Survey on Security Issues of Internet of Things (IoT)Devices

Ajish K S[1], Athira Prem[2], Reshma R[3], Minu Lalitha Madhavu[4]

[1,2,3] *Student, Dept of Computer Science & Engineering, Sree Buddha College of Engineering, Kerala, India*
[4] *Asst.Professor, Dept of Computer Science & Engineering, Sree Buddha College of Engineering, Kerala, India*

Abstract – *Internet of Things is the internetworking of physical devices embedded with software, electronics and sensors which enable these devices to connect with each other and exchange data. There are many problems in security of Internet of Things(IoT) devices. The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, RF modules and sensing modules. RF modules manage communication through their signal processing, WIFI, ZigBee, Bluetooth etc. This paper introduces some of the treats that the IoT devices cause.*

Key Words: **Internet of Things(IoT), RFID, Beacon, Raspberry pi**

1.INTRODUCTION

Internet of Things is the internetworking of physical devices embedded with software, electronics and sensors and enable the devices to connect with each other and exchange data. IoT is very wide and includes a variety of physical elements. In this era of Internet of Things, short range mobile transceivers are embedded in daily necessities, human beings will get a wide range of communication, from any location at any time. Communication connection extended to persons and things, and between things which means, embedding the sensors to the other devices [2]. The IoT enables physical objects to think and perform jobs by having them communicate with each other and to share information and to coordinate decisions. Security is a major concern while dealing with the Internet of Things. They are vulnerable to attacks and security treats which leads to lot of security issues [4]. Majority of IoT enabled devices are not secure and can be easily accessed by an attacker. Thus there is a severe need to secure it in order to ensure that the privacy of the user is not exploited. This paper is a survey of the popular IoT hardware devices and their security issues.

2. LITERATURE SURVEY

2.1 RFID

RFID identification is an automatic identification technology which identify moving objects, the identification work without human involvement and operation is also very convenient and easy.

Fig -1: RFID

RFID system is vulnerable to various attacks. This is mainly because of the communication between the tag and reader which is achieved by the form of electromagnetic waves. RFID security defects may be explained. It is essential to have a clear vision of what data security means [3]. Only then we can identify the security of RFID. Some of the security problems are:

- Controlled access to Authorized Entities-Only the authorized entities can configure and add to the system, and all devices connected to this system are secure.
- Every communication system consists of different data security levels. Higher levels of security tend to introduce extra cost and technological complexity. It is critical to balance security threats against security costs.
- In front-end, the connection between reader and the tag takes place hence the front-end is considered to be complex and important [3]. This makes the RFID more powerful, and also leads to many security threats like unauthorized access, cloning of tags, attacks through side channels.

2.2 BEACON

Beacon is a Bluetooth Radio transmitter which repeatedly transmits signals which is detected by the devices connected to the beacon

Fig -2: Beacon

The major security issues of beacon are:

- Piggybacking, occurs when an attacker listens to your beacon and captures your beacon’s UUID, Majors and Minors and adds them to your application without your consent. Sharing these details for free with strangers is inconvenient, but it doesn’t damage your device [1].
- Cloning, it means copying your beacons configuration and putting it into another beacon to mislead the users. It can cause disastrous experience for the users as the signals may be overlapped [1].
- Hijacking, usually beacons communicate in the clear and don’t encrypt data that is sent to them. So when any user has to connect to a beacon, they can see the password the user has sent to connect to the beacon and then use it and change it, so original user can’t connect anymore [1]. The hacker, then has a full control over connected device. The whole IoT infrastructure could be at risk from this [1].
- Cracking, even if the user has secured beacon from remote attacks, it can always fall victim to someone who physically removes your beacon from the wall, opens it up, and probes the memory directly [1].

2.3 RASPBERRY PI

Raspberry Pi, in many aspects, an excellent system to use as the processing core of IoT devices. The main security issues with the Raspberry Pi set up is the widely known username/password (pi/raspberry) combination which half the bots in the world are trying on everything with an internet connection. Change the username and password and it is as secure as any ordinary Linux system. The biggest exposure is that the pi id has sudo access but sudo isn’t configured to require a password. That means if you compromised the whole machine and every machine on the LAN it’s connected to.

Fig -3: Raspberry Pi

3. CONCLUSIONS

IoT security is becoming a huge problem in our day to day life. Since it is the interconnection of various physical devices, security between these connected devices is a major concern, due to the rise of cyber-attacks, and the rise of black hats, security of users connected are a major concern, this paper is the survey of all these situations, we would like to bring in the insight of security issues of some of the common and major hardware devices used in IoT devices.

ACKNOWLEDGEMENT

We are grateful to our guide and PG Coordinator Prof. Minu Lalitha Madhavu for her remarks, suggestions and for providing all the vital facilities which were essential. We are thankful to all the staff members of the department of Computer Science & Engineering of Sree Buddha College of Engineering, Alappuzha

REFERENCES

[1] https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwi6jYu0m8_XAhXGPY8KHQ_fC-AQFghiMAM&url=https%3A%2F%2Fkontakt.io%2Fblog%2Fbeacon-security%2F&usg=AOvVaw3J8kT2h9ulyBte1oVIdzRB

[2] Shivangi Vashi, Jyotsnamayee Ram,Janit Modi, “Internet of Things (IoT),A Vision, Architectural Elements, and Security Issues”, International conference on I-SMAC,2017

[3] http://www.thingmagic.com/index.php/rfid-security-issues.

[4] https://www.tutorialspoint.com/internet_of_things/internet_of_things_hardware.htm

BIOGRAPHIES

Ajish K S, pursuing B.Tech Degree in Computer Science & Engineering from Kerala University, India

Athira Prem pursuing B.Tech Degree in Computer Science & Engineering from Kerala University, India

Reshma R, pursuing B.Tech Degree in Computer Science & Engineering from Kerala University, India

Minu Lalitha Madhavu received B.Tech. Degree in Computer Science and Engineering from Rajiv Gandhi Institute of Technology, MG University, India, received M.Tech Degree in Technology Management from Kerala University, India. Currently, she is Assistant Professor at Sree Buddha College of Engineering, Kerala University, India.