Savitribai Phule Pune University, Pune

A Project Report

on

FIRMWARE SECURITY

Submitted by

Mr. Amit Vitekar	**B150323144**
Miss.Anushri Dabhade	**B150323004**
Miss.Pradnya Paigude	**B150323064**

Under the guidance of

Dr. P.N. Kota

Department of E&TC Engineering

Modern Education Society's

College Engineering, Pune-411 001

[2018-19]

MODERN EDUCATION SOCIETY'S

College of Engineering, Pune-01

CERTIFICATE

This is to certify that the project work entitled **"FIRMWARE SECURITY"** is a bonafide work carried out by

Mr. Amit Vitekar	**B150323144**
Miss.Anushri Dabhade	**B150323004**
Miss.Pradnya Paigude	**B150323064**

In partial fulfilment for the award of Bachelor of Engineering in E&TC Engineering of the Savitribai Phule Pune University during the year 2018-19. It is certified that all the corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the department library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering degree.

Dr. P.N. Kota
Guide
Dept of E&TC Engineering
MESCOE Pune-411001

Dr. P. B. Chopade
Head of Department
Dept of E&TC Engineering
MESCOE Pune-411001

Prof. Kadam R.S.
Project Coordinator, E&TC
MESCOE, Pune-411001

Dr. A. A. KESTE
Principal
MESCOE, Pune-411001

External Examiner

ACKNOWLEDGEMENT

It gives us an immense pleasure to express our gratitude and thanks to all those who helped in the timely completion of the project work.

We have a great pleasure in expressing our deep sense of gratitude and indebtedness to **Dr. P. B. Chopade**, Head of Department, Department of E&TC Engineering, Modern Education Society's College of Engineering Pune for their invaluable guidance, constant supervision and sustained encouragement throughout the tenure in this project work.

We would like to express our thanks to **Dr. P.N. Kota,** Project Guide, for his constant support and encouragement.

We would like to express our thanks to **Dr. A. A. Keste**, Principal, Modern Education Society's College of Engineering Pune for permitting us to take up the project work.

We are thankful of our parent and friends for their kind help and support throughout the course.

Mr. Amit Vitekar

Miss.Anushri Dabhade

Miss.Pradnya Paigude

ABSTRACT

Internet of Things (IoT) is fast becoming a disruptive technology business opportunity, with standards emerging primarily for wireless communication between sensors, actuators and gadgets in day-to-day human life, all in general being referred to as "Things". This offers the capability to measure for understanding environment indicators. This paper addresses the internet of things (IoT) as the main enabling factor of promising paradigm for integration and comprehensive of several technologies for communication solution, Identification and integrating for tracking of technologies as wireless sensor and actuators. IoT as envisioned is billion sensors connected to the internet through the sensors that would be generate large amount of data which need to analysed, interpreted and utilized.

Being surrounded by smart devices made me think how must've the developers, designers and engineers made so small gadgets so much powerful? As much as they're powerful are they really secure? Is the user who daily relies on the gadget for his personal assistance truly being given the privacy he needs? Are the gadgets completely following the commands stated only by the owner and not some intruder? Most importantly is the firmware which handles all the communication and bridges the hardware, network and application layer completely secure? If not, what possible ways could one exploit it and abuse it?

Designing and developing firmware's or the so-called embedded Linux operating systems which are hardly 10 megabytes in size and consume few hundred megabytes of flash storage in your smart device made me curious to study about all the error correction, security mechanism and other protocols that are being embedded into these firmware's. From reverse engineering proprietary firmware's of various vendors to building some of my own firmware's from scratch led me to survey the different security vulnerabilities and various mitigation techniques being used in them and for prevention of the same.

TABLE OF CONTENTS

List of figures

CHAPTER 1

INTRODUCTION

1.1. Background

The Internet of Things (IoT) opens opportunities for wearable devices, home appliances, and software to share and communicate information on the Internet. Given that the shared data contains a large amount of private information, preserving information security on the shared data is an important issue that cannot be neglected. We begin with general information security background of IoT and continue on with information security related challenges that IoT will encountered.

Firmware plays an important role in any IoT device with providing new features and running high end applications on an IoT device it becomes very essential to focus on different vulnerabilities present in these firmware's that can cause huge loss of private data and breach of security.

Embedded systems play a vital role in the development of an IoT device but not implementing preventive measures against hardware attacks and exploitation of different communication protocols can lead to heinous consequences.

1.2 Problem Statement

To prevent and mitigate various cybersecurity attacks on the IoT device and develop secure systems and to prevent the same attacks in the future.

1.3 Objectives

- To study and analyse the IoT hub device and various protocols and modules it supports

- To study and analyse the firmware and understand the internal working of the same also study the security vulnerabilities if any present in the firmware's or try to find some.

- To survey all the different security vulnerabilities found and propose techniques or methods for their mitigation.

CHAPTER 2

LITERATURE SURVEY

We have studied the Wink Hub 1 by Wink Inc. which is an IoT hub device that supports different RF protocols like Zigbee, Wi-Fi/BT: 802.11bgn (2.4GHz), Kidde (433MHz), Lutron (433MHz) and is vulnerable to different attacks on the hardware and firmware level.

"Vulnerabilities in Hub Architecture IoT Devices"
In this paper the author has reverse engineered the IoT hub devices analysed the specs of the devices, its protocols, firmware that runs on top of the devices etc. The author has studied in-depth various security attacks on the Embedded device and applied the same on the IoT hub devices.[1] The author has also suggested various mitigation techniques to prevent the attacks in the future.

"IoT Security: An End-to-End View and Case Study"
Comparing the various protocols an IoT device uses with the OSI model of networking the author has done an End-to-End case study i.e. in-depth study of various protocols and technologies used at each layer of the OSI model and the attacks possible on them along with mitigation techniques to prevent the same.[2]

"Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: A Survey of Potent Micro architectural Attacks "
The author describes various attacks possible on the hardware arch of the device be it on the physical bare metal or manipulating and corrupting the instructions running on the SoC or microcontroller which causes the system to misbehave and leak all the crucial information it possesses.[3]

CHAPTER 3

THEORY AND CONCEPTS

3.1 What Is the Internet of Things (IoT)?

The Internet of Things may be a hot topic in the industry but it's not a new concept. In the early 2000's, Kevin Ashton was laying the groundwork for what would become the Internet of Things (IoT) at MIT's Auto ID lab. Ashton was one of the pioneers who conceived this notion as he searched for ways that Proctor & Gamble could improve its business by linking RFID information to the Internet. The concept was simple but powerful. If all objects in daily life were equipped with identifiers and wireless connectivity, these objects could be communicating with each other and be managed by computers. In a 1999 article for the RFID Journal Ashton wrote: "If we had computers that knew everything there was to know about things—using data they gathered without any help from us -- we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe identify and understand the world—without the limitations of human-entered data."1 At the time, this vision required major technology improvements. After all, how would we connect everything on the planet? What type of wireless communications could be built into devices? What changes would need to be made to the existing Internet infrastructure to support billions of new devices communicating? What would power these devices? What must be developed to make the solutions cost effective? There were more questions than answers to the IoT concepts in 1999. Today, many of these obstacles have been solved.

The size and cost of wireless radios has dropped tremendously. IPv6 allows us to assign a communications address to billions of devices. Electronics companies are building Wi-Fi and cellular wireless connectivity into a wide range of devices. ABI Research estimates over five billion wireless chips will ship in 2013.2 Mobile data coverage has improved significantly with many networks offering broadband speeds. While not perfect, battery technology has improved and solar recharging has been built into numerous devices. There will be billions of objects connecting to the network with the next several years.

3.2 Why to use IoT?

IoT communicates information to people and systems, such as state and health of equipment (e.g. it's on or off, charged, full or empty) and data from sensors that can monitor a person's vital signs. In most cases, we didn't have access to this information before or it was collected manually and infrequently. For example, an IOT-enabled HVAC system can report if its air filter is clean and functioning properly. Almost every company has a class of assets it could track. GPS-enabled assets can communicate their current location and movement. Location is important for items that move, such as trucks, but it's also applicable for locating items and people within an organization. In the healthcare industry, IoT can help a hospital track the location of everything from wheelchairs to cardiac defibrillators to surgeons. In the transportation industry, a business can deliver real-time tracking and condition of parcels and pallets. For example, Maersk can use sensors to track the location of a refrigerated shipping container and its current temperature. In a connected world, a business will have visibility into a device's condition. In many cases, a business or consumer will also be able to remotely control a device. For example, a business can remotely turn on or shut down a specific piece of equipment or adjust the temperature in a climate-controlled environment. Meanwhile, a consumer can use IoT to unlock their car or start the washing machine. Once a performance baseline has been established, a process can send alerts for anomalies and possibly deliver an automated response. For example, if the

brake pads on a truck are about to fail, it can prompt the company to take the vehicle out of service and automatically schedule maintenance.

Many companies will adopt IoT to save money. Measurement provides actual performance data and equipment health, instead of just estimates. Businesses, particularly industrial companies, lose money when equipment fails. With new sensor information, IoT can help a company save money by minimizing equipment failure and allowing the business to perform planned maintenance. Sensors can also measure items, such as driving behaviour and speed, to reduce fuel expense and wear and tear on consumables. New smart meters in homes and businesses can also provide data that helps people understand energy consumption and opportunities for cost savings' (IOTG) predicts there will be over 50 billion connected devices by 2020.

IoT describes a system where items in the physical world, and sensors within or attached to these items, are connected to the Internet via wireless and wired Internet connections. These sensors can use various types of local area connections such as RFID, NFC, Wi-Fi, Bluetooth, and ZigBee. Sensors can also have wide area connectivity such as GSM, GPRS, 3G, and LTE. The Internet of Things will connect both inanimate and living things. Early trials and deployments of Internet of Things networks began with connecting industrial equipment. Today, the vision of IoT has expanded to connect everything from industrial equipment to everyday objects. The types of items range from gas turbines to automobiles to utility meters. It can also include living organisms such as plants, farm animals and people. For example, the Cow Tracking Project in Essex uses data collected from radio positioning tags to monitor cows for illness and track behaviour in the herd. Wearable computing and digital health devices, such as Nike+ Fuel band and Fit bit, are examples of how people are connecting in the Internet of Things landscape. Cisco has expanded the definition of IoT to the Internet of Everything (IoE), which includes people, places, objects and things. Basically, anything you can attach a sensor and connectivity to can participate in the new connected ecosystems. Use sensors for data collection. The physical objects that

are being connected will possess one or more sensors. Each sensor will monitor a specific condition such as location, vibration, motion and temperature. In IoT, these sensors will connect to each other and to systems that can understand or present information from the sensor's data feeds. These sensors will provide new information to a company's systems and to people. Change what types of item communicate over an IP Network. In the past, people communicated with people and with machines. Imagine if all of your equipment had the ability to communicate. What would it tell you? IoT-enabled objects will share information about their condition and the surrounding environment with people, software systems and other machines. This information can be shared in real time or collected and shared at defined intervals. Going forward, everything will have a digital identity and connectivity, which means you, can identify, track and communicate with objects. IoT data differs from traditional computing. The data can be small in size and frequent in transmission. The numbers of devices or nodes that are connecting to the network are also greater in IoT than in traditional PC computing. Machine-to-Machine communications and intelligence drawn from the devices and the network will allow businesses to automate certain basic tasks without depending on central or cloud-based applications and services.

3.3 Project Overview

In this project we will analyse and assess a IoT hub device, we will look into its hardware components, firmware and RF protocols it supports. We will also look for default misconfigurations if any present in the device and try to exploit the same. Overall, we will try to hack the device and measure till what extent the attacker can leverage the system to get user data and corrupt/destroy the system remotely.

This system has following hardware components:

1. Wink Hub 1 by Wink Inc Corp.

2. Expliot Nano for JTAG

3. USB-TTL converter for communicating with UART port.

3.3.1 Feasibility Study

In our analysis the methodology we use is more feasible than the existing methods of measuring the patient body parameters.

1. Economical Feasibility

The existing devices are not so cheaper because it has many disadvantages like all systems are being designed for measuring a specific parameter only. The systems which are existing today are also pretty costly. Lot of IoT devices are needed in order to make the complete use of IoT hub device which increases the cost.

2. Operational Feasibility

The setup and operation is pretty easy as compared to other IoT devices even though some areas RF operation of Zigbee, Lutron etc sometimes becomes hectic.

3. Technical Feasibility

The existing methods must have a trained person to operate that system any one cannot operate the easily. If problem comes to user end it is not easy to solve. In our system it is very easy to operate and ordinary person who know to operate a pc can operate the software very easily for monitoring purpose.

CHAPTER 4

METHODOLOGY

We will examine the protocols and technologies used at each layer of the IoT and OSI model stack. Then we will study its internals, threats it possesses and the mitigation techniques for the same. In this way we will cover the most frequently used standards and protocols in the IoT systems. We will also analyse some case studies of various attacks and how it affected the device and services running on top of it also what various measures were taken by the vendors to prevent similar attacks in the future.

4.1 Service / System Scanning.

4.2 Vulnerability Analysis.

4.3 Study of Exploits.

4.4 Exploitation.

4.5 Post Exploitation.

4.6 Mitigation Techniques.

CHAPTER 5

BLOCK DIAGRAM

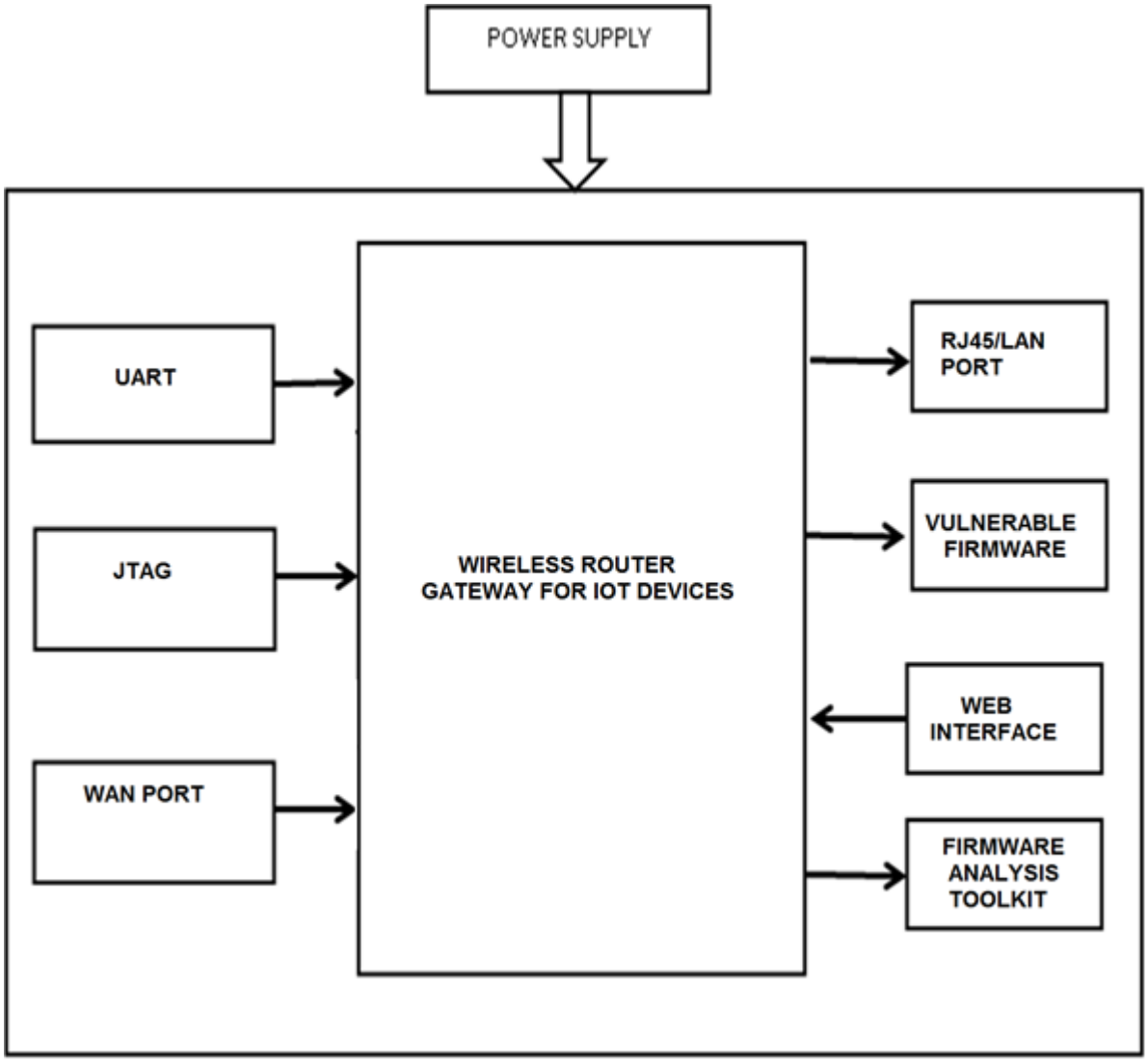


Fig: 5.1 Block diagram

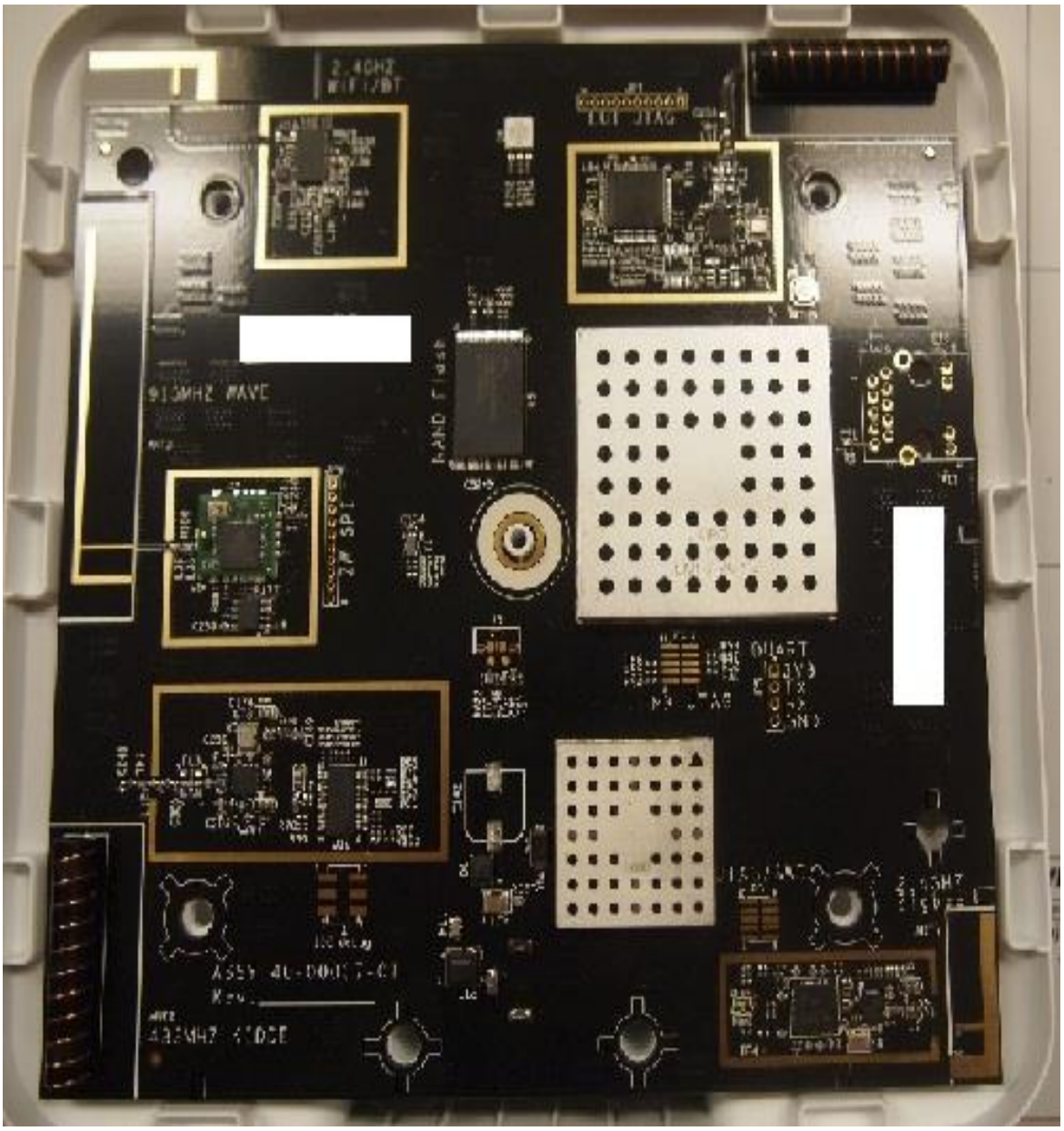


Fig: 5.2 Case diagram

5.1 Power Supply

The power supply specification for the wireless router is 12V/5A which powers the router.

5.2 UART (Universal Asynchronous Receiver/Transmitter)

UART stands for Universal Asynchronous Receiver/Transmitter. It's not a communication protocol like SPI and I2C, but a physical circuit in a microcontroller, or a stand-alone IC. A UART's main purpose is to transmit and receive serial data.

5.3 JTAG

JTAG is an industry standard for verifying designs and testing printed circuit boards after manufacture. JTAG implements standards for on-chip instrumentation in electronic design automation as a complementary tool to digital simulation.

5.4 WAN PORT (WIDE AREA NETWORK)

A WAN port is an RJ-45 Ethernet port on a router that is wired to a cable or DSL modem. On small routers, the WAN port may be labeled simply "Internet."

5.5 LAN PORT (LOCAL AREA NETWORK)

An RJ-45 Ethernet socket on a computer or network device such as a switch or router. All client machines, servers and network devices on the local network are cabled together at their LAN ports.

5.6 VULNERABLE FIRMWARE

Firmware is a software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.

5.7 WEB INTERFACE

The interaction between a user and software running on a Web server. The user interface is the Web browser and the Web page it downloaded and rendered. See Web application and Web server.

5.8 FIRMWARE ANALYSIS TOOLKIT

FAT is a toolkit built in order to help security researchers analyze and identify vulnerabilities in IoT and embedded device firmware.

Firmware Analysis Toolkit is built on top of the following existing tools and projects:

- Firmadyne
- Binwalk
- Firmware-Mod-Kit
- MITM-proxy
- Firmwalker

CHAPTER 6

PROTOCOL STACK & ITS THREATS

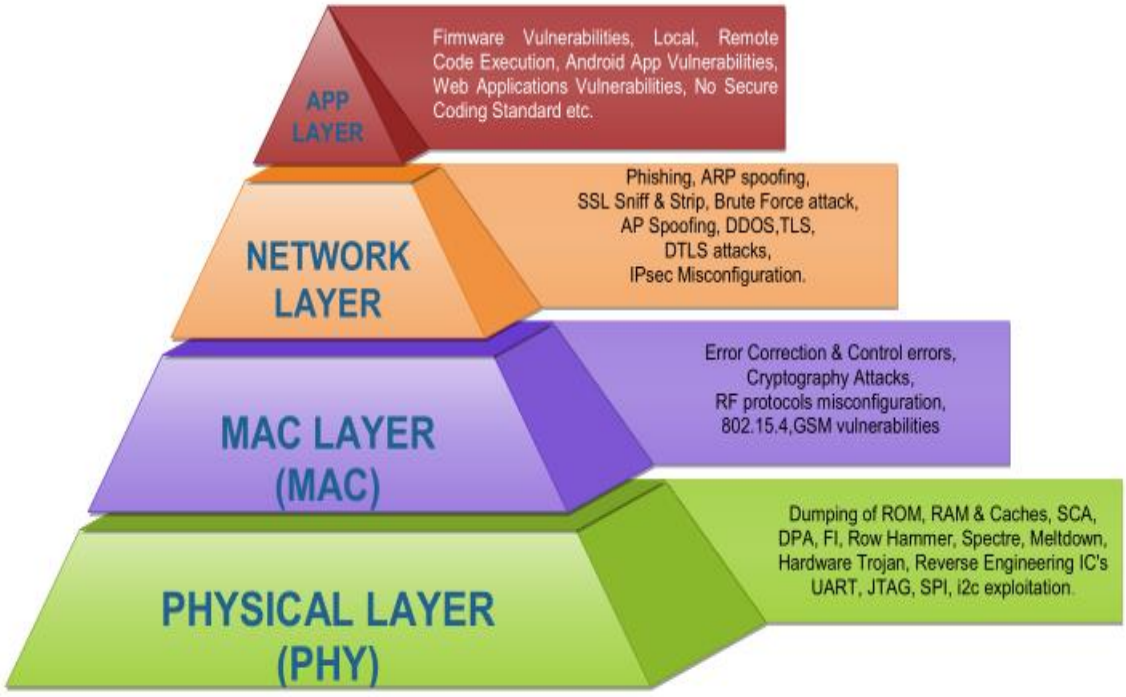


Fig.6.1 Protocol stack

6.1 PHYSICAL LAYER

In fig. the Physical Layer represents the hardware components of the IoT device. This mainly consists of the Printed Circuit Board (PCB) and the different components mounted upon it namely the System on Chip (SoC) or Network on Chip (NOC), NAND memory, GPU, Ethernet, USB ports, power jack, General Purpose Input Output Pins (GPIO) etc. Serial Communication peripherals like the Universal Asynchronous Receiver / Transmitter (UART) port, debug Interfaces like Joint Test Action Group (JTAG) help the attacker to exploit the device physically, using UART the attacker can communicate with the device and get complete super user (root) access to the firmware running on the device

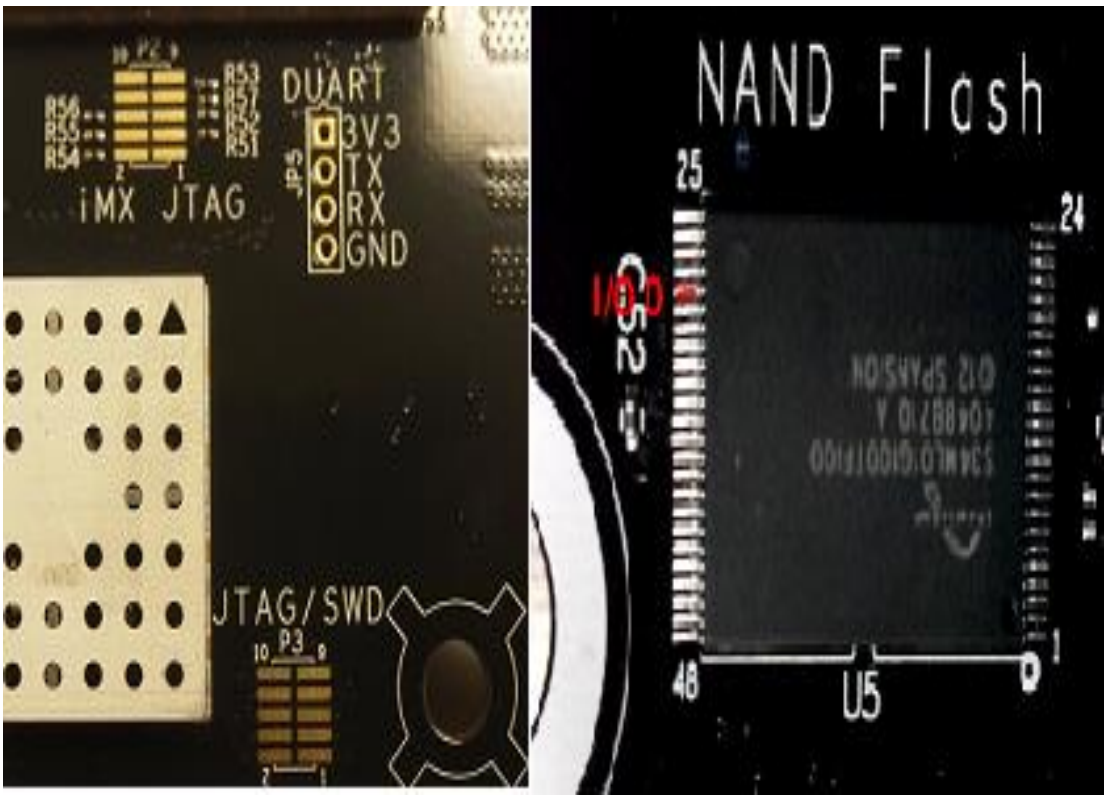


Fig. 6.1.1 UART, JTAG PORTS & NAND Storage.

As all this firmware binary files are stored into a storage medium like the NAND memory the attacker can easily access through the UART port or even debug the processor or RAM through a JTAG port using a JTAG adapter. Once the firmware is acquired the attacker can install a malware into the firmware as a module which can give remote root access.

In case of encrypted firmware the attacker can used hardware attacks like the Power Analysis (PA), Differential Power Analysis (DPA), Fault Injection (FI) and Timing Attacks (TA) suing these attacks the attacker can study at various instances of the firmware what are the encrypted private and public keys of the cryptographic algorithm stored and how can one extract those keys to decrypt the data. Carrying out these attacks is very tedious and time consuming also needs very good knowledge of hardware cryptography and its implementation.

To mitigate attacks at the PHY layer one should use strong passwords for UART ports and mostly scatter the JTAG pin-outs which make it difficult to debug the IoT device from a hardwareperspective.

6.2 MEDIA ACCESS CONTROL (MAC)

Form fig. 6.1 from [4] it is clear that the MAC layer resides above the PHY layer and its core functionalities are to implement and monitor various Error Checking &Correction (ECC) algorithms like the Cyclic Redundancy Check (CRC) which helps in detection whether is there any error in the data and to prevent the same by adding a parity bit into the data that is being processed. The MAC layer also implements various RF protocols like the ZigBee based on IEEE 802.15.4 Low Rate Wireless Personal Area Networks (LR-WPAN) which uses TLS as an encryption protocol and protocols like IPv6 Low Power Personal Area Network (6LoWPAN), Z-Wave, LoRA and other RF protocols.

The above stated RF protocols are vulnerable to various replay and brute force attack. An attacker can easily sniff the data packets at the operating radio frequencies like 315 MHz, 433 MHz or 868 MHz these are the most widely used radio frequencies for IoT protocols.

Using a Software Defined Radio (SDR) one can design a radio receiver for the stated frequencies using open source software like GNU Radio and other freely available tools like baud line, phosphor, RpiTx, gr-GSM etc.

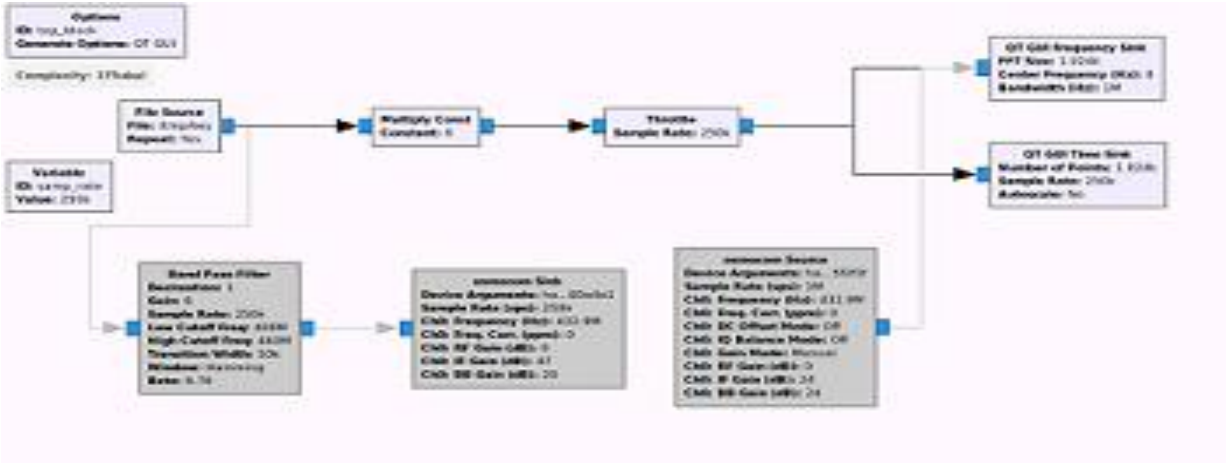


Fig. 6.2.1 Replay attack using GNU Radio.

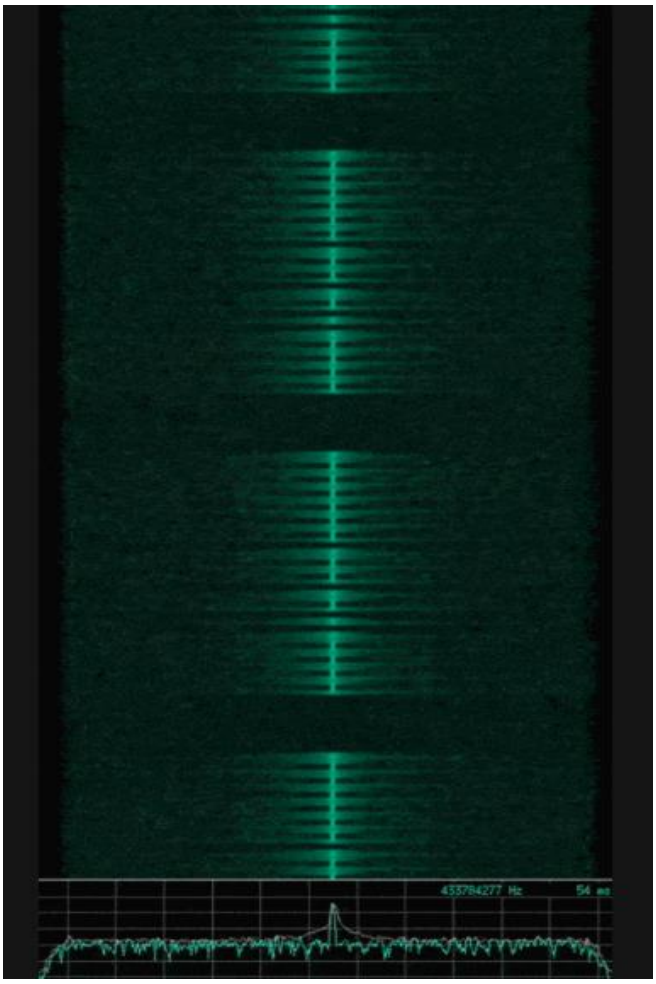


Fig. 6.2.2 Bits & Modulation inspection using Inspectrum.

The Fig 6.2.2 from [4] above shows the pulse width modulation technique being used by the RF protocol.

Fig. 6.2.3 Bits & Modulation reversing using Inspectrum.

In fig 6.2.1 we can see the GNU Radio (.grc) file which turns the SDR into a RF receiver and starts intercepting analog data being transmitted by the IoT device at 433.784 MHz In fig (D) and (E) once the bits are captured the attacker uses a software tool like Inspectrum or Universal Radio Hacker (URH) to analyze the frame structure of the data packets being transmitted.

After analysing we can conclude that it uses an On-Off Amplitude Shift Keying (OO-ASK) modulation technique to transmit data over the air. From fig 6.2.3[4] The structure is as follows 1 start bit, 6 bits Payload, 2 Parity bits and then a 1 bit for trailer which ends the signal. Now once the attacker knows this structure using a SDR he will replay this bit stream and start controlling the IoT device. The device starts intercepting the data being sent an follows the commands. There are some ways to mitigate these attacks i.e. to add some random bits every time the user sends commands over the air and only if these bits match then the device will execute certain commands etc.

6.3 Network Layer

The sole purpose of the Network Layer is to assign virtual addresses to the host and the IoT device and align them under the same network for ease of communication and data sharing. The network layer uses IPv4 & IPv6 to assign a unique IP address to the different devices connected on the same network for unique identification. It uses MAC address to link the devices to their IP addresses. The different service likes SSH, Telnet or some other proprietary protocols for remote communication are also deployed at the network layer.

The different attacks an attacker can perform at the network layer are Phishing, ARP spoofing i.e. spoofing ARP requests and forcing the host to believe a non-trusted device to be legit. Secure Socket Layer (SSL) sniffing and stripping i.e. using a protocol analyzer tool like Wireshark to capture data packets and filter the SSL packets to look for public and private keys being used for authentication. Brute Force attacks to try different combination of passwords to access unauthorized network services running on the device.

Access Point (AP) spoofing i.e. forcing the IoT device to associate to a fake wireless network by replicating the same properties of the legitimate wireless network and then stealing credentials like username and passwords from the device and different nodes connected to it. One of the most deadly attacks being the Denial of Service (DOS) or Distributed Denial of Service (DDOS) in which the attacker sends N number of infinite request to the device which causes the device to malfunction and give unauthorized access to the network.

Last but not least is the network misconfiguration the vendors and the end user do to the device making the device more vulnerable to network based attacks and compromise data. Mitigation of such attacks is mainly by using strong encryption algorithms, enabling strict MAC based authentication and using firewalls which give limited access to the network services of the device being connected to the network. Securing the network layer is as important as securing the physical and mac layer is because of the advancements in the routing algorithms and invention of new protocols it becomes necessary to pay close attention to network security of the devices and network they connect to.

6.4 Application Layer

The top most layer in fig. 6.1 Is the application layer this layer in the IoT stack uses various user interfaces to help the user interact with the device locally or remotely. Usually a web application running php on lightweight server like light-httpd hosts dynamic web pages programmed using HTML5, CCS3 etc. to provide a user friendly interface. In the back-end these web pages execute commands over the command line shell which in return controls the device remotely over the internet or helps configuring the same. The various functionalities like configuring the network subnet, access to android apps for remote access, customizing the voice commands and alerts for various activities etc. are some functionalities which can be configures using this interface.

The vulnerabilities lie in the web applications running on these devices or the Linux firmware which controls it. Vulnerabilities like SQL (Structured Query Language) injection, XSS (Cross Site Scripting), CSRF (Cross Site Request Forgery) etc. can give an attacker remote access to the device as the services which are vulnerable to these attacks use API's to communicate with the Linux Kernel running in the backend. Talking about the Linux Kernel it being open source and most widely used firmware in most of the IoT device is vulnerable to a lot of memory corruption attacks like Stack Overflow, Heap Overflow etc. type confusion bugs like the Use-After-Free bug which leads to access of the core services running on the kernel and once remotely compromised lives the device vulnerable to any attacker who is aware of the vulnerabilities can easily access the device once the IP address of the device is known.

The other way to compromise a device at an application layer would be to write a malware and spread it across one IoT device which will infect other devices on the same network and in return gives complete access of all the devices on the network. There is also quite a possibility that it might infect the remote server of the vendor which sends Over the Air (OTA) updates for the devices compromising N number of devices can create a huge botnet which in turn can be used for illegal purposes like mining crypto currencies, launching a DDOS attack on some government site or even disrupting services on network.

CHAPTER 7

HARDWARE ANALYSIS

Fig.7.1 WINK HUB 1

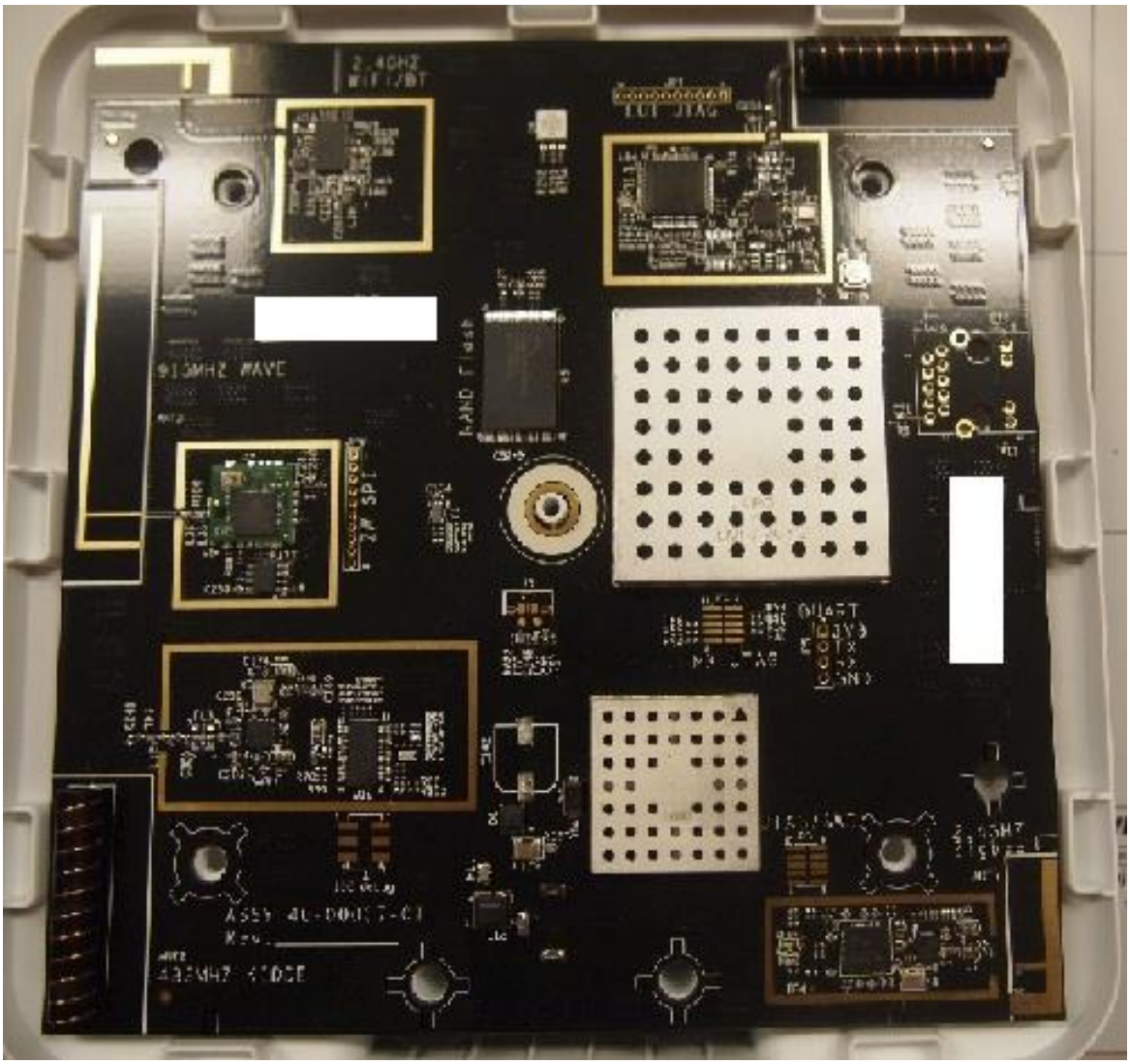


Fig.7.2 Analysis Board

7.1 UART port is enabled.

UART stands for Universal Asynchronous Receiver/Transmitter. It's not a communication protocol like SPI and I2C, but a physical circuit in a microcontroller, or a stand-alone IC. A UART's main purpose is to transmit and receive serial data. UARTs transmit data asynchronously, which means there is no clock signal to synchronize the output of bits from the transmitting UART to the sampling of bits by the receiving UART. Instead of a clock signal, the transmitting UART adds start and stop bits to the data packet being transferred. These bits define the beginning and end of the data packet so the receiving UART knows when to start reading the bits.

We have used a USB-TTL converter to interface laptop and UART port of Wink Hub 1.

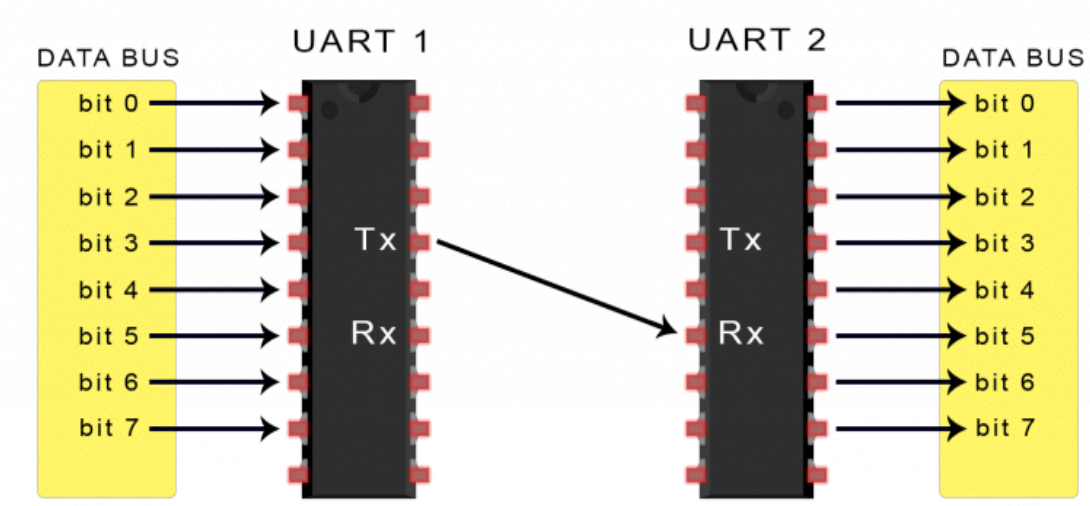


Fig. 7.1.1 UART Basics

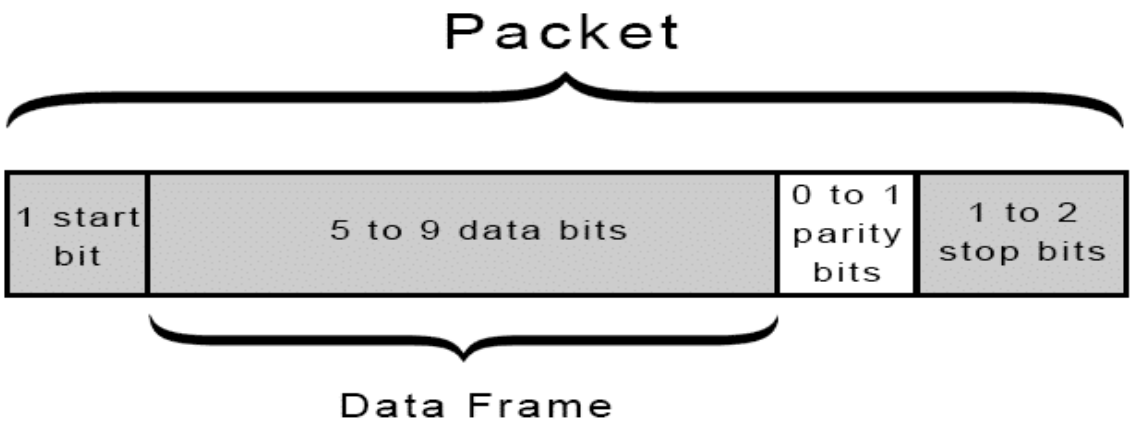


Fig 7.1.2 UART frame structure

Usually UART should have a password to protect it from unauthorized access. In this case as it was not password protected the attacker could use USB-to-UART converter and access the firmware running inside it.

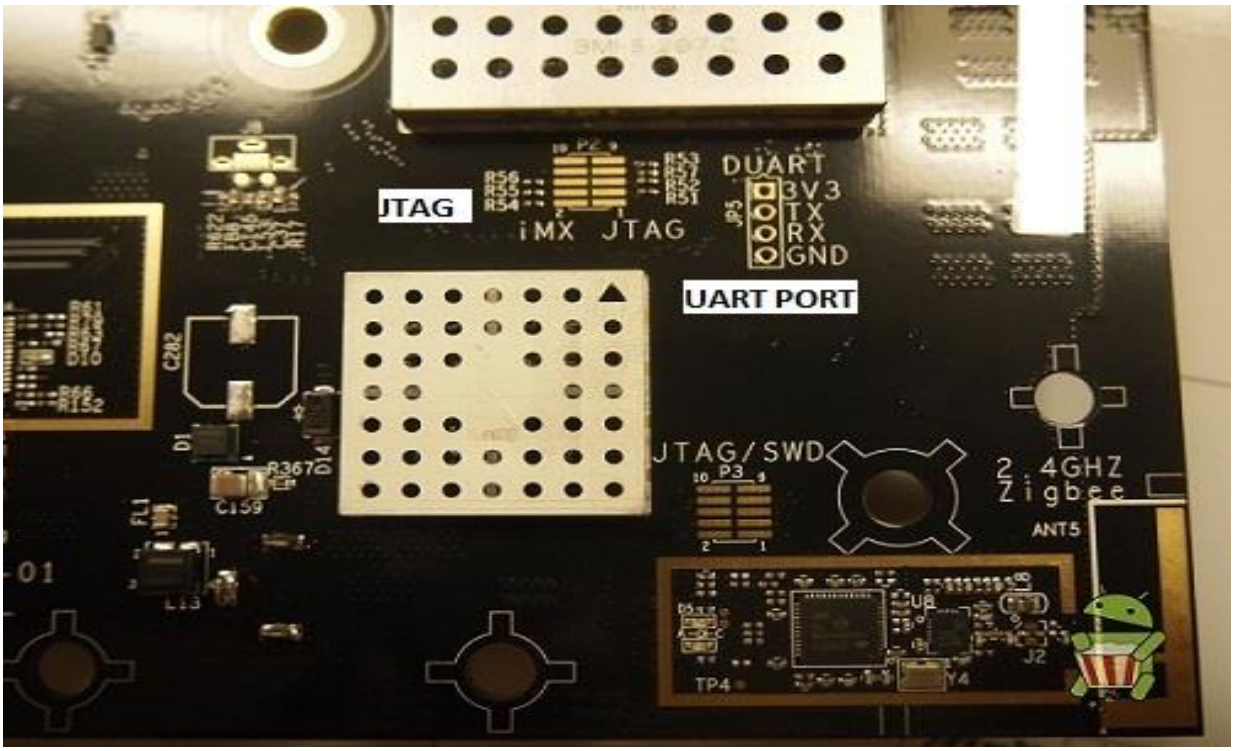


Fig7.1.3 UART port Wink Hub 1.

7.2 JTAG WAS NOT LOCKED

JTAG (named after the Joint Test Action Group which codified it) is an industry standard for verifying designs and testing printed circuit boards after manufacture. JTAG implements standards for on-chip instrumentation in electronic design automation (EDA) as a complementary tool to digital simulation.

It specifies the use of a dedicated debug port implementing a serial communications interface for low-overhead access without requiring direct external access to the system address and data buses. The interface connects to an on-chip Test Access Port (TAP) that implements a stateful protocol to access a set of test registers that present chip logic levels and device capabilities of various parts. The Joint Test Action Group formed in 1985 to develop a method of verifying designs and testing printed circuit boards after manufacture.

In 1990 the Institute of Electrical and Electronics Engineers codified the results of the effort in IEEE Standard 1149.1-1990, entitled Standard Test Access Port and Boundary-Scan Architecture. The JTAG standards have been extended by many semiconductor chip manufacturers with specialized variants to provide vendor-specific features

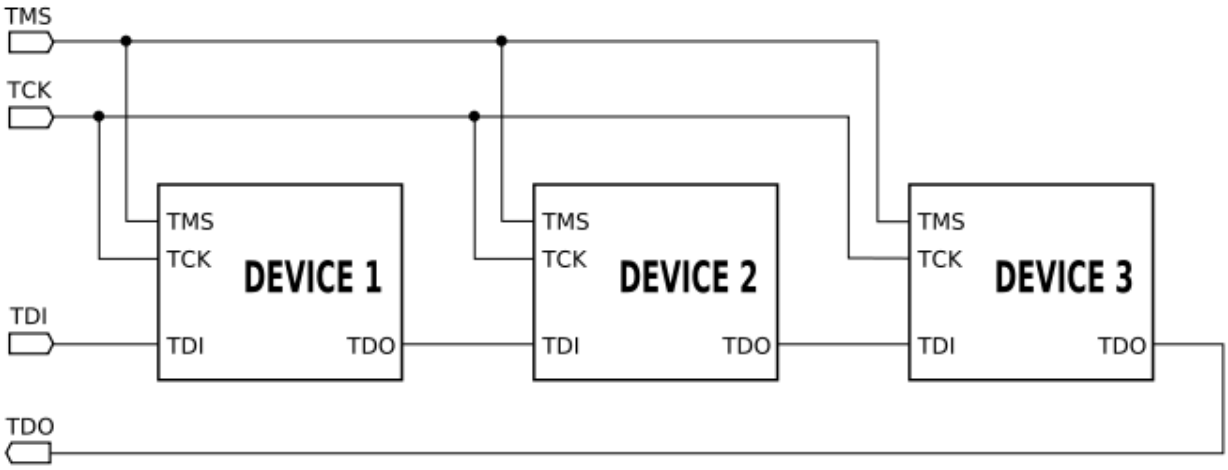


Fig 7.2.1 JTAG Algorithm

JTAG was not locked using JSWAGGER or JLINK the attacker could just connect to the TRST, TMS, TCK, TDI, TDO, GND and halt, manipulate the PC value etc. of the SoC.

The JTAG adapter used for accessing JTAG on the Wink Hub 1 is FT232H along with Expliot Nano which is a JTAG adapter.

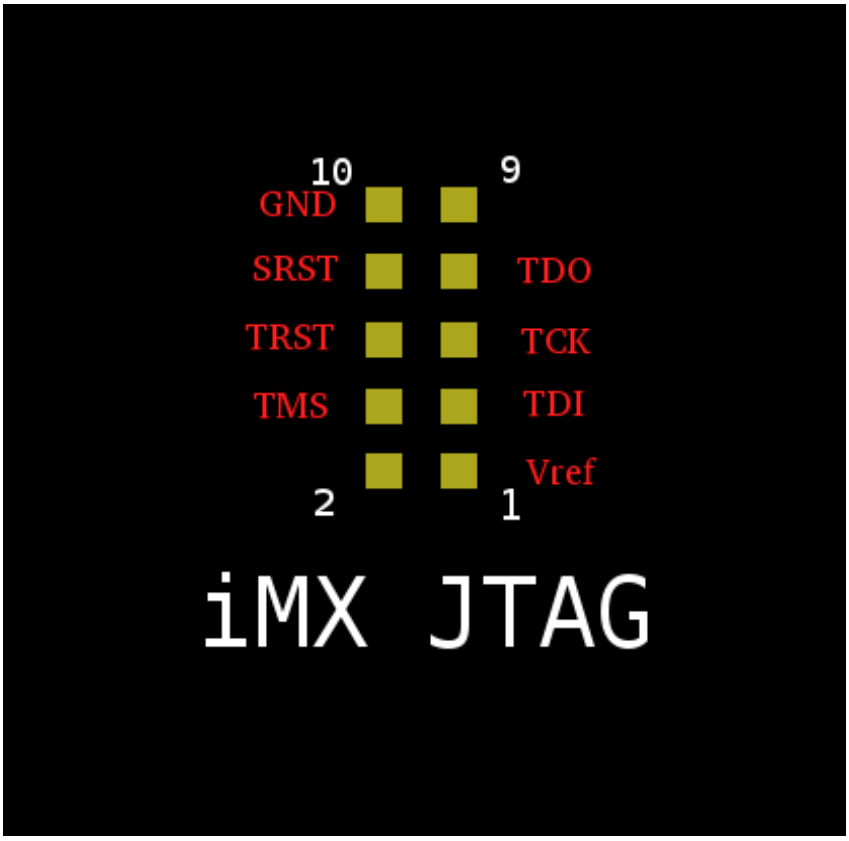


Fig.7.2.2 JTAG Pinout

The above fig 7.2.2 shows the pin layout of the JTAG using a JTAG adapter the CPU or memory can be manipulated.

7.3 NAND Glitch Attack and Analysis

Through UART the complete firmware was not accessible the vendor did a smart work here by allowing only to access the boot loader not the kernel.

So what? Time for NAND glitch attack.

After U-Boot starts, as the kernel begins loading, hold a wire and run it from GND to the NAND I/O 0 pin (#29). The kernel image will fail to load, dropping the user back to a U-Boot shell.

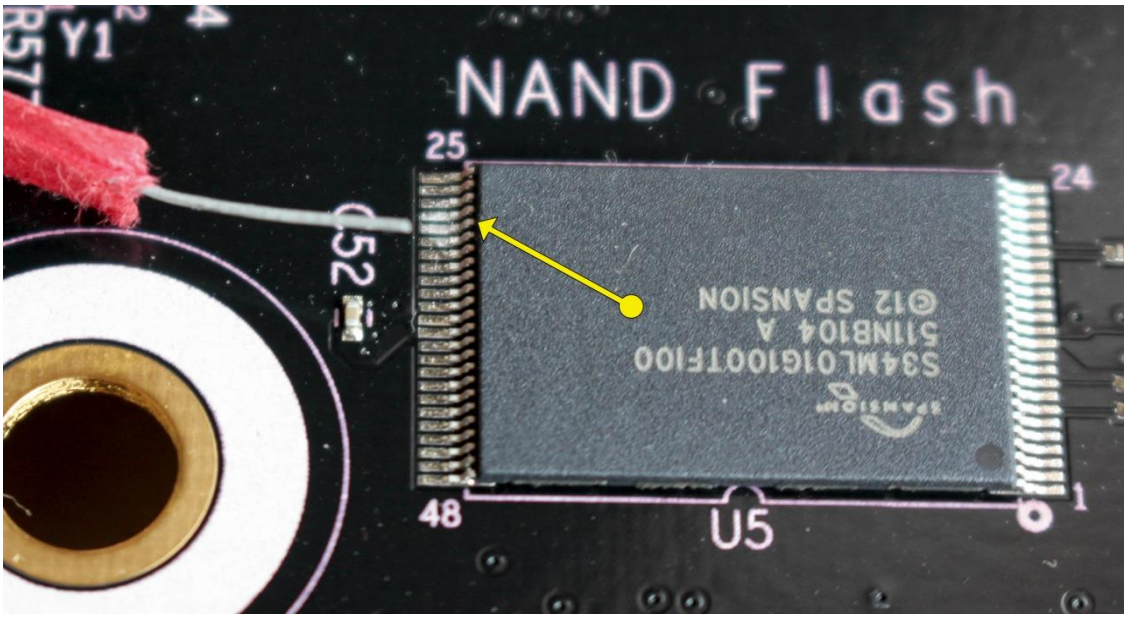


Fig.7.3.1 NAND Glitching

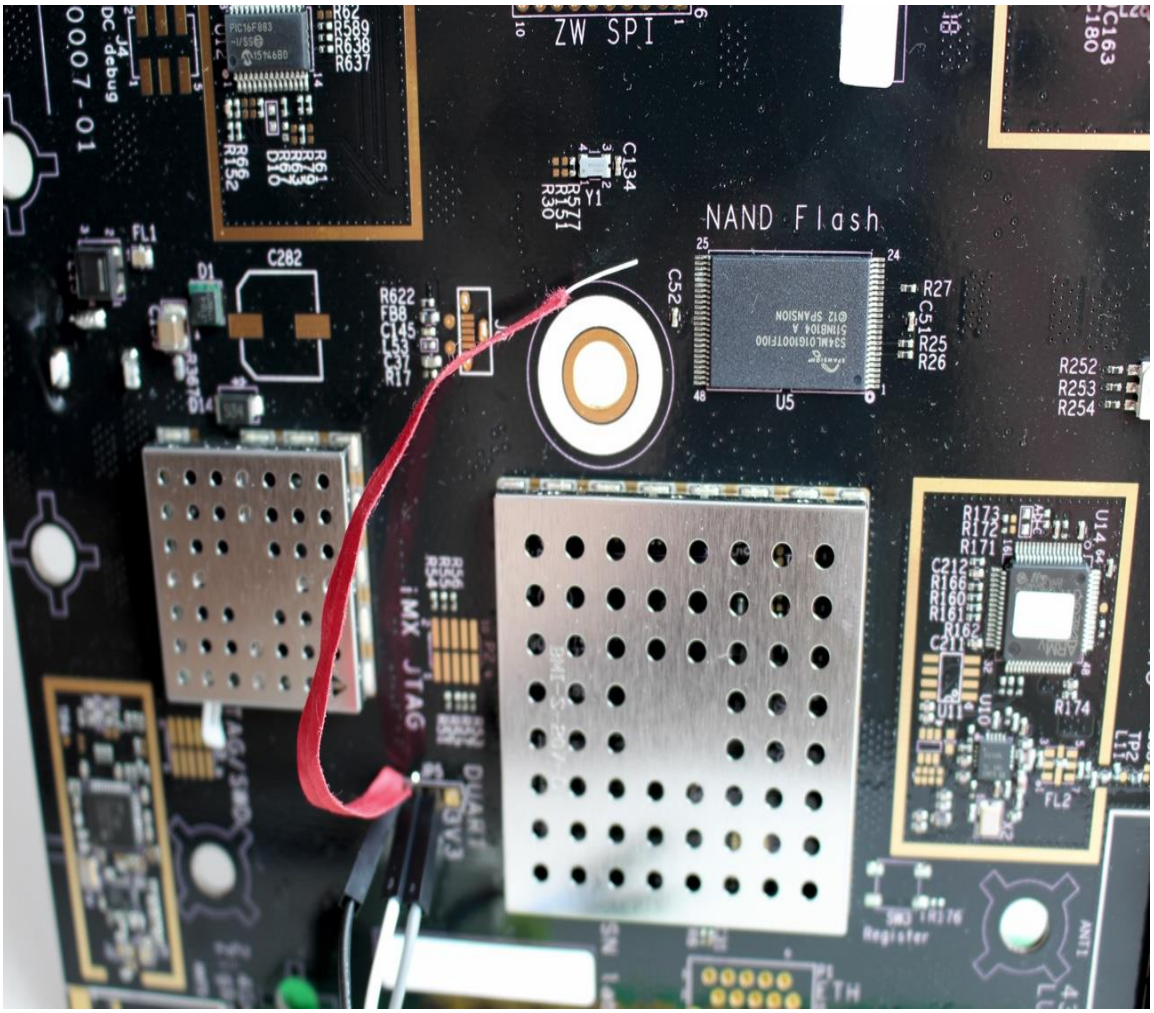


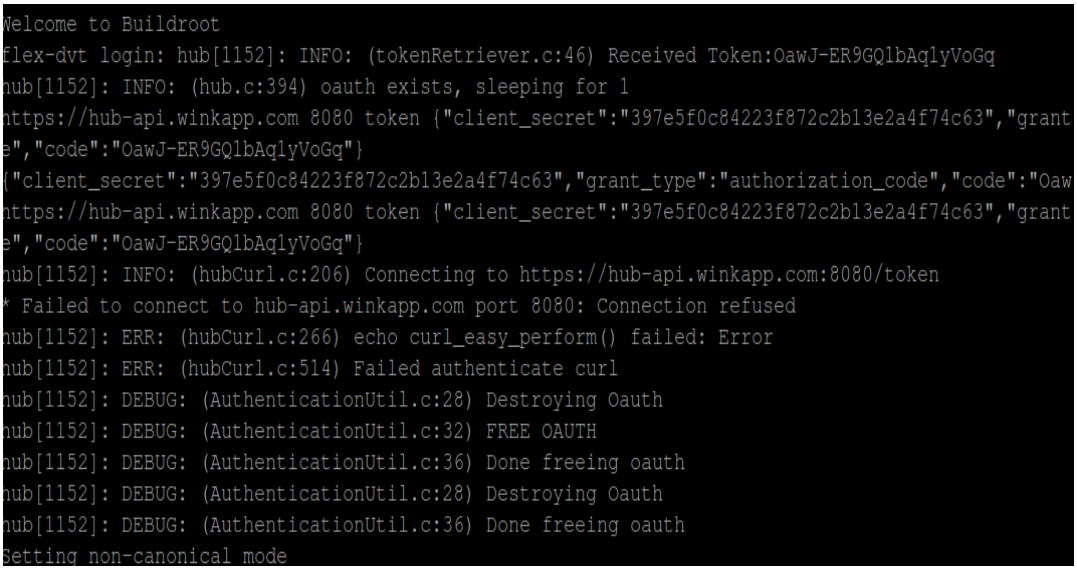
Fig 7.3.2 NAND Glitch attack setup

7.4 Firmware analysis and attack

Using the above to vulnerabilities at the hardware layer we were able to access the internal firmware of the device and navigate through the Root Filesystem i.e. RFS and obtain the password for the ***root*** account which was ***123456.***

Also, services like SSH were pre-installed and we just needed to enable the OpenSSH server and SSH into the device remotely which gave us complete root access overtheairthroughWi-Fi.

Similarly while the device boots up it displays all the username and password authentication along with OAUTH to communicate to the remote wink hub server at http://api.wink.com:8080 using the below info:



Using the above info, the attacker can easily hijack the communication between the device and its remote server and install malicious firmware.

RESULTS

7.5 Results

From all the previous stated attacks if any attacker gets access to the device, he can access the internal firmware where all the user passwords, browser passwords, Wi-Fi/BLE/Zigbee passwords are stored in /etc folder in the firmware.

Also, we can conclude that the IoT devices aren't secure enough for day to day use. The user's sensitive information is available wild open to anyone who gets access to device. The IoT device can be backdoored and can be converted into a ransomware or botnet which can cause havoc worldwide.

7.6 Mitigation Technique

1. Always password protect the UART port of any embedded / IoT device

2. Lock JTAG port to prevent unauthorized access otherwise it can lead to deadly consequences.

3. Use secure boot techniques for firmware and upgrade only to secure signed i.e. digitally signed firmware's.

7.7 Advantages

1. As an IoT hub device it can cater to many RF protocols ranging from Bluetooth, Zigbee, Lutron, Kidde, Wi-Fi etc which brings down the cost for having multiple routers for different IoT devices.

2. The device is scalable i.e. newer protocols can be added to the device using updates over theairlikeFOTA(FirmwareOvertheAir).

3. It's cheap and powerful.

7.8 Disadvantages

1. Vulnerable to hardware attacks.
2. Vulnerable to Memory based attacks.
3. Vulnerable to firmware attacks
4. Vulnerable to RF attacks

CHAPTER 8

CONCLUSION

In first case where we studied the different hardware attacks, they give us an idea how an IoT device can be physically tampered and exploited in order to gain complete access and once exploited what an attacker can do to silently dump all the data and misuse the information. On the other hand, in the RF attack vectors one can easily demodulate the modulated signal and decode the bits transmitted to obtain the bits being used to control the device remotely and lastly the network layer attacks depict how once can easily sniff all the data packets and compromise the network.

As Internet of Things is growing rapidly so are the risk involved when it comes to security and privacy of the user increasing at a greater cost. After analysing and studying different protocols and the threats they possess it's quite evident that no IoT device is secure and the only thing a user can do is to improve the standards of security and keep himself acquainted with latest security standards, keep the device up to date with latest updates that the vendor provides and follow security guidelines provided by the vendor.

FUTURE SCOPE

With the ever-increasing use of smart devices can we assure the life of an individual is secure? As routers and other smart devices are now adapting artificial intelligence and providing additional features like:

1. Malware protection on the edge
2. VPN inbuilt in the router
3. Bit torrent protocol support
4. Media server

Security of IoT devices will be a major concern as new technologies are being embedded into these devices. Newer protocols will give birth to newer vulnerabilities which need to be looked up on and fixed before they cause havoc in the world.

With more and more services like low range contactless payments, Crypto currencies being transacted over the air the IoT hubs will play an important key role in interconnecting such services with integration of various RF protocols and if such services aren't secure on hardware, firmware & RF layers then what's the point in using such devices?

In future IoT hubs or routers will be routing and switching gigabits of data also they will be interfaced with not only ethernet but with OFC (Optic Fibre Cable) direct to home or industry which will incorporate large number of smart devices interconnected to a single hub also as newer communication protocols will be incorporated will the hub remain secure? For example, in this case can the data transmitted over the OFC, can it be sniffed? Is it Secure? Even if the Hub is secure the external factors aren't and so a secure device is just a nightmare.

The RF protocols like BLE, Zigbee, Z-Wave, Lutron, Kiddie are prone to various attacks and data can be sniffed over the air using an SDR in future strong encryption algorithms can secure such communications.

REFERENCES

[1] Bogdan Alexandru Visan, Jiyoon Lee, Baijian Yang, Anthony H. Smith and Eric T. Matson, ***"Vulnerabilities in Hub Architecture IoT Devices"*** 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 83-88, May 2017.

[2] Zhen Ling, Kaizheng Liu, Yiling Xu, Chao Gao, Yier Jin, Cliff Zou, Xinwen Fu, and Wei Zhao, ***" IoT Security: An End-to-End View and Case Study***", arXiv:1805.05853v1 [cs.CR] 15 May 2018, pp. 1-12, May 15, 2018.

[3] Apostolos P. Fournaris, Lidia Pocero Fraile and Odysseas Koufopavlou, ***"Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: a Survey of Potent Microarchitectural Attacks",*** Article in Electronics Magzine , pp. 1-5, July 13, 2017.

[4] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, ***" Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues",*** IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 3, pp. 1294-1312, 2015.

[5] KaiZhao, LinaGe, ***"A Survey on the Internet of Things Security"***, Ninth International Conference on Computational Intelligence and Security, pp.663-667,2013

BEST PAPER AWARD

Modern Education Society's

COLLEGE OF ENGINEERING

19, Late Prin. V.K. Joag Path, Wadia College Campus, Pune – 411001.

[Institute NAAC (A grade) Accredited and UG Programs Mech & E&TC NBA Accredited till 2021]

IETE Pune Centre Approved

6th National Conference on

Advancement in Communication, Computing and Electronics Technology (ACCET 2019)

25-26th March 2019

Certificate

This is to certify that Dr. /Prof. /Mr. /Mrs./Ms. AMIT VITEKAR

has been awarded with **Best Paper** entitled

INTERNET OF INSECURITIES : IOT THREATS AND MITIGATIONS

in 6th National Conference on **"Advancement in Communication, Computing and Electronics Technology"** held during 25-26th March 2019, organized by the Department of Electronics and Telecommunication Engineering at Modern Education Society's College of Engineering, Pune.

Prof. A. A. Dhavlikar
Co-ordinator

Dr. P. B. Chopade
Convener & HOD

Dr. A. A. Keste
Principal