**Detection and Prevention of Bluebugging in Bluetooth Devices & Networks**

**Abstract-** Over last two decades Bluetooth has marked an important line on the surface of Wireless Personal Communication due to its free availability and other adaptable features. It has dynamic topology in which connections become and terminate frequently due to which the probability of black hat node(s) cannot be ignored rather should be put on high probability. There are several security threats in these networks. One of such latest security threat which is considered as most daring also is “Bluebugging”. This paper presents detection and prevention of Bluebugging in Bluetooth Networks.

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

**1. INTRODUCTION**

Bluetooth is a wireless technology that is embrace in the electronic devices raising PANs (Personal Area Networks).Bluetooth Wireless Technology (BWT) is a less-distance or short-distance communication technology using encryption for data security [1]. It discovered by telecom seller Ericsson in 1994. Bluetooth stand for data or information redemption over short distances. Harold Blatand was a king of Danish, his father put together uniting the Danish kingdom. When Blatand took over the infusion then he suppressed the success. It was cause of the unification that was called Bluetooth [2]. The Bluetooth technology is helpful to transfer information and data between two or more devices [3]. It permit to share information such as voice, music, and videos without wire. Bluetooth elaborates in many products, like as telephones, media players, tablets, laptops, robotics system, and etc. [4]. It is necessary to be efficient to declare specific devices and thus enable control over which devices are allowed to put together to a given Bluetooth device [5, 6, and 7].

**1.1Advantages of Bluetooth Technology**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr.no. | Advantage | Summarize view | References | Images |
| 1. | Simple way of sharing | A Bluetooth-enabled device can help file sharing feasibility or potentialities with other Bluetooth devices, like as laptops [9]. | [9] |  |
| 2. | Cable Replacement | With the help of Bluetooth technology (wireless) a diversity or transformation of cables changes, like as mouse, keyboard, printers, and wireless headsets that easily interface or communicate with personal computer or mobile phones [8, 10]. | [8,10] |  |
| 3. | Internet connectivity or appertain | Mobile phones, laptops, tablets, and like these things can simply access or connect the internet. But important thing is that laptops can also access the internet through phone. The origin of this point is that Bluetooth device can share that access with the help of internet connectivity and with other device via dial-up connection [9]. | [9] |  |
| 4. | Wireless synchronization | Bluetooth technology provide automatic synchronization b/w Bluetooth enabled devices [10]. | [10] |  |
| 5. | Feature simplicity | Bluetooth technology has very good important feature of simplicity in functioning. | [8] |  |
| 6. | Controlled by you | Control of function, it only depends on you that what you want to do with this technology, do itself without any restrictions. | [9,10] |  |
| 7. | Bluetooth is everywhere like in your car, ear, fitness, home, office, and etc. | Now these days Bluetooth technology is growing up that’s why it is available almost everywhere. | [8] |  |
| 8. | Standardized protocol | Bluetooth connects devices with each other, even if they are not in same model | [9,10] |  |
| 9. | Low energy consumption | In Bluetooth technology, uses of low level signal makes low energy consumption. | [9] |  |

*Table-1: Advantages of Bluetooth Technology*

**1.2 Bluetooth security procedure**

Here the description of main three security methods or steps is given, which are follow as:

**(a.) Authentication:**

The important aspect is that authentication of any devices that should be done properly but it does not authenticate that why problems occur. So the main motive of authentication is to examine the client’s level authentication. Link keys are helpful to check or calibrate the authentication [12]. Encrypted address that is given by sender help in proper authentication. Firstly the sender send the encrypted address of Bluetooth device and receiver use the link keys for producing a random number to signed response authentication result [11, 13]. The signed response authentication result is sent to the receiver and the connection is established.

**(b.) Authorization:**

It is a process of presenting access to a network resource. It permits the control of resources by confirming that a device is authorized to access a service before permitting it [11].

**(c.) Confidentiality:**

Only authorized devices can access and view its own data it means the preventing information can resolve caused by eavesdropping.

**(d.) Optional Encryption:**

The key size of encryption should be longer optimally. An abnormal number must be sent one device to the other devices want to communicate with each other [12]. Then a link key is generated on both devices to submit it and then devices are connected to each other. The encryption process is a constitutive segment for Bluetooth wireless technology. The encryption key may be between 8 to 128 bits. It is encoding data or information being swapped but it cannot decode its contents [10].

*Fig.1: Key steps in Bluetooth Security*

**2. PROCEDURE OF BLUETOOTH USE**

**.** Recognize that your device are Bluetooth capable or not.

**.** Read about capability of device.

**.** Start scanning for Bluetooth device.

**.** Pair with device.

**.** Use Bluetooth to drive safer.

**.** Now you can transfer files between devices.

**.** Talk on the cell phone by using Bluetooth.

**.** You can synchronize data [10, 11, and 14].

**2.1 Bluetooth architecture**

In Bluetooth architecture [9, 14, 11, and 10]:

Base band: - baseband is used for managing physical channel and links. It checks error refining, data whitening, and Bluetooth security.

Link manager: - It endow or supply link setup, authentication, and link configuration.

L2CAP: - It gives data services to the upper level host protocol. It also gives connection-oriented and connection less data services.

RFCOMM: - It makes available for use a simple reliable data stream to the user, similar to TCP.

TCS: - It used to setup and control speech and data calls between Bluetooth devices.

SDP: - It used to detect which services are available and what type of characteristics of those services.

OBEX: - It is used for simple data exchange (file transfer, basic imaging, printing, phone book access, etc.).

AT COMMAND: - It provide for devices, make/break connections and inquiry.

TCP/

IP

APPLICATION

PPP

AT COMMANDS

OBEX

RFCOMM

TCS

SDP

L2CAP

HCI

AUDIO

LINK MANAGER (LM)

BASEBAND

BLUETOOTH RADIO

*Fig.2: Bluetooth Architecture*

**3. DANGEROUS THINGS ABOUT BLUETOOTH**

There are so many dangerous things or variety of attacks that can be engaged against Bluetooth devices such as blue-bugging, blue-snarfing, blue-tooone, blue-jacking, blue-bumping, blue-dumping, blue-spoofig, etc. [16]. Because of weakness of Bluetooth security system that make free an attacker unauthorized access to a victim’s phone. By using blue-tooone, attacks on Bluetooth devices have been presented or documented at ranges in extra of 1,500m but normally Bluetooth is allied with networks limited in scope to 100m [17, 18, and 19].

Blue-jacking: - Sending anonymous message to another device without authentication and approval.

Blue-snarfing: - Attackers establish or organize connection without authentication then attacker can do anything like theft of data, calendar information, phonebook contacts, and phone’s IMEI number.

Blue-tooone: - It is useful for increasing range of Bluetooth connectivity by using a directional antenna.

Now come to the point that is Blue-bugging.

**4. BLUEBUGGING**

Two security researchers Adam Laurie and Martin Herfurt demonstrated or accomplished the Blue-bug attacks at the Black Hat and DefCon security and hacker conferences in Las Vegas back in 2004. They constructed a collection of attacks, such as Blue-snarfing and Blue-bugging [24].

Ever since Bluetooth enabled mobile phones started publishing in the early 2000’s, numerous reports have suggested that there are serious security flaws in Bluetooth technology and that it is vulnerable to Blue-bugging. Blue Bug is the name of a Bluetooth security loophole on Bluetooth enabled devices [22]. Attackers use this weakness of Bluetooth and they can attack on your phones. By using this loophole they can able to access contacts, call logs, and send or receive message. Blue Bug attack divests only a few second under the circumstances. This security flaw does permit a massive number of things or actions that may be done when phone is attacked via Bluetooth.

Blue-bugging is basically a Bluetooth attack that makes free skilled hackers to access mobile commands in some Bluetooth-enabled phones and it’s like a phone eavesdropping, or bugging [20]. If any device with its Bluetooth turned on and set to “discoverable” (capacitate to be established by other device) can be susceptible or open-minded to blue-bugging. Most types of Blue-bugging attacks can be done without leaving a trace or clue (Better Business Bureau, 2013 [21]). Blue-bugging is also responsible for accessing identity that is growing up very fast. Because of this identity theft has been easy to refer and it results in fruitful gains or benefits. The general trust or lack of knowledge on behalf of public create an avenue for savvy criminal to commit these fraudulent acts [21].

On the other hand we can say about it 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 can take control a phone [25]. The victim cannot even consider that a mobile phone can be victim or front part of this attack. It makes free the hacker to read the information in your cell phone. Sometimes you receive a call on your phone it may be hacked, because even if the Bluetooth device is disabled or turned off the mobile cell phone the call is also forwarded to the hacker and he can listen the conversation and also can commit theft of all the data and information in your mobile phone using his laptop [23].

Now come to the important point about Blue-bugging is that it permits a genuine takeover of the target phone. It manipulates the phone into understanding its security, so as to create a backdoor attack without informing or alerting the phone’s user, accessing the user to “take control” of a victim’s phone. The Blue-bug program also has the capability to create a call forwarding application whereby the hacker receives calls intended or earmarked for the target phone. A Blue-bug user can simply make notes to any conversation his victim is having in real life [26, 27]. Blue-bugging attack is targeted for privacy issues that are specific to cell phones and Bluetooth headsets. Blue-bugging needs skilled hackers with knowledge of Bluetooth protection and protocols. In this attack the attacker connects to the target device without any permission from its owner, and steal some sensitive information [21, 23, 25, and 27].

**4.1. MOST EFFECTIVE TOOLS FOR BLUEBUGGING**

There are so many tool that used in the Bluebugging, Most of them are as follows: Super Bluetooth Hack 1.08, Blue scanner, Blue Sniffer, Blue Bugger, BT Browser, BT Crawler, Red-Fang, Blue-Print, PSM Scan, RFCOMM Scan, T-crack, Blue-Smack, Nasty vCard, L2CAP Header Overflow, HCI Dump Crash, and Blue-Spam [28].

*Fig.3: Most Effective Tools for Bluetooth*

**4.1.1. Super Bluetooth Hack 1.08**

Super Bluetooth is used for controlling, decoding, and reading information from phone via Bluetooth or infra [28, 29, 30]. Phone list and SMS can be stored in HTML format. In addition to this, it will show information about battery, network and SIM card. Once connected to another phone via Bluetooth you can:

**.** Read messages.

**.** Read contacts list

**.** Change profile

**.** Play with ringtone even if phone is on silent mode

**.** Switch off, and also restart the phone

**.** Restore factory settings and much more

**How to Install:**

**.** Download the Super Bluetooth Hack.

**.** Unzip the file and send it to your phone.

**.** Install the software in your mobile phone.

**.** Inquire new devices through the software.

**.** Connect with some code.

**4.1.2. Blue scanner**

Blue scanner tool can capture or seize the information from a Bluetooth device without pairing. It look for devices and point out them on screen and if you want to see more information just hit enter and it will show devices MAC (Media Access Control) address.

|  |  |  |  |
| --- | --- | --- | --- |
| SR.NO | NAME OF TOOLS | DESCRIPTION | REFERENCES |
| 1. | Super Bluetooth Hack 1.8 | Super Bluetooth is used for controlling, decoding, and reading information from phone via Bluetooth | [28,29] |
| 2. | Blue-sniff | It try to extract more information for each new discovered device. | [28,29] |
| 3. | BT Crawler | It is a scanner for Windows mobile based devices. | [28,29,30] |
| 4. | BT Browser | It can explore and browse the technical specification of surrounding Bluetooth enabled devices. | [28,29] |
| 5. | Blue scanner | Blue scanner tool can capture or seize the information from a Bluetooth device without pairing | [28,29,30] |

*Table-2: Description of various Bluetooth hacking tools*

**4.2. Blue Bug Process**

Here description of blue bug process is given and we can use these commands in backtrack and Linux etc.

Step 1: First we have to configure Bluetooth devices by using

bt~# hciconfig hci0

Output will show like this

Hci0: USB

BD Address: 00:22:44:66:77:33 ACL MTU 987:9 SCO MTU: 34:90

UP RUNNING

RX bytes: 43 acl: 0 sco: 3 events: 8 errors: 0

TX bytes: 44 acl: 0 sco: 3 commands: 8 errors: 0

Step 3: For scanning other devices

bt~# hcitool scan hci0

Step 4: Note down the name and MAC Address of the target device

Step 5: By using this command, we will find target device

Sdptools browse –tree –I2cap (target MAC)

Step 6: To start blue bugger type this command

bluebugger –h

Now there will show all information about phone by using following commands

-m -Name

-d -Device to use

-c -Channel to use

-n - no device look up

-t - time out in second

-o - write output to (file)

Mode:

Info- Read phone information

Phonebook – Read phonebook

Message-Read message

**5. TIPS FOR SECURING OR PREVENTING CELL PHONES**

Firstly we have to improve present Bluetooth security architecture that is not better so it needs a constant upgrading to prevent new unknown threats or blusters but normally we should keep in mind basic steps that is given below:

1. We should start Bluetooth or internet only when required.
2. Keep turn off wireless connection when not needed.
3. Regularly update your cell phone software.
4. Install latest Anti-Virus Software, and keep it update.
5. We should use strong or encrypted password to lock your cell phone.
6. Never share personal information with stranger.
7. Never store personal banking details in cell phones.
8. Make suspicious on social networking websites.
9. Consider disabling the geo-tagging feature on your phone.
10. If you connected public Wi-Fi, do not access susceptible sites where you need to enter your passwords, credit card details and etc.

**6. REPORTS OF BLUETOOTH BLUSTERS**

An overview of some attacks is given below:

A. Adam and Band from A.L Digital Ltd published or disclosed some serious flaws in Bluetooth wireless technology regarding the protocol in 2003 and because of this flaws or vulnerability user can feel trouble and loss of data or information.

B. The first virus related to Bluetooth was disclosed in 2004 in the literatures as a “proof-of-concept”.

C. A mobile malware was detected in January 2005 that is “Lasco”.

**7. SECURITY VULNERABILITY IN BLUETOOTH VERSIONS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SR. NO. | BLUETOOTH VERSIONS | SECURITY VULNERABILITIES | YEAR | REFERENCES | SHOULD BE | DATA RATE | RATIFIED |
| 1. | Bluetooth version v1.0, v1.0B | 1. Here included compulsory Hardware Device Address.  2. Signal strength low. | 1998-1999 | [1,2,31] | 1. The signal strength should be increased | 1Mbit/s | IEEE standard 802.15.1 |
| 2. | Bluetooth version v1.1 | 1. Signal strength was not good.  2. Connection was connect slow process.  3. Discovery strength was not fast. | 1999-2000 | [1,2, 31] | 1. Discovery strength should faster. | 1Mbit/s | IEEE standard 802.15.1 |
| 3. | Bluetooth versions v1.2 | 1. Unit key is reusable and becomes public once used.  2. Unit key sharing can lead to eavesdropping. | 2000-2002 | [1,2, 31] | 1. Unit key use only three time  2. Unit key sharing allowed with password | 1Mbit/s | IEEE standard 802.15.1 |
| 4. | Bluetooth version v2.0 | 1. Transmission speed was not good.  2. Power consumption was little bit high. | 2002-2003 | [1,2, 31] | 1. Transfer data rate should be increased. | 3Mbit/s | IEEE standard 802.15.1 |
| 5. | Bluetooth versions v2.1 | 1. Short PINs are allowed.  2. PIN management is lacking.  3. Encryption key system did not work properly.  4. Encryption key stream repeats after 23.3 hours of use to keep the connection alive. | 2003-2007 | [1,2, 31] | 1. PINs should be larger, and stronger.  2. Strong PIN management.  3. Proper encryption. | 3Mbit/s | IEEE standard 802.15.1 |
| 6. | Bluetooth versions v3.0 | 1. Background compatibility low.  2. Data transmission speed little bit slowly. | 2007-2008 | [1,2,31] | 1. High Background compatibility. | 24Mbit/s | IEEE standard 802.15.1 |
| 7. | Bluetooth versions v3.1 | 1. Link keys are stored improperly.  2. Attempt for authentication are repeated.  3. Encryption key length is negotiable.  4. The master key is shared.  5. No user authentication exists.  6. Algorithm used for Bluetooth encryption is weak.  7. Privacy may be compromised if the Bluetooth device address is captured and associated with the particular user. | 2008-2010 | [1,2, 31] | 1. Proper storage of link keys.  2. Only three attempt for authentication.  3. Encryption key length should be longer and strong. | 24Mbit/s | IEEE standard 802.15.1 |
| 8. | Bluetooth versions v4.0 | 1. Device security was not proper.  2. Power consumption little bit high. | 2010-2011 | [1,2, 31] | 1. Power consumption low.  2. Strong algorithm. | 24Mbit/s | IEEE standard 802.15.1 |
| 9. | Bluetooth versions v4.1 | 1. Device authentication is simple.  2. End to end security is not performed.  3. Security services are limited. | 2011-running | [1,2, 31] | 1. Strong algorithm should be used.  2. Security management should be perfect. | 24Mbit/s | IEEE standard 802.15.1 |

*Table-3: Various Bluetooth versions and their key vulnerabilities*

**8. CONCLUSION**

Bluetooth is occurring a universal protocol. While general applications comprise global positioning devices, smartphones, hands-free audio, and peripheral. Bluetooth devices also exist in health care, mobile banking, and military application. Bluetooth enabled devices now take and handle sensitive information, which can be suspicious position. The lack of mandatory authentication, a weak encryption key scheme, and different vendor protocol implementations have created the possibility for several attacks on Bluetooth devices. This paper presents a ‘BLUEBUGGING” ATTACK and normal security mismanagements in Bluetooth security system.

**9. FUTURE RESEARCH DIRECTIONS**

????????????????????????????????????????????

**REFERENCES**

[1]. http://www.bluetooth.com/Pages/History-of-Bluetooth.aspx (Introduction of Bluetooth).

[2]. http://www.bluelon.com/index.php?id=411 (Introduction of Bluetooth).

[3].http://www.radioectronics.com/info/wireless/bluetooth/bluetooth\_overview.php (Introduction of Bluetooth).

[4].http://bluetooth-mouse-review.toptenreviews.com/bluetooth-devices-a-history.html (Introduction of Bluetooth).

[5].http://www.eetimes.com/document.asp?doc\_id=1269737 (Introduction of Bluetooth).

[6].http://gizmodo.com/5899082/the-secret-history-of-Bluetooth (advantages of Bluetooth technology).

[7].http://www.informit.com/articles/article.aspx?p=27656&seqNum=4 (advantages of Bluetooth technology).

[8]. http://www.wikihow.com/Use-Bluetooth-Technology (advantages of Bluetooth technology).

[9]. http://nds1.nokia.com/phones/files/main\_page/Nokia\_BH-110\_UG\_en (procedure of Bluetooth technology).

[10]. http://www.motorola.com/mdirect/manuals/qg-h500\_9494a56o.pdf (procedure of Bluetooth technology).

[11]. http://www.myblueant.com/downloads/manuals/ST3\_manual.pdf (procedure of Bluetooth technology).

[12]. http://www.bose.com/assets/pdf/soundlink/owg\_en\_soundlink2.pdf (Architecture and using procedure).

[13]. http://www.logitech.com/images/pdf/userguides/bluetooth-faq.pdf (Architecture and using procedure).

[14]. https://www.nsa.gov/ia/\_files/factsheets/i732-016r-07.pdf (Architecture and using procedure).

[15].http://www.hp.com/rnd/library/pdf/understandingBluetooth.pdf (dangerous things about Bluetooth).

[16]. http://emfblues.com/bluetooth-radiation/ (dangerous things about Bluetooth).

[17]. http://inflanation.com/cell-phone-radiation/bluetooth-radiation-may-be-more-dangerous- than-cell-phone-radiation-2/ (dangerous things about Bluetooth).

[18]. http://www.rfsafe.com/bluetooth-radiation-dangerous-cell-phone-radiation/ (dangerous things about Bluetooth).

[19]. http://www.slaw.ca/2014/01/20/protecting-yourself-from-cybercrime-dangers-harden-your-wireless-bluetooth-connections-and-use-public-wifi-with-extreme-caution/ (dangerous things about Bluetooth).

[20]. www.garykessler.net\_li (Blue-bugging).

[21]. www.kaspersky.com2 (Blue-bugging).

[22]. www.larsentoubro.com\_l3 (Blue-bugging).

[23]. http://www.wisegeek.com/what-is-bluebugging.htm (Blue-bugging).

[24]. http://www.mysecurecyberspace.com/encyclopedia/index/bluebugging.html (Blue-bugging).

[25]. http://governing-cyberspace.com/2014/03/07/bluebugging-research-and-analysis-2/ (Blue-bugging).

[27]. http://en.wikipedia.org/wiki/Bluebugging 1/ (Blue-bugging).

[28]. http://www.darkreading.com/risk/new-hacking-tools-bite-bluetooth/d/d-id/1128509? (Most effective tools).

[29]. http://hackinghumans.blogspot.nl/2011/12/bluetooth-hacking-tools.html (Most effective tools).

[30]. http://hackyogi.com/top-5-bluetooth-hacking-tools/ (Most effective tools).

[31]. http://www.bluetoothreport.com/bluetooth-versions-comparison-whats-the-difference-between-the-versions/