
4. Comparative Analysis can be extended from covering only computer system to covering various devices that can be connected through physical cables including mobile systems

B. *Conclusion*

In the current technically advanced world, most of the computer systems possess threats of infection through the hardware ports since cybercriminals and hackers are always thinking of clever, new ways to exploit your devices. A malicious cable can compromise security of the computer system. We performed Vulnerability checks on the most common hardware ports that are found on existing computers in use by infecting them using various cables and different payloads and summarized the effects of these attacks. Our analysis classifies the effects after infection under the fundamental security triad “The C.I.A. Triad” (C.I.A. stands for Confidentiality, Integrity, Availability of data). Our project gives a broad perspective of the fact that security of a computer system can be compromised just with the use of a faulty or malicious cable.

REFERENCES

[1] Connecting and Programming Your Digispark. URL: https://digistump.com/wiki/digispark/tutorials/connecting

[2] USB Rubber Ducky. URL: https://shop.hak5.org/products/usb-rubber-ducky-deluxe

[3] Sumeet Kumar. "Simulating DDoS attacks on the us fiber-optics internet infrastructure" Winter Simulation Conference, 2017.

[4] Dave (Jing) Tian ,Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bate, Kevin R. B. "SoK: “Plug & Pray” Today – Understanding USB Insecurity in Versions 1 through C". IEEE Symposium on Security and Privacy, 2018

[5] Luis Puche Rondon, Leonardo Babun, Kemal Akkaya, and A. Selcuk Uluaga. "HDMI-Walk: Attacking HDMI Distribution Networks via Consumer Electronic Control Protocol". ACSAC’19.

[6] Exploit utilizing packet-in-packet attacks on ethernet cables to bypass firewalls & NATs. URL: https://www.armis.com/research/etheroops/

[7] LANtenna attack allows exfiltrating data from Air-Gapped systems via Ethernet cables URL: https://securityaffairs.co/wordpress/123008/hacking/lantenna-attack-exfiltration-technique.html