Internet of Insecurities: IoT Threats and Mitigations

(Dr P.N.Kota, Professor in Department of Electronics and Telecommunication Engineering,
Modern Education Society's College of Engineering,Pune)

Amit Vitekar, Anushri Dabhade, Pradnya Paigude

Department of Electronics and Telecommunication Engineering,
Modern Education Society's College of Engineering, Pune, Maharashtra, India.
amitvitekar@ymail.com
anushridabhade23@gmail.com
pradnyapaigude78@gmail.com

Abstract— **The Internet of Things (IoT) is growing at a very high speed and evolving at a great pace. As new devices are being connected to the internet, new protocols are being developed to improve the efficiency of communication between these devices, keeping in mind the scalability of new devices and the services these devices will offer no doubt IoT is going bring a new industrial revolution in the field of Technology, Hospitality, Medicine & other domains. With all these new advancements the one aspect that most people tend to forget and seem careless about is Security and Privacy of the user relying on these IoT devices & services in day to day life. This paper focuses on various threats present in an IoT device right from Physical to the Application layer with reference to the Operating System Interconnect (OSI) model and what impact it will have on the life of a layman if the Security & Privacy is taken for granted.**

INTRODUCTION

The Internet of Things (IoT) is nothing but a phenomenon of interconnecting different devices altogether using existing technologies like the Embedded & Field Programmable Gate Arrays (FPGA) based microcontrollers and sensors at the Physical (PHY) layer, defining various Radio Frequencies (RF) on the Media Access Control (MAC) layer like the 802.15.4 protocol stack which is Low Rate – Wireless Personal Area Network (LR-WPAN) for the intercommunication between sensor nodes and heterogeneous IoT devices within the vicinity or coverage area Over the Air (OTA).

In order the identify different nodes and devices at the Physical (PHY) layer Media Access Control (MAC) Addresses are assigned to these devices based on this MAC addresses these IoT devices are assigned virtual ID numbers which is nothing but Internet Protocol (IP) based Address which helps in identification of the nodes at the network layer that eases routing of data packets for sharing and communication of data between the devices. At the Application Layer a seamless and easy to use User Interface (UI) is used which can be accessed locally or remotely over internet using cloud computing services and with the help of Application Programming Interfaces (API's) can be integrated into various platforms which use different software runtime environment's and programming languages.

This all sounds to be perfect and easy to implement which it is but, there lies an aspect which is overlooked at each and every layer of this protocol stack and that is security. As we are implementing new technologies using various protocols which rely on legacy core principles there are some loopholes which allow attackers or security researchers to gain unauthorized access to these devices and acquire confidential data. Once that is accomplished an attacker can steal all the data present in the storage memory i.e. NAND or Flash memory of the device or even force the Random Access Memory (RAM) to dump confidential data like the Username and Passwords, various processes running in the virtual memory of the device and the temporary or cache data these processes hold also the browsers and applications running on these devices have access to the network configuration and credentials stored on the device.

It does not stop here some IoT devices which offer to make your home "smart" also make your home devices vulnerable by making them available over the internet without any authentication mechanism which can be located using search engines like Google or Shodanhq. Nowadays, these devices also store banking information like the credit card and debit card info which could be leaked once the device is compromised.

All this could lead to nothing but havoc and can cause massive disruption of devices and data stored in them.

OBJECTIVES

- To explore various IoT protocols and security threats they possess.
- To discuss mitigation techniques of similar threats.
- The purpose of making user and vendors aware of the security flaws in IoT devices and the IoT ecosystem.
- To give security experts and innovators a taste of insecurity in the so called Internet of Things or should we call it Internet of Apocalypse?

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 analyze some case studies of

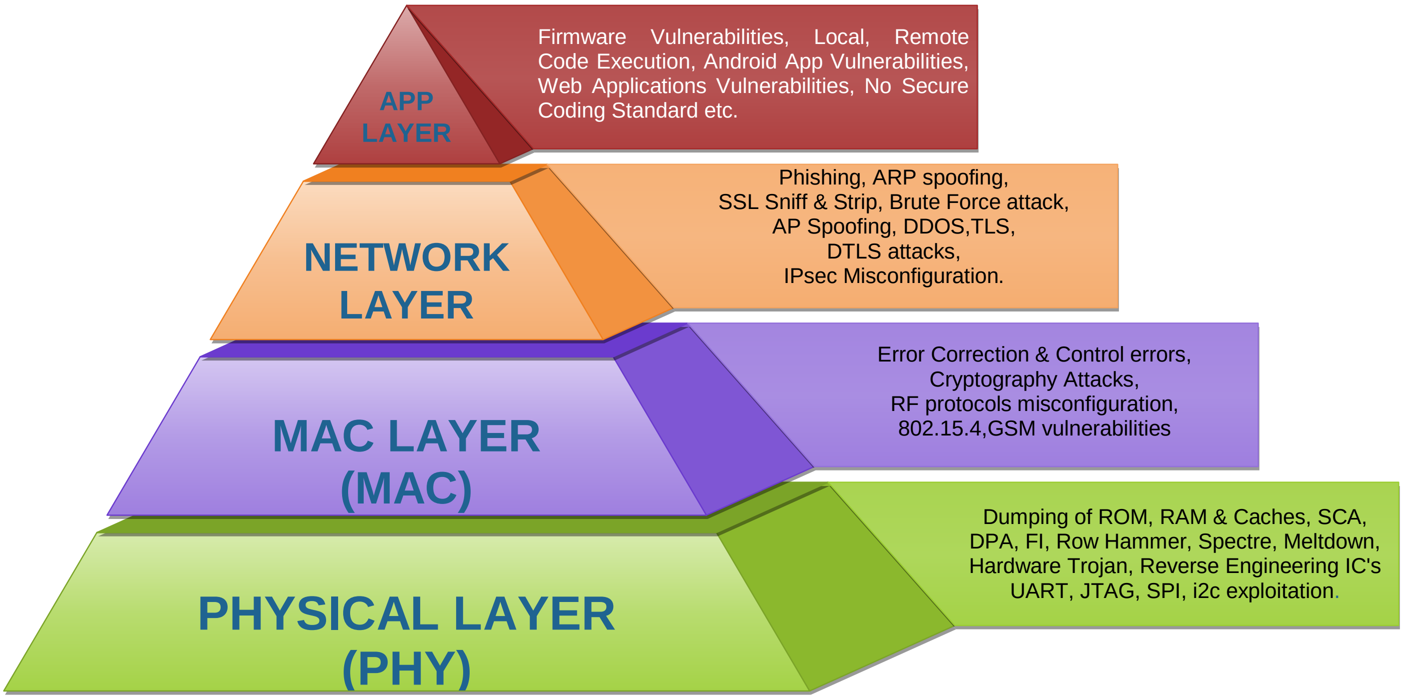
APP LAYER
Firmware Vulnerabilities, Local, Remote Code Execution, Android App Vulnerabilities, Web Applications Vulnerabilities, No Secure Coding Standard etc.
NETWORK LAYER
Phishing, ARP spoofing,
SSL Sniff & Strip, Brute Force attack,
AP Spoofing, DDOS,TLS,
DTLS attacks,
IPsec Misconfiguration.
MAC LAYER (MAC)
Error Correction & Control errors,
Cryptography Attacks,
RF protocols misconfiguration,
802.15.4,GSM vulnerabilities
PHYSICAL LAYER (PHY)
Dumping of ROM, RAM & Caches, SCA,
DPA, FI, Row Hammer, Spectre, Meltdown,
Hardware Trojan, Reverse Engineering IC's
UART, JTAG, SPI, i2c exploitation.

Fig. (A) IoT Protocol Stack & its threats.

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.

ANALYSIS

PhysicalLayer(PHY)

In fig(A) 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. When the device boots up it goes through a series of steps first being to initialize the hardware components of the device which is done by the boot loader, which decompresses the kernel and loads the entire required driver for RF protocols, services to manage these protocols etc.

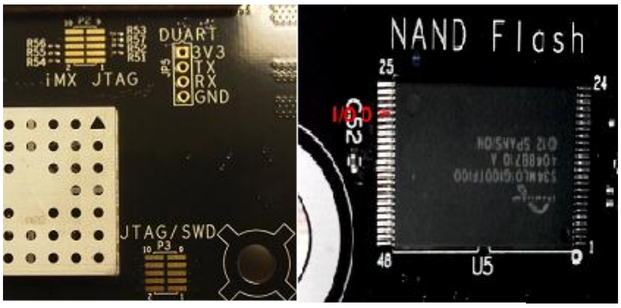

Fig. (B) UART, JTAG PORTS & NAND Storage.

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 hardware perspective.

MediaAccessControlLayer(MAC)

Form fig (A) 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 baudline, phosphor, RpiTx, gr-GSM etc.

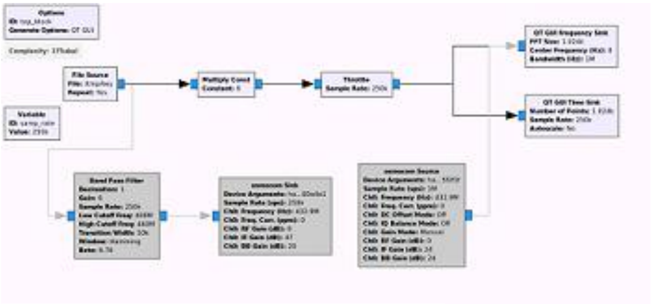

Fig. (C) Replay attack using GNU Radio.

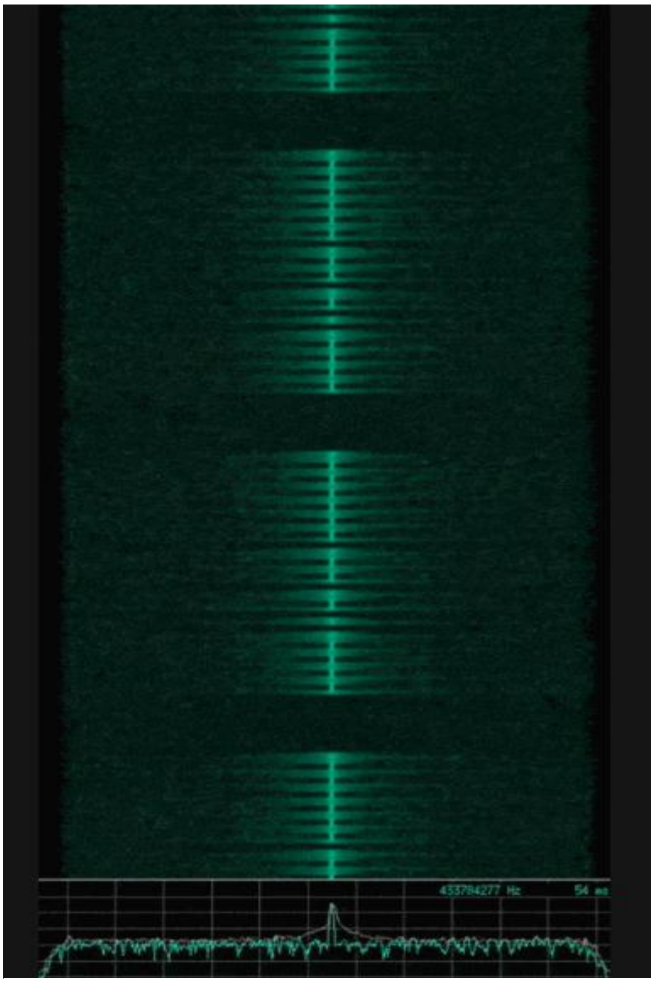

Fig. (D) Bits & Modulation inspection using Inspectrum.

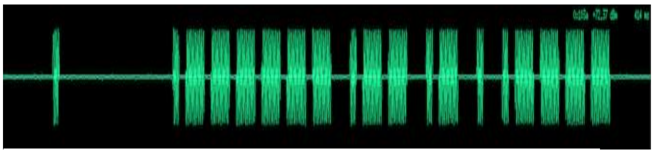

Fig. (E) Bits & Modulation reversing using Inspectrum.

In fig (C), 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 analyzing we can conclude that it uses an On-Off Amplitude Shift Keying (OO-ASK) modulation technique to transmit data over the air. 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 and 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.

NetworkLayer

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.

ApplciationLayer

The top most layer in fig. (A) 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 lighthttpd 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 of crypto currencies, launching a DDOS attack on some government site or even disrupting services on a network.

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 analyzing 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.

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", a*rXiv: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 Securit*,pp.663-667,2013.

[6] Security Research blog by Ettlam Security ltd. *https://www.elttam.com.au/blog/intro-sdr-and-rf-analysis/*