**An Inclusive Review on Security Concerns and Current Hacking Tools in Bluetooth**

***Abstract: -*** With its inception approximately before two decades Bluetooth has marked an exponential growth and had become one of the most efficient and free of cost communication mechanism for small distance. It is basically a personal area network which is used up to very short distance but still is highly efficient for the personal use like in the mobile phones while driving or in other daily electronic appliances. With its Easy availability and deployability is the intrusion is very easy and hence hacking of the same. This paper presents an Inclusive Review on the latest Bluetooth hacking tools which has been available over the years and till date.

*Keywords: -* PAN, Bluetooth, Security, Personal Area Network

**INTRODUCTION**

As we all should know that Bluetooth is a wireless technology for exchanging, and communication data over the short distance. In this paper we are going to figure out some of the most popular Bluetooth hacking tools. So first of all one question came out from mind that, what is Bluetooth hacking? Is it easy to hack a device (like cell phone) via Bluetooth? Discovering any device for starting communication is important procedure [11]. It can be hold up by scanning for other active devices and depends on range. Bluetooth technology has been considered as a reliable, cheap, and effective replacement of cables for communicating electronic devices. This technology was officially approved in 1999, since then it has instantly increasing been used in various types of electronic devices. Bluetooth technology was formed to promote by Special Interest Group (SIG). Bluetooth is a combination of software and hardware technology, the main control and security protocols have been implemented and processed in the software [15]. On the other hand the hardware is riding on a radio chip and by using both hardware and software Bluetooth has taken place a smart, efficient, flexible, and wireless communication system. The communicating distance between two Bluetooth enabled devices ranges from 10m to 100m. Bluetooth security is very active research area in both industry and academia. Powerful directional antenna can be used to increase the scanning and eavesdropping. Example of long-distance attacking tools is the Blue Sniper Rifle and it attached to a Bluetooth-enabled computer. By using this we can be done eavesdropping, scanning, and attacking over long away from the target devices. Directional antenna and some amplifiers improve and extend the range of Bluetooth device over a mile away [16]. Bluetooth technology operates in a licence-free Industrial, Scientific and Medical Band ranging from 2.4 to 2.4835MHz in Bluetooth technology “Paring “is a very important term. By using pairing procedure are formed by interchanging shared secret codes referred to as PINs. Piconet is a network in which a ‘master’ slave has the option of pairing with up to 7 ‘slave’ devices. There are different types of tools of Bluetooth related attacks and threats that can be executed against unforeseen cell phone users [13], [1].

**BLUETOOTH TECHNICAL SPECIFICATION**

Bluetooth technology works on the ISM (Industrial, Scientific and Medicine) Frequency Band with is freely available without any charge. Some of the basic Technical specifications of Bluetooth are tabulated as follows for making easy and quick understanding about the Bluetooth technology for the new readers.

**Table-1: Technical Specifications of Bluetooth [11, 12, 13]**

|  |  |
| --- | --- |
| Connection | Spread spectrum Frequency |
| Frequency band | 2.4GHz ISM |
| Modulation Technique | Gaussian Frequency Shift |
| MAC Scheduling scheme | KFHey-CinDg(MGAFS K) |
| Transmission Power | >20dBm |
| Aggregate Data rate | 0.721-1Mbps |
| Range | 10m-100m |
| Supported Station | 8devices |
| Voice channels | 3 |
| Data security | Authentication Key 128 bit key |
| Data security | Encryption 8-128 bits |

There are billions of Bluetooth devices and technology in use, so unkind and malicious security threats, violations are common events. Hence Bluetooth security architecture needs a constant upgrading to prevent new threats [11]. Cyber criminals could pass malicious data or information to the device. Security threats in Bluetooth into three common categories as follows:

1. Denial of Service (DoS) attack:-

Authorised users sometimes do not access services because the user can be blocked to get access by making it [11], [12]. DoS attack typically only infest Bluetooth network users and it is not very dangerous threat.

2. Disclosure threat:-

Information or data may be leaked by some mistakes and eavesdropper can also leak information from the target system [13]. Disclosure attacks normally comprise some sensitive data and therefore, may be very harmful [12].

3. Integrity threat:-

Receiver may not get precious information or data sent by sender and also the information can be intently altered to mislead the recipient. Integrity attacks normally comprise some sensitive data and therefore, may be very harmful [13], [15].

**KEY TERMS USED IN BLUETOOTH TECHNOLOGY**

**1.1 Frequency Hopping Spread Spectrum:-**

Using transmitter and receiver, it can be transmitted radio signals by switching among many frequencies channels, this method is called Frequency hopping spread spectrum [13].

1.1.1 Benefits of spread spectrum:

- It can share a frequency band with many types of transmissions with some interfaces that’s why bandwidth utilization can perfectly [15], [13].

- It Signals are difficult to intercept. An eavesdropper would only be able to intercept the transmission.

- It signals are highly resistant to narrow band interfaces.

**1.2 Packet Based Protocol**

Packets means all transmitted data vacantly of content, type or structure into suitable sized blocks. So packet switching is generally a technique that is digital networking communications of packets [13], [15].

**1.3 Master Slave Structure**

One device has one-way control over the one or more devices, this is called master slave model of communication. Sometime master is pick out a group of eligible devices in some system with the other devices acting as slave [12].

**1.4 Pico-net**

Pico-net is used to link group of devices, it is like an ad-hoc computer network, where protocol permit one master device to connect with up to seven active slaves [13].

**1.5 Uses [11, 12, 13, 15]**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Uses** | **Evaluation** |
| **1** | Low power consumption, with a short distance, Low energy. | The Bluetooth technology requires very low energy and use minimum battery and electric power because Bluetooth use the low power signals. This is useful to mobile users. |
| **2** | Wireless technology. | As we all should know that Bluetooth is a wireless technology for exchanging, and communication data over the short distance and many benefits to using wireless devices. Wireless also provides you secure use of technology. If you are traveling with Bluetooth devices, so you will not require to distress about bringing connecting cables. |
| **3** | Inexpensive. | For based on implementation Bluetooth is cost- effective for companies, which results in lower expenses. |
| **4** | Automatic. | Bluetooth is a free setup technology, it means it does not have set up a connection. When two or more devices enter a range of up to 30 feet of each other, they may certainly start to connect. |
| **5** | Low interfaces. | Bluetooth devices are used to low grade wireless signals. Bluetooth devices exclude interfaces from other devices. |
| **6** | Helpful to create personal area network. | We can connect up to seven Bluetooth devices within appropriate range, forming a personal network. |
| **7** | Upgradable. | Upgradeable is the standard of Bluetooth, new version of Bluetooth have much more efficient benefits. |
| **8** | Highly compatible. | Bluetooth is standardised level of compatibility among devices is guaranteed. If devices is not the same model then also it will connect devices to each other. |

**TOOLS USED IN BLUETOOTH HACKING**

**Table: Tools used in Bluetooth Hacking**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name Of Tools | Year | Types | Definitions | Specifications | References |
| Blue Scanner | License Free, Operating System Windows,  Security Level 100% Safe,  Date 24th July 2006 | Bluetooth Discovering Device | Blue Scanner will try to Conclusion or extract as much more information and data for newly discovered device. | * Reading Phonebooks * Writing Phonebooks entries * Reading or decoding SMS stored on the device setting * call forward, * Initiating phone call | * [1],[2] |
| Blue Sniff | Blue-Sniff has been identified September 2003. | Bluetooth Discovering Device | Blue sniff is a GUI (Graphical User Interface) based for finding discoverable and hidden Bluetooth enabled devices. | * Downloads the phonebooks * Connect to phone without alerting the owner if a mobile phone is vulnerable. * Gain access to restricted portion of stored data. | * [3],[4] |
| BT Browser | 2007 | Bluetooth Discovering Device | It is based on J2ME (Java 2 Platform Micro Edition) application that is helpful to browse and explore the technical specification, it works on phones that supports JSR-82 (Java Specification Request). | * Devices discovering. * Remote control over devices details. * Control services records. * Save and load information. | * [6],[7] |
| BT Crawler | May 2008 | Bluetooth Discovering Device, it also implements Blue-jacking and Blue-Snarfing. | Blue Crawler is a scanner for Windows based devices. | * Search a list of Mobile devices based on Windows. | * [1],[6] |
| BT Scanner | June 2010 | Hacking Bluetooth device | BT Scanner is a tool that help to gather an information and related data and it also permits attacker to query devices without the need to carry out pairing. BT Scanner is a Bluetooth environment auditing tool. Implemented using the blue-cove libraries (an open source implementation of the JSR-82 Bluetooth API for java. | * Capture the information from Bluetooth enabled device without pairing. * It will show MAC address of devices just hit enter on the devices which show on screen. | * [3],[7] |
| BT Crack | 2007 | Hacking Bluetooth device | BT Crack is the Bluetooth PIN and LINK\_KEY cracker. It purpose to change or redesign the password key and link key from captured pairing interchanges. PIN can be used to authenticate with device in pairing mode. The resulting Link key can be used to decrypt the data stream. | * First of all it crack PIN and after it we can do anything. | * [1],[4],[6] |

**CLASSIFICATION OF BLUETOOTH ATTACKS**

Bluetooth attacks can be classified among the following Eight Categories:

1. Blue- Bugging Attack
2. Blue-Printing Attack
3. Blue-Over Attack
4. Blue-jacking Attack
5. Man-in-the-Middle/Impersonation Attack
6. MAC Spoofing Attack
7. Off-Line PIN Recovery Attack
8. Brute-Force Attack

Figure-1: Classification of Bluetooth attacks

**1. Blue- Bugging Attack**

We can say that Blue-bugging is a hacking mechanism and it is dangerous and most powerful attack where mobile phone is hacked by an attacker. It takes total control of a victim’s phone. Blue-bugging caused by lack of awareness, which means that anyone with the right knowledge and tool and take control a phone**.** Assuming an attacker has full access to the address translation (AT) command set available in GSM (Global System for Mobile Communication) then an attacker can exploit the AT commands, simply means an attacker can steal the information [11], [12], [19].

**2. Blue-Printing Attack**

Blue-Printing helps to determine device model, firmware version, and manufacturer of the device. An attacker also generates statics about Bluetooth device and also figure out Bluetooth vulnerable device [1], [19].

**3. Blue-Over Attack**

It helps to steal sensitive information from another Bluetooth enabled device and also help in Blue-Bugging attack. Blue-Over run on almost every J2ME compatible handheld device. They are intended to provide as auditing tools [1], [19], and [3].

**4. Blue-jacking Attack**

Blue-Jacking is a technique based attack of sending incredulous messages to Bluetooth enabled devices.

This does not include altering any information from the device, but nonetheless, it is unfaithful. Devices that are set in non-discoverable mode are not high strung to Blue-Jacking [8], [14], and [19].

**5. Man-in-the-Middle/Impersonation Attack**

Man-in-the-Middle/Impersonation Attacks include the modification or transformation of data between Bluetooth enabled devices. It involves also relaying or propagation of authentication message between two devices without knowing the secret keys [20], [19].

**6. MAC Spoofing Attack**

MAC spoofing attack and PIN cracking attack are classified as most frequently attack. Malicious attackers can perform MAC spoofing during the link key generation. Attackers with highly specified hardware can simply intercept data, capture data, manipulate information, and spoof. Bluetooth SIG does not provide appropriate solution to prevent this attack [1], [8], [19].

**7. Off-Line PIN Recovery Attack**

An off-line PIN recovery attack is based on intercepting the IN\_RAND value, AU\_RAND value, and LK\_RAND values and after that trying to evaluate correct value of guessing different PIN, Sometimes this attack can run [19], [20].

**8. Brute-Force Attack**

A Brute-Force BD\_ADDR searching attack uses a method that is brute force only on the three bytes of a BD\_ADDR, because first three bytes can be set as fixed [21], [22], and [23].

**Conclusion**

In this paper we reviewed the Common Bluetooth Attacks together with the Present Hacking Tools. We also presented the Future Research Directions in this area for a secure Bluetooth technology.

**Future Research Directions**

On the basis of the literature reviewer we can make a convention towards the future research directions to make Blue tooth secure and viable enough in the present era. We can point out the following directions:

1. Depth Study on the Individual Hacking Mechanisms
2. Like Blue-bugging
3. And other mechanisms etc.

**References**

1. http://gexos.github.io/Hacking-Tools-Repository/
2. http://btcrawler.soft112.com/
3. http://www.bluejackingtools.com/
4. http://www.bluejackingtools.com/bluesnarfing/
5. http://www.pentest.co.uk/wireless.html
6. http://bt-scanner.software.informer.com/1.0/
7. http://www.darkreading.com/risk/new-hacking-tools-bite-bluetooth/d/d-id/1128509?
8. http://techpp.com/2010/06/30/7-most-popular-bluetooth-hacking-software-to-hack-your-mobile-phone/
9. http://hackaday.com/2008/08/01/essential-bluetooth-hacking-tools/
10. http://hackyogi.com/top-5-bluetooth-hacking-tools/
11. www.airccse.org
12. www.ijarcsse.com
13. www.wegilant.com
14. http://www.careerride.com/bluetooth-bluebugging-bluesnarfing-bluejacking.aspx
15. ijcit.org
16. http://docsfiles.com/view.php?view=http://www.mulliner.org/bluetooth/morefunwithblueradiowaves.pdf&keyword=bluetooth%20sniffing%20is%20for%20free%20now&count=
17. http://bluescanner.en.softonic.com/java
18. http://gallery.mobile9.com/f/616754/
19. http://trifinite.org/trifinite\_stuff.html
20. http://en.wikipedia.org/wiki/Man-in-the-middle\_attack
21. http://en.wikipedia.org/wiki/Brute-force\_attack
22. http://codex.wordpress.org/Brute\_Force\_Attacks
23. https://www.owasp.org/index.php/Brute\_force\_attack