IPEC Journal of Science & Technology, Vol. 02 (01), June 2023
ISSN: 2583-3286(Online)

Design And Development of USB Cauterizer

Ajay Chauhan, Kartikey Bhardwaj, Jinendar Kothari, Aman Nagar
Department of Electronics and Communication Engineering
Inderprastha Engineering College, Ghaziabad, Uttar Pradesh, India

***Abstract* - In this paper we are deploping USB Cauterizer using the Altium Design tool for designing our hardware from scratch to complete the board, nowadays Altium is a highly demanded tool in the PCB industry. On the other hand, we will be using Linux OS for writing our program in Bash to detect the Integrity, Confidentiality and authenticity of the files present in a USB drive for real life real-life applications, this project is a combination of two emerging domains i.e. Electronics Domain and The cyber Security Domain. This project is focused on designing our raspberry pi using the Altium Design (V-20) Tool which is extended further to the application of the Designed Raspberry Pi in the cyber security domain.**

Keywords – Raspberry Pi4, USB, Spyware, Cyber Security, PCB Designer.

I. INTRODUCTION

Nowadays, everything in our life is shifting toward digitalization. Technological advancements are happening every day and the world is trying to catch up with these advancements. Due to this digitalization, our data is constantly present on some server of a certain company, which leads us to think about who or what is protecting our precious data. If these stores do not have proper security Implementations to comply with, it could lead to a cyber-attack that will put our data into jeopardy. Now, the first step taken by any hacker is to gain access to the network on which the server is running.

If you work in IT Sector, you've probably had someone show up at your office with a questionable USB drive they want you to check out. Now, you plug that USB drive without checking it and that's it. They gain access to your system and now it can be used to move anywhere, gain privileges within the network, and ultimately accessing access the server.

So, to stop all of these things to happen, we need to put up our defense in the very first step. We have come up with a tool which can reduce the risks of a company falling into a cyber-attack and ultimately reducing reduce the chances of our data falling in the wrong hands.

II. LITRETURE SURVEY

USB sticks are a common vector of infection for malware, and their abuse is prevalent. For instance, lost USB devices have a 66% chance of containing malware and infecting their victim. "USB CAUTERIZER" is an independent hardware solution to clean documents from untrusted (obtained) USB keys / USB sticks. The device has an automatic feature that transforms untrusted documents into a readable yet disarmed format. It then saves these sanitized files on a USB device that is owned by the user and considered trustworthy.

The focus of "USB CAUTERIZER" is to accept document exchange even if the used transport layer (the USB device) cannot be trusted or if there is a suspicion about whether Can the documents contained within the device be infected with malware?

In the worst case, only the "USB CAUTERIZER" would be compromised, but not the computer reading the target (trusted) USB device The code runs on a Raspberry Pi (a small hardware device), which also means it is not required to plug the original USB device into a computer. "USB CAUTERIZER" can be seen as a kind of air gap between the untrusted USB device and your operational computer.

This mounting script is used to mount a given bootable image file in loop mode and make debugging easier. The mounting script double-checks the path and offsets to install boot image.

We also specify the locations at which we'd like the Partitions to be mounted.

After mounting the partition Offsets are calculated for each partition and logic is added for creating directories if they aren't already there.

Cybersecurity refers to the process of implementing

Date of Submission: 05 May 2023
Date of Acceptance: 20 June 2023
Corresponding Author: Kartikey Bhardwaj
(E-mail: kartik01bhardwaj@gmail.com).

ISSN: 2583-3286(Online)

measures to mitigate security concerns in order to protect an organization from reputation damage, commercial loss, or financial loss. This type of security is specifically designed for networks or systems that are accessible via the internet. A variety of tools and techniques are used to deploy cybersecurity, and it is important to note that it is not a one-time process but an ongoing one that requires regular updates to keep the risk low.

Implementing cybersecurity measures can make work much easier by ensuring the availability of resources within a network. Failure to prioritize the safety of an online presence can result in significant losses for a business or organization. In today's connected world, everyone benefits from advanced cyber defense strategies. Cybersecurity breaches can range from identity theft to the destruction of vital data, and it is crucial to secure critical infrastructure such as power plants, hospitals, and financial service providers to maintain a functioning society.

A. *Type of cybersecurity threats*

There are several types of cybersecurity threats, including phishing, ransomware, malware, and social engineering.

B. *Phishing*

Phishing involves the distribution of fake emails that appear to be from legitimate sources with the goal of stealing sensitive data such as credit card details and login information

C. *Ransomware*

Ransomware is a type of malicious software designed to extract money by blocking access to files or the entire system until a ransom is paid.

D. *Malware*

Malware is any software designed to gain unauthorized access or cause damage to a system.

E. *Social Engineering*

Social engineering involves tricking individuals into divulging sensitive information through techniques such as requesting a financial payment or gaining access to personal information. These tactics can be combined with other strategies to increase the likelihood of clicking on links, downloading malware, or trusting a malicious source.

The primary goal of cybersecurity is to prevent the theft or compromise of data. To achieve this, there are three essential objectives of cybersecurity which are as follows:

1. Ensuring the Privacy of Information
2. Maintaining the Integrity of Information
3. Regulating the Accessibility of Information only to authorized users.

These objectives are based on the confidentiality, integrity, availability (CIA) triad, which serves as the foundation of all security measures. The CIA triad model is a safety model designed to guide strategies for data security in organizations or corporations. It is important to note that all three elements of the triad are critical to data security, and therefore, must be implemented together.

The CIA triad is the most widely used standard to evaluate, select, and apply appropriate security controls to reduce risk.

Confidentiality

The first element of the triad is confidentiality, which ensures that complex statistics are accessible only to authorized users and that no information is revealed to unintended parties. Methods to safeguard confidentiality include data encryption, two or multifactor authentication, and confirming biometrics.

F. *Integrity*

The second element is integrity, which ensures that all data is accurate, reliable, and not altered in transit from one fact to another. Measures to ensure integrity include operator contact controls, appropriate backups, and version supervision.

G. *Availability*

The third element is availability, which ensures that data is always available to authorized users without any interruptions or delays. To maintain availability, it is essential to categorize possessions based on their position and precedence, hold down possible threats, determine the method of security guards for each threat, monitor any breaching activities, manage data at rest and data in motion, and update policies to handle risk based on previous assessments.

III. SCHEMATIC

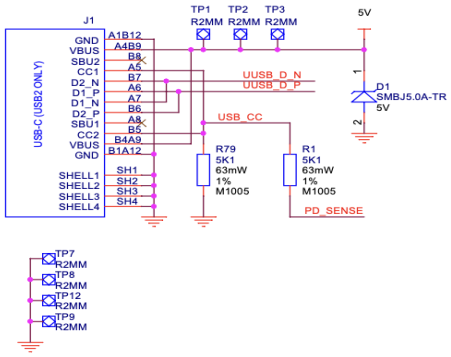

Figure. 1 Micro USB Port.

ISSN: 2583-3286(Online)

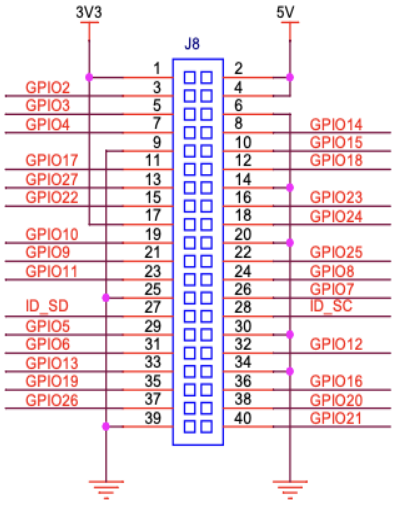

Figure. 2 GPIO

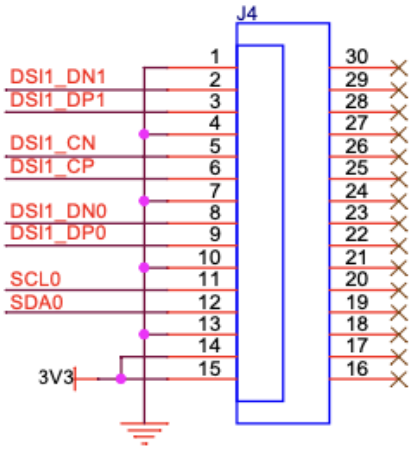

Figure. 4 Display Port

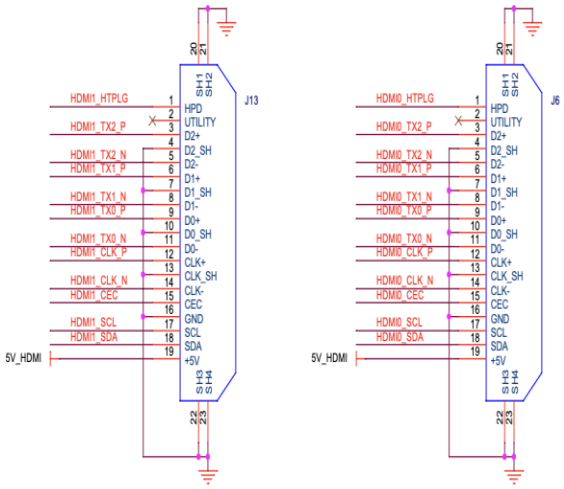

Figure. 3 HDMI Port

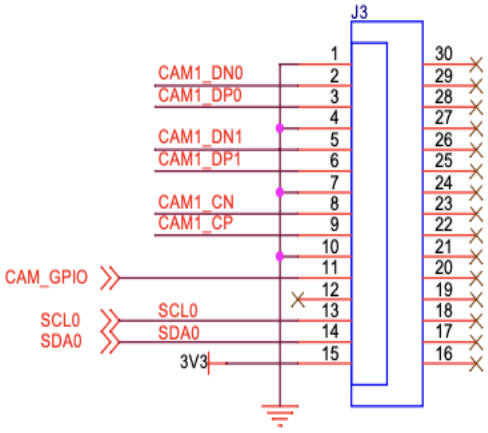

Figure . 5 Camera Port

ISSN: 2583-3286(Online)

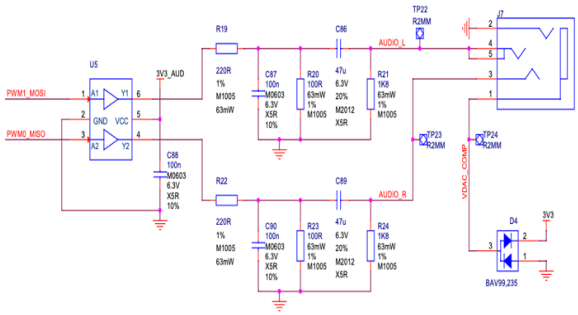

Figure . 6 Audio Video Jack

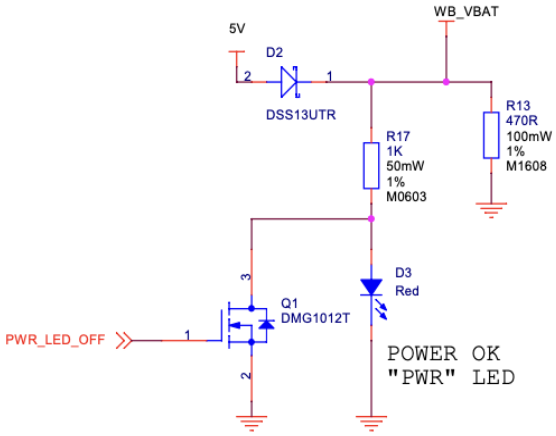

Figure . 7 Power LED

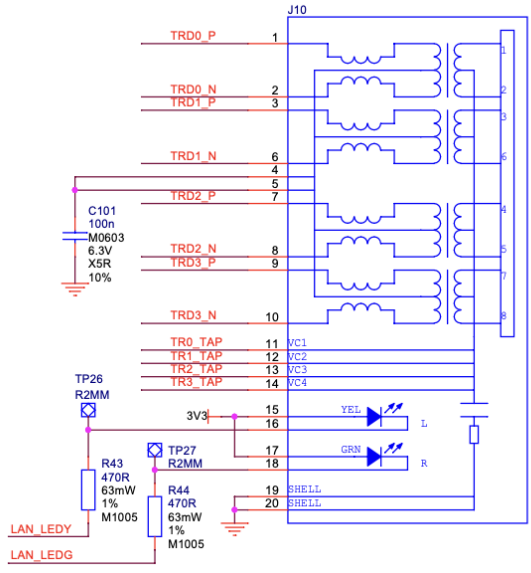

Figure . 8 Ethernet Port

IV. WORKING

We design our project from zero, in which we design our controller board which is popularly named Raspberry Pi, we are using the Altium design tool, this tool provides us with the freedom to make our library and use them. Firstly, we are making a schematics library then we are moving to our next step. i.e., PCB library schematics, in schematics library we have to make a symbol of our component after a complete study of our datasheet we move to 3d diagram modelling. i.e., PCB library schematics, in this we are making schematics in 3D, where we can use a Step file 3d model of components and ICs, according to our desired dimensions after that we again move to our previous step where we have already designed our schematics symbols, now we attached both symbol and 3D model to each other, then save the file, now our component is ready to place at a board.

After these two steps, we moved ahead toward our third step. i.e., Schematics sheet design, in which first we are changing the measuring scale typically it is in the mill but we are changing our scale to mm scale according to industry point of view mm in standard, then we move to the sheet property and set the alignment of sheet typically we are taking an A4 sheet and then set all the parameters of the sheet after applying all the changes on the sheet we start our design and after design validates our design and check the error message if we get an error then correct that node/terminal of the component after all these things save the file and move towards next step. i.e., PCB Design,

In this firstly we save that file in the same location where we save our previous sheet then we import the sheet in PCB Design file, we import all the components except Vnet, Class member, some unusable nets and background frame as well, After importing all the component we will properly arrange all the component after arrangement we will go to board planning mode and adjust a board shape.

After that, we will start routing but before routing we have to adjust everything firstly we have to set the masking and clearance of the wire, the width of the routing wire also gets from IPC Standard, for example for 1 Amp. Current the width of the wire is 0.74mm, for every value of current there are different widths of wire, and there are some specific formulas for finding the width of wire there were some fixed IPC rules, after that, we set the layer of PCB typically PCB are of 2 layers with single plane wire in order of solder mask layer, high-speed signal layer, core, bottom high-speed layer, bottom solder mask, this is a structure of 2 layer PCB, here core is a hard part which makes PCB rigid, mainly we are friendly with 2 types for PCB one is wooden which are look brown in colour and the other one is of Epoxy, which varies from FR-2 to Fr-6, which looks Green, Blue, Red, white and different colour, FR-4 is widely used

ISSN: 2583-3286(Online)

epoxy material for designing PCB, there is a different layer of PCB which we are used according to our requirements according to PIN density we are select our layers, there are minimum 2 layer and maximum 14 layers of board and the width of PCB board is fixed. i.e., 1600uM, PIN density also we get from standard IPC formula, after settling all the things we start routing of component, there are three types of routing, Blind Via, Buried Via, Through hole Via, After completing all the things save our file and Generate our Gerber file after creating Gerber file we add drill pad in our PCB design the generate Holes file after generating that, we will create smart PDF in which we can attach both the file and also BOM – Bill Of Material, which will send to the manufacturer for manufacture our desire PCB.

After Receiving the PCB board, we will start configuring it in Linux We will write bash scripts and confit here it in such a way that the services start with the insertion of the USB drive and detection could be initiated, For the detection of malicious files we have written bash scripts.

First bash script updates the system requirements and dependencies. Second script is used to copy the meta-data of the files. Metadata is essentially information that describes certain aspects of data, rather than the data itself. It includes details such as the title of the data, how the data is structured (such as page order), when and who created the data, and even lists of websites visited by individuals. In other words, metadata is data about the data.

The third script also called as mounting script will be used to check the meta data of the file and analyse it and mark it as dangerous if it is dangerous. This script runs in a loop mode to check every file in the untrusted USB key.

V. Output Result

The malicious USB drive consists of 18 items including audio file, windows executable file, Word file etc. We have taken the files consisting of different virus, malwares and ransomwares to check whether the USB cauterizer is detecting the harmful files with same efficiency or not, The malicious files from malicious USB drive is taken and processed. After processing the content of the files, all files, which are dangerous, are isolated and marked dangerous. Now, these files are copied to the Safe USB drive

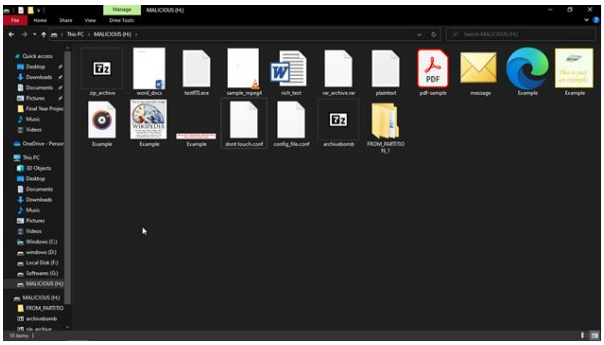

Figure . 9 Files present in the malicious drive

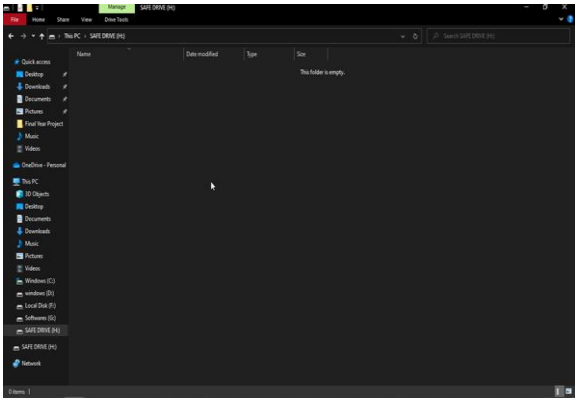

Figure. 10 content of safe drive before using usb cauterizer

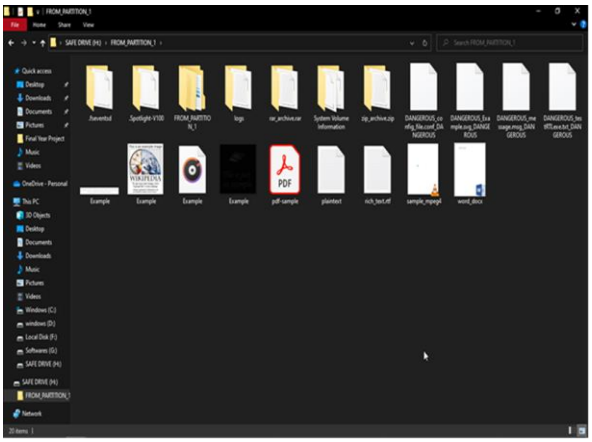

Figure. 11 contents of safe drive after using usb cauterizer

References

[1] Laura M., “What is Cyber Security: Learning About the Network Security”,

[2] N.M. Singh, K. C. Sarma, N.G. Singh, “Design and Development of Low Cost Multi-Channel USB Data”, International Journal of Computer Applications 48(18) July 2012

[3] A. Sheth, S. Bhosale, F. Kurupkar, “Research Paper on Cyber Security”, contemporary research in india (issn 2231-2137): special issue : april, 2021

[4]https ://www.raspberrypi.com/documentation/computers/raspberry-pi.html

[5] https://cltc.berkeley.edu/scenario-back-matter/