JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

A Study on Bluetooth Security Connection and Attacks

M. Dukitha[1*], D. Harikrishnan[2]

[1,2]Dept. of Master of Computer Applications, Er. Perumal Manimekalai College of Engineering, Hosur

Corresponding Author: dukitham@gmail.com, Tel.- 9486344558

Available online at: www.ijcseonline.org

Abstract— Increasing popularity of wireless communication systems, Bluetooth has become one of the most widely used short range wireless protocols. Unfortunately, due to the nature of wireless communication networks, Bluetooth has security vulnerabilities particularly through eavesdropping. Despite newer and more secure versions of Bluetooth being released, older versions such as Bluetooth four.0 and 4.1 are still widespread all over the world. After thoroughly exploring the current Bluetooth security model and reasons for potential vulnerability, this report performs a comparative analysis of different Bluetooth security attacks, extending them and applying them to readily accessible devices, and offering countermeasures. Based on our results and discussion, it's clear that Bluetooth is a widespread technology with significant security vulnerabilities in the real world today.

Keywords— Bluetooth,wifi-security,wireless protocal

I. INTRODUCTION

Bluetooth is a wireless technology from the very inception of the network and communication era, wires has been used to exchange data. Bluetooth is one of the solutions to a wireless communication. First invented in 1994 and ever since then it has been a popular technology, primarily due to being a cost free technology. Since Bluetooth use unlicensed ISM band, it does not require any regulatory authority and consumes very limited power. Moreover, Bluetooth is an automated technology that requires no extra setup to initiate a communication. Devices of different manufacturers and models can easily communicate without any compatibility error through Bluetooth. People can easily share files, photos, music, videos, etc. through Bluetooth. For all these reasons Bluetooth is a well preferred and frequently used technology. Bluetooth technology is available nearly in every phone, tablet, PDA, laptop, gaming console, smart card reader and many other electronic gadgets. However, Bluetooth is prone to several attacks and malware infections. Attacks may steal, alter or delete sensitive data (such as personal photos, videos, banking information, credit card numbers, text messages, calendar schedule, email messages, contact information, etc.)

II. EXISTING WORK

Some of the existing works on Bluetooth security only focus on a specific type of attack on Bluetooth. Haataja et al. discussed Bluetooth security mechanism including secure simple pairing. Mutchukota et al. Made a comparative study on Bluetooth MITM attacks and proposed how the existing simple secure pairing can be improved to prevent MITM Attacks. Iqbal et al. Described weaknesses in existing security architecture and proposed a secure architecture to prevent MITM attack and DoS attack. [2].

III. METHODOLOGY

Bluetooth communication and present them with illustrations. No such comprehensive survey on Bluetooth security exists in the literature. The contributions of this work are

(i) survey of Bluetooth security loopholes with illustrations,
(ii) classifying the threats according to their severity, and
(iii) Proposing techniques for mitigation of the attacks.

IV. BLUETOOTH SECURITY

Bluetooth security as well as security risk and mitigation in general. They discussed Bluetooth security issues and vulnerabilities based on the version of the Bluetooth technology along with with risk mitigation and countermeasures. However, these works did not categorize the attacks and did not rate the severity of the threats. As discussed in this section, there is a lack of survey work on Bluetooth security that compiles all the security threats on Bluetooth technology with illustrations. The objective of this paper is to provide a comprehensive survey of existing threats to Bluetooth technology, thereby letting users knows about these vulnerabilities. We have performed a comprehensive survey to identify major security threats for Bluetooth technology and presented them with illustrations. This paper will help general users of Bluetooth technology to know the possible vulnerabilities of this technology and the countermeasures to mitigate those threats.

The rest of the paper is organized as follows.
In Section 1, we discuss the existing works on Bluetooth security. In Section 2, we explain Bluetooth technology and its architecture briefly. Vulnerabilities in the architecture are pointed out. In Section 3, we define and categorise Bluetooth threats. We also describe a brief history of threats on Bluetooth devices. In Section 4, attacks on Bluetooth are categorised and described elaborately with illustration. In Section 5, malware on Bluetooth are categorised and described elaborately with illustration. In Section 6 gives few probable solutions to mitigate the attacks. Finally, In Section 7 has the concluding remarks and few guidelines for future research.

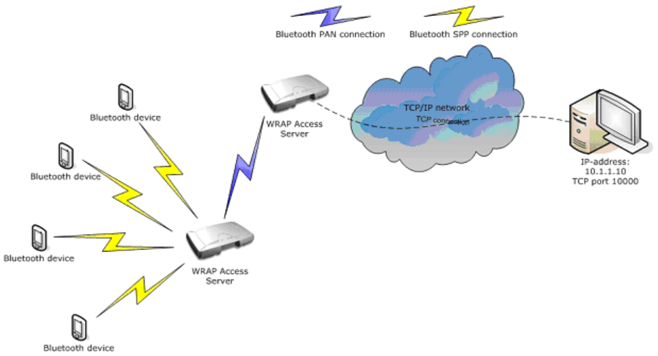

Fig. 1

V. BLUETOOTH CORE ARCHITECTURE

Host Controller Interface (HCI) Transport Layer:
This layer acts as a liaison between Bluetooth host and Bluetooth controller. Bluetooth host communicates with Bluetooth controller by sending and receiving commands through HCI layer.

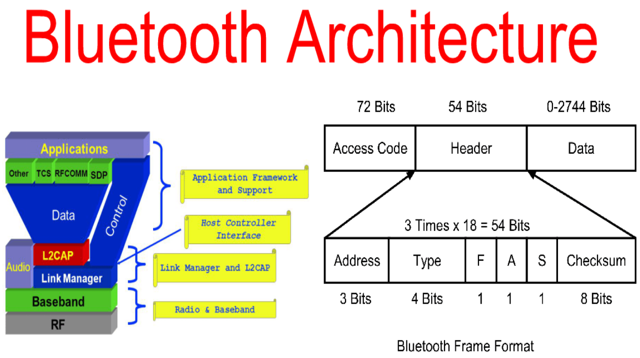

Fig. 2

VI. BLUETOOTH SECURITY THREATS

Any action that is pernicious to a system can be termed as a threat. Threats are danger that might cause harm to the system. They are constantly evolving and changing their methods of penetration. Different threat leaves different effect on the system. According to the glossary of key information security terms by National Institute of Standards and Technology (NIST), [5].threat is defined as Äny circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service". There are a number of security threats for Bluetooth and they can be broadly divided into
Two types:
(i) Attacks
(ii) Malware.

A. Attacks

Attack is an attempt to gain unauthorized access to victim device without the knowledge of the victim. It is meant to destroy, alter, disable, or steal data from the victim. Attacks on Bluetooth devices may be active or passive. Attacker may directly breach the security system of the device and gain control of the victim device. Again attackers may manipulate the victim or apply different schemes to gain control of the victim device. In the glossary of key information security terms by NIST, attack is defined as "An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity." or "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

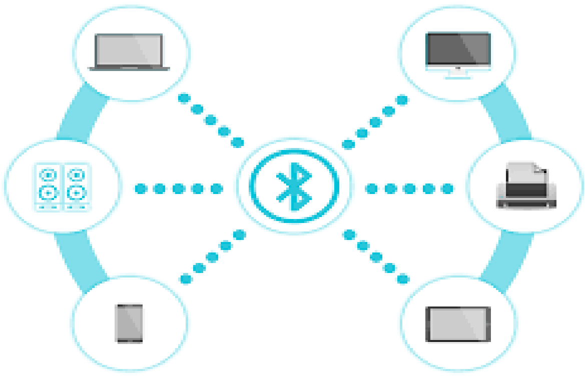

Fig. 3

B. Evolution Of Bluetooth Attacks

Since most of the Bluetooth attacks are undetected and unreported, it is not specifically known when and how the first Bluetooth attack was carried out. But there are some information regarding the detection of some of the attacks. In 2001, researchers at Nokia Bell Labs detected flaws in the pairing mechanism and mentioned that Bluetooth communication can be intruded. The first PIN cracking attack was detected in April 2005 by researchers at Cambridge University. Surveillance attack using Bluetooth device was first reported in August 2005 by police department at Cambridgeshire, England.

C. Malware

Malware is a malicious software that is programmed with an intention to do harm. The term malware was coined by Yisrael Radai in 1990. Malware comes in various forms. In the glossary of key information security terms by NIST, malware is defined as "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victims data, applications, or operating system or of otherwise annoying or disrupting the victim.". Bluetooth malware can further be divided into
two types

(i) Trojan
(ii) Worms.

D. Evolution Of Bluetooth Malware

The first Bluetooth worm was Cabir which was reported to infect Symbian OS in 2004 almost 7 years after the invention of Symbian OS. Cabir took epidemic form during the 10th World Athletics Championship in August 2005 which took place at Helsinki, Finland. It took such a severe form that warning was displayed on the big screen of the stadium. Comm-Warrior was first detected in March, 2005. Other worms like skull, Drever, Card-Block etc were reported in the consecutive years. The latest Bluetooth Trojan reported is Obad which was discovered on 4th June 2013. There is no recent report on Bluetooth attacks or malwares, but this does not mean that Bluetooth is absolutely secure.

VII. BLUETOOTH ATTACKS

Bluetooth attacks are classified in Attacks which follow similar method of penetration or leave same effect on the victim are grouped under one single title. Severity of attacks are listed in these attacks are classified as high, medium and low based on the extent of effects they leave on the victim. Attacks those gain full control of the victim device and can steal, alter or delete data from the memory or external storage of the victim device are categorised as high severity attacks. These threats may also cause financial damage to the victim. Attacks those steal data and extract information from the victim device during the transmission of data between two or more Bluetooth devices are categorised as medium severity attacks. Attacks those track the victim, monitor the activities of the victim or create disturbance to the victim are categorised as low severity attacks. The security threats are described and illustrated in the following subsections chronologically as they are represented in

A. Pin Theft Attack

These attacks involve stealing the PIN and subsequently establishing a connection with the victim device with an intention to carry out malicious activities.

B. Pin Cracking Attack

In order to start communication between two Bluetooth devices, a trusted relationship must be established. This process is known as pairing which is done by exchanging secret codes, a.k.a., Personal Identification Number (PIN). The PIN can be 1 to 8 bytes long.

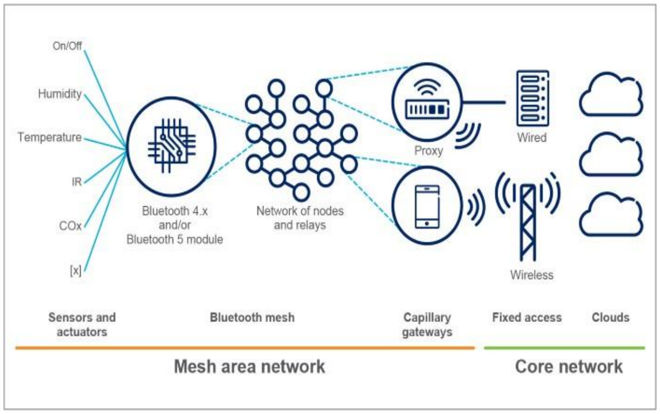

Fig. 4

The attacker eavesdrops the entire process of pairing and authentication and collects all the messages. Next, the attacker uses a brute force algorithm to find the PIN used. Then the attacker lists all the possible permutations of the PIN. If the MAC Address of Bluetooth Device is already known then by using a 128-bit random number, correct initialization key can be detected. The next step is to find the shared session link key using all the collected data. If all the collected information is correct PIN can be easily cracked .Once the attacker crack the pin, then he can pair with the victim device and can steal data without the consent of the victim.

C. Off-Line Pin Recovery Attack

Off-line PIN recovery attack is the method of intercepting the PIN in order to get access to the victim device. First of all an initialization key, IK (128 bits) is generated by using a device MAC Address (48 bits) and the PIN code with its length. Using this initialization key the devices generate two random values RAND-1 (128 bits) and RAND-2 (128 bits). These two random values are used by the devices to create the link key in-order to establish connection. By using a decryption algorithm the PIN is calculated. It is shown with illustration In this method it is not certain that an attacker can discover the PIN correctly, but there is a possibility of discovering the PIN code if the PIN is short in length. Once the attacker recover the pin, then he can pair with the victim device and can steal data without the consent of the victim.

VIII. CONCLUSION

Bluetooth is an open system so it can have some security risks. Nowadays a lot of mobile phones and other different devices include Bluetooth and in some cases the people who buy those devices don´t now even that the Bluetooth system is operating. There are some opinions which say that Bluetooth is unsecure in the encryption and some other technical aspects but most of the information I found about Bluetooth security is quite technical. Anyway I think that some information about Bluetooth security must be included in this inform, because security is one subject of our subject. So I decide to include the clearer and simple text I found about Bluetooth security, with the link below: Today's wireless world means that data is being sent invisibly from device to device and person to person. This data, in the form of emails, photos, contacts, addresses and more needs to be sent securely. Bluetooth wireless technology has, from its inception, put an emphasis on security while making connections among devices. The Bluetooth Special Interest Group (SIG), made up of more than 8,000 members, has a Security Expert Group. It includes engineers from its member companies who provide critical security information and requirements as the Bluetooth wireless specification evolves.

REFERENCES

[1] Bluetooth.org. New Bluetooth Specifications Enable IP Connectivity and Deliver Industry-leading Privacy and Increased Speed. Technical report, Bluetooth Special Interest Group, 2014. http: //www.bluetooth.com/Pages/PressReleases-Detail.aspx?ItemID=220.

[2] Bluetooth.org. History of the Bluetooth Special Interest Group. Technical report, Bluetooth Special Interest Group, Available on February 2015. http://www.bluetooth.com/Pages/ History-of-Bluetooth.aspx.

[3] Bluetooth.org. Security, Bluetooth Smart (Low Energy). Technical report, Bluetooth Special Interest Group, 2015. https://developer. bluetooth.org/TechnologyOverview/ Pages/LE-Security.aspx.

[4] Bluetooth.org. The Low Energy Technology Behind Bluetooth Smart. Technical report, Bluetooth Special Interest Group, Available on February 2015. http://www.bluetooth.com/Pages/ low-energy-tech-info.aspx.

[5] J. P. Carles Gomez, Joaquim Oller. Overview and Evaluation of Bluetooth Low Energy: An Emerging LowPower Wireless Technology. Technical report, Universitat PolitÃ´lcnica de Catalunya/FundaciÃ¸s i2Cat, August 2012. http://www.mdpi.com/1424- 8220/12/9/11734/htm.

[6] V. Gao. Everything that you always want to know about Bluetooth security in Bluetooth 4.1. Technical report, Bluetooth Special Interest Group, 2014. http: //blog.bluetooth.com/everythingyou-always-wanted-to-know-aboutbluetooth-security-in-bluetooth-4- 2/.

[7] R. Heydon. *“Bluetooth Low Energy: the developer’s handbook”*, Vol.0,2013.

[8] S. A. Joe Decuir. Bluetooth 4.0: Low Energy. Technical report, CSR plc,Available on February 2015. http://chapters.comsoc.org/ vancouver/BTLER3.pdf.

[9] A. West. Smartphone, the key for Bluetooth low energy technology. Technical report, IMS Research, Available on February 2015. http://www.bluetooth. com/Pages/Smartphones.aspx.