ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/89769, December 2016* *ISSN (Online) : 0974-5645*

A Strenous Macroanalysis on the Substratals of Securing Bluetooth Mobile Workforce Devices

B. Nagajayanthi[1]*, V. Vijayakumari[2] and R. Radhakrishnan[3]

[1]VIT University, Chennai - 632014, Tamil Nadu, India;
nagajayanthi.b@vit.ac.in
[2]Jawaharlal College of Engineering and Technology, Ottapalam - 679301, Kerala, India;
ebinviji@rediffmail.com
[3]Sasurie College of Engineering, Vijayamangalam - 638056, Tamil Nadu, India;
rlgs14466@rediffmail.com

Abstract

Objectives: Bluetooth is extending to the blooming Internet of Things (IoT). This article provides an extensive literature survey on the security mechanisms; operational range of Bluetooth. **Statistical Analysis**: The user can achieve 3 Mbps data rate across an operational range of 100 meters. Bluetooth is a pretty impressive technology that connects and controls all the devices over a distance by using an IoT enabled APP due to which is there is a high possibility of Bluetooth charging for its services like the Internet Service Provider (ISP). Bluetooth 4.0 features reliable pairing and encryption whereas the earlier versions had less importance on security. **Findings**: In spite of the inherent security in Bluetooth, insidious security issues remain around Bluetooth transfer. Most of the problems were identified and rectified but still as the usage and technology improves, undiscovered problems bloom. There is no software in Bluetooth that has zero security vulnerabilities. Security threats can be overcome by generating a random key. This key is generated in random by combining the significant features of the device along with the customized features of the person. **Improvements**: Security can be upgraded by improving the strength of Authentication; Encryption algorithm; Augmenting Range of Bluetooth by making it IoT Enabled.

Keywords: Authentication, Encryption, Interoperable, Internet-of-Things, Range

1. Introduction

Bluetooth conceived in the year 1998 with five companies forming the Bluetooth Special Interest Group (SIG) group; and currently it is coordinated and developed by 27,500 companies. Bluetooth Smart or Bluetooth Low Energy (BLE) cable free ad-hoc network operates in the globally available unlicensed 2.4 GHz ISM Band (Industrial, Scientific and Medicinal Band) to transfer data persistently for longer periods of time with low power consuming batteries. Bluetooth encases the users in at rifling bubble of network connectivity to share voice and data using RF waves. The device that initiates the connection becomes the "Master" and the device that gets the information is called the "Slave". There can be upto seven active slaves in a piconet as shown in Figure 1. The slaves should synchronize their frequency hop and lock with the master. Each piconet has a different hopping sequence. Security becomes an issue when the same frequency is always used for transmission. Interference is caused by neighboring devices operating at adjacent frequencies. Bluetooth devices are protected from radio

*Author for correspondence

interference by using frequency hopping. The channel-hopping pseudo-random sequence is generated by using the unique 48 bit MAC address (BD_ADDR) and the clock of the master. Groups of piconet form a scatter net which can be used for range extension. Bluetooth devices are symmetric in the sense that same device can operate as the master or the slave in different piconets; with the communication occurring between the master and the slave, but not between the slaves. Slaves participate in the transfer using Time Division Multiplexing (TDM) in different piconets; with the slave transmitting on odd numbered slots and the master transmitting on even numbered slots. All the devices within the piconet share the same channel using Frequency Hopping Spread Spectrum (FHSS) and transfer over 40 channels spaced 2 MHz apart at the rate of 1600 times per second (every 625 microseconds).Interoperability is achieved between heterogeneous Bluetooth enabled devices: by exchanging the protocol messages between the equivalent layers.

Low power consumption is a stringent requirement for mobile devices and IoT enabled applications. Bluetooth targets on low power consumption by operating the device in the “hold” mode using 30 microampere which would otherwise consume 8-30 milliamps in the active state. This radio chip consumes even more minimized power of 0.3 mA when operated in power optimized modes like standby mode, which is comparably less than 3% of the power consumed used by a standard mobile phone. Bluetooth has provision to automatically shift to a low-power mode as soon as traffic volume lessens or stops thereby saving power. Bluetooth does not require Line Of Sight (LOS) as in Infrared (IR). Bluetooth has upgraded itself in terms of data rate , pairing and Speed from Bluetooth 1.2 till Bluetooth 4.0[1]; but has not evolved much in terms of authentication ,encryption and range extension.

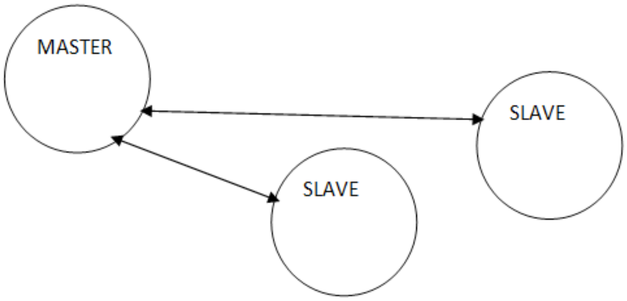

Figure 1. Piconet.

2. Bluetooth Architecture[2]

Bluetooth Stack consists of the Bluetooth Host and the Bluetooth Controller Figure 2, with a Host Controller Interface (HCI) interface connecting both to exchange information. For example the laptop on which the attacks are performed is the Bluetooth Host; forming the software and the Bluetooth dongle is the Bluetooth Controller; forming the hardware which interprets the commands from the Bluetooth Host. The security protocols below HCI are embedded inside the hardware microchip whereas the layers above HCI are infused into the devices software.

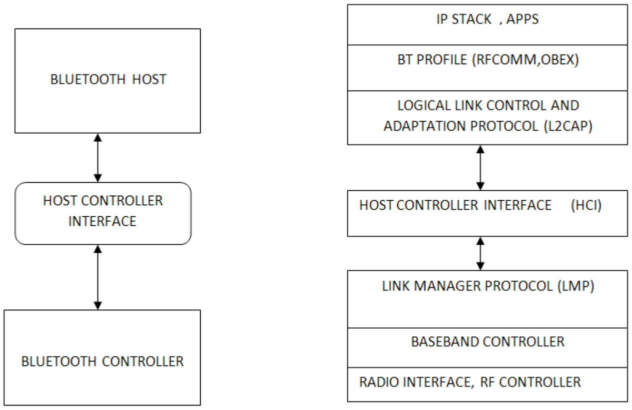
BLUETOOTH HOST
HOST CONTROLLER INTERFACE
BLUETOOTH CONTROLLER
IP STACK , APPS
BT PROFILE (RFCOMM,OBEX)
LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL (L2CAP)
HOST CONTROLLER INTERFACE (HCI)
LINK MANAGER PROTOCOL (LMP)
BASEBAND CONTROLLER
RADIO INTERFACE, RF CONTROLLER

Figure 2. Bluetooth architecture.

The Bluetooth host includes the higher layer protocol: Logical Link Control and Adaptation Protocol (L2CAP); Service Discovery Protocol (SDP). RFCOMM is the transport protocol through which reliable information and commands are sent to the devices using RS-232. L2CAP is used to initiate security procedures and carry high level data packets to RFCOMM. The Bluetooth controller includes the lower layers: Radio Layer; Baseband Layer; Link Control and Management Layers. Practically, the controller functions are performed by the integrated Bluetooth adapter. The Link Manager Protocol is responsible for handling authentication, encryption, power control and pairing. The Baseband layer provides over the air characteristics and rate of transmission. Encryption and Authentication is the responsibility of the Bluetooth Controller.

3. Security in Bluetooth

Bluetooth operates in three modes. In Silent Mode; Bluetooth device monitors the traffic but does not accept any connections. In Private Mode, the device accepts connections from known Bluetooth devices only whereas in Public Mode the device which is in the discoverable mode is open for pairing.

Bluetooth security is managed by the Bluetooth Controller. Bluetooth data transfer is safe, provided the discoverable mode is switched off. Malicious attackers could make the device inoperable by blocking the devices from receiving calls; draining the battery, etc., Hackers can get the data using smart antennas. Researchers pictured the severity of attacks by demonstrating an attack on a Bluetooth device by using an antenna. Naive users are not aware about the hackers who are accessing sensitive information from their Bluetooth enabled phones and other devices. So it is vital that security issues need to be addressed in Bluetooth.

Bluetooth devices are prone to Denial of Service attacks[3] (DoS), virus threats, battery depletion, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation as referred to in Table 3 which substantiates the necessity for security in Bluetooth.

Basic Bluetooth security is ensured by providing:

- **Authentication:** Which issued to validate the uniqueness of the intended devices? User authentication and device authentication are the main elements of Bluetooth Security. Bluetooth architecture concentrates on device authentication. User Authentication should be incorporated**.**
- **Confidentiality:** Ensures that only authorized persons are able to access and view the data.
- **Authorization:** Provides service only to authorized or intended users.
- Three major entities incorporated in generating the link key includes:
- **Bluetooth device address (BD_ADDR/48 bits):** Which is a unique number assigned to each device by the manufacturer .This could be obtained through the inquiry procedure.
- **Private user key (128 bits): A** secret key generated during initialization.
- **A Random number:** (128 bits) is generated by the unit for each new transaction.

Table 3. Security vulnerabilities in Bluetooth

S. No	Security Vulnerabilities
1	For pairing and authentication link key is shared which leads to eavesdropping.
2	Bluetooth 2.0 used Short pins.
3	E0 stream cipher algorithm used for Encryption is weak. Robust encryption key is required.
4	No user authentication is available. Application level security including user authentication can be added via overlay by the application developer.
5	Once the BD_ADDR device address is captured, the user activities can be logged which is a breach of privacy.
6	End to End security is not provided. Only the individual links are encrypted and authenticated.
7	Security services are limited. Services like non-repudiation are not included.
8	Discoverable devices are prone to attack.

4. Existing Methodologies for Secured Data Transfer

For conventional pairing, the user enters a Personal Identification Number (PIN) in both the devices which could be a four digit or eight characters alphanumeric for increased security. A 128 bit Link key is generated by combining the PIN; the device address (BD_ADDR) and a Random number (RAND) generated by the device. Once the link key is generated, they are exchanged and the devices are paired.

Other versions adapted Secure Simple Pairing (SSP) which included ECDH public key cryptography for security. Researchers proposed Auxiliary or Out Of Band (OOB) channels including video and audio to provide protection from eavesdropping.

Data is transferred in a personal area network using Bluetooth, IR etc., Bluetooth is preferred because it is prevalent in the devices used in our day to day activities .Bluetooth is compatible among heterogeneous devices operating on differing operating systems. Pairing mechanism allows the users to authenticate each other.

Commendable research work has been carried out by Mohammed[4] to preserve location privacy in addition to energy conservation for healthcare applications. Researchers Yasir Arfat and Lachhman, proposed a device pairing simulator PSim, to check the usability and security of Bluetooth using Out-of-Band channel methods for increased device security[5]. Kumar analyzed the existing device pairing methods by exchanging the information over human imperceptible channels[6]. For authentication, Rene Mayrhofer carried out research on Specific auxiliary channels[7]. Channels used video, barcodes, blinking patterns, motion by common movement[7], gestures[8], or by synchronized button presses[9] for authentication.

Received Signal Strength Indicator (RSSI) was used as a parameter for authentication to identify the location of the device.

Authentication involves creating and exchanging a link key for pairing. Once verified, the link key is used for encryption. Once generated and exchanged the devices will use this link key for future communication and pairing.

5. Security Oversight

Toby Nixon the chairman of the Board of Directors for the Bluetooth SIG (Special Interest Group) has reasoned out the advancements in Bluetooth 4.2 as the motivation for the spectacular growth in IoT.

For enhanced security Bluetooth operates in four modes[10].

Bluetooth Security Mode 1: Non-secure. In this mode, devices are easily accessible; authentication and encryption are by passed but the devices are susceptible to hacking. This method is suitable when the number of devices is less in the network.

Bluetooth Security Mode 2: A service level-enforced security mode, where the link is established and then the security procedures are initiated.

Bluetooth Security Mode 3: Alink level-enforced security mode in which the Bluetooth device initiates security procedures before the physical link is made.

Bluetooth Security Mode 4: A secured mode in which the security procedures are initiated after the link is established using SSP. This mode requires encryption for all its services. In version Bluetooth 4.2, security is greatly enhanced along with optimizing Energy consumption[11,12].

6. Encryption

Bluetooth 3.0+HS (High Speed) version uses Secure And Fast Encryption Routine + (SAFER+) algorithm for authentication and key generation while Bluetooth 4.0 (Bluetooth Low Energy) used 128-bit Advanced Encryption Standard (AES) algorithm. Recent BLE uses AES-CCM for encryption[13].

7. Vulnerable Threats Faced by Bluetooth in Real time Scenarios

Researchers have probed into the vulnerabilities by performing attacks and simulations. Bluetooth sniffing has become a very popular sport among hackers. The problems regarding Bluetooth security have been reported since its inception. Practical threats incurred in Bluetooth Devices[14] lead to the disclosure of vital information[15]. A mobile malware called 'Lasco' was detected and tested as a self-replicating worm that made the device inoperable[16]. Cambridge University researched and published the threats due to PIN cracking[17]. Kevin Finistere and Thierry Zoller demonstrated the PIN cracking technique by performing a demo .Bluetooth enabled phones posed privacy threats by tracking the users in discoverable mode[18]. Researchers from Secure Network and declared that devices in discoverable mode were more prone to attacks.[19.]

Other major forms of Bluetooth threats were due to malware infused in Bluetooth enabled devices: Blue jacking attack enabled an attacker to probe into the device and get personal details by sending a Card message; Car Whispering allowed the hackers to send and receive audio to and from a Bluetooth enabled car stereo system.

In order to protect the devices against these forms of vulnerabilities, the SIG group and the device manufacturers of Bluetooth enabled devices upgraded security features to ensure that these security lapses do not arise in their products.

8. Comparison

The earlier versions of Bluetooth 2.0 and 3.0 used E0/SAFER+ algorithm for Encryption and the range extended from 10m to 30 m. In the recent version Bluetooth uses AES-CCM algorithm for encryption and also supports upto 50 m for data transfer. Bluetooth 4.1, presented more resourceful features which are analyzed in Table 1 and Table 2.

Table 1. Operating features of Bluetooth

Version	Data Rate and Modulation	Security	Enhancement
1.2	1 Mbps, GFSK	Legacy Pairing	Did not support multihop.
2.1+EDR	2-3 Mbps, π/4 DQPSK, 8DPSK	SHA-256, P-192 ELLIPTIC CURVE	SSP, BR/EDR
3.1+HS	24 Mbps, OFDM	Security Mechanisms are implemented in the LMP layer of the Controller.	Uses Alternate MAC/PHY (AMP) layer, HS
4.0+LE Bluetooth Smart	26 Mbps	Security Mechanisms are implemented in the security manager on the host.	LE, Generic Attribute Profile (GATT) and Security Manager (SM) services with AES Encryption. "Wibree" and "Ultra Low Power Bluetooth
4.1	26 Mbps	P-256 elliptic curve for public key exchange, HMAC –SHA -256 and AES-CTR for authentication, and AES-CCM	Had incremental software updates.
4.2	260 Kbps	Elliptic Curve Diffie–Hellman (ECDH) for key generation, and a new pairing procedure for the key exchange.	IoT, IPv6, Better privacy, Increased speed

Table 2. Key differences between the basic and the updated versions of Bluetooth

Features	Br/Edr (2.0)	Bluetooth Le (4.0)
Encryption Algorithm	E0/SAFER+	AES-CCM
Range	30 m	50 m
Power Consumption	100mW(20dBm)	10 mW (10dBm)
RF Physical Channels	79 Channels With 1 MHz spacing	40 channels with 2 MHz spacing
Slaves	7 active upto 255	Unlimited
Data Rate	1-3 Mbps	1 Mbps

9. Proposed Countermeasures and Enhancements

Bluetooth is becoming widespread because of its inheritance in almost all the electronic gadgets. Bluetooth usage is limited due to its restricted range of operation and prevalent security threats. Security threats can be overcome by generating a random key. By increasing the transmitting power, optimized range could be extended from 10 m to 100 m .Recently Bluetooth devices extends to IoT. Applications include healthcare; remote monitoring and controlling Bluetooth enabled devices. RF based technique depends on Positioning based on signal strength parameters. In Bluetooth Smart, major changes were made in the Bluetooth Protocol Stack and the power consumption was reduced thus making it suitable for IoT. Bluetooth connects to the Internet through IPv6/6LoWPAN. Google is developing an OS for the Internet of Things which serves as the proof of concept.

10. Conclusion and Future Work

A survey report in London analyzed the pattern of Bluetooth users who served as victims. Out of 943 mobile phones, 40% had their default settings in discoverable mode. Moreover, 138 of them were proven to be vulnerable to Blue Snarf attacks. The future of Bluetooth is limited and left open to the developer's imagination. Apple has proved its ongoing support for Bluetooth through its frequent software and SDK updates. In future, range extension of upto 40 to 100 meters is visualized through IoT. By doing this, Bluetooth devices could be deployed in both indoors and outdoors. By increasing the data rate, new ventures are open to Bluetooth to provide real-time services in healthcare; thereby reducing the infrastructure requirements for security. By increasing the range; the devices form a mesh network which forms the key architecture for IoT[21]. Using this topology, the devices interconnect and exchange data to other nodes by accepting and forwarding data thereby providing cost effective solutions with scalability and easier deployment. Ongoing applications of Bluetooth are related to IoT. So strenuous research in security based on device authentication and user authentication is required as more applications evolve[22]. Range extension is possible in Bluetooth using application specific antennas[23].

11. References

1. Haataja K, Hypponen K, Pasanen S, Toivanen P. Bluetooth security attacks: Comaparitive analysis, attacks and counter measures. Springer Briefs in Computer Science. Heidelberg: Springer; 2013.
2. Haataja K. Security threats and counter measures in bluetooth-enabled systems. Kuopio University Library; 2009. p. 68–80.
3. Minar NB-N, Tarique M. Bluetooth security threats and solutions: A Survey. IJDPS. 2012; 3(1):127–48.
4. Mana M, Feham M, Bensaber BA. A light weight protocol to provide location privacy in wireless body area networks. IJNSA. 2011; 3(2):1–11.
5. Malkani YA, Dhomeja LD. PSim: A tool for analysis of device pairing methods. IJNSA. 2009; 1(3):39–49.
6. Kumar. A comparative study of secure device pairing methods. IEEE International Conference on Pervasive Computing and Communications, (PerCom-09); 2009. p. 1–10.
7. Mayrhofer R, Fuss J, Ion I. UACAP: A Unified Auxiliary Channel Authentication Protocol. Transactions on Mobile Computing. 2012; 1(1):710–21.
8. Mayrhofer R, Gellersen H. Shake well before use: Authentication based on accelerometer data. 5th International Conference on Proceedings of Pervasive Computing, ser. LNCS; 2007. p. 144–61.
9. Soriente C, Tsudik G, Uzun E. BEDA: Button-enabled device pairing. Proceedings of IWSSI; 2007. p. 443–9.
10. Available from: https://developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx
11. Bluetooth Specification Version 4.2. Vol. 1: Part A. 5.4.2 Key Generation.
12. Bluetooth Specification Version 4.2. Vol. 3: Part H. 3.6.1 Key Distribution and Generation.
13. Bluetooth Specification Version 4.2. Vol. 3: Part H. 3.6.2 Encryption Information.
14. Streff K. Haar J. An examination of information security in mobile banking architectures. Journal of Information Systems Applied Research. 2009; 1–14.
15. Oates J. Virus Attacks Mobiles via Bluetooth. Available from: http://www.theregister.co.uk/2004/06/15/symbian_virus 22-09-2015
16. F-Secure Article on Lasco. A Worm. 2015. Available from: http://www.f-secure.com/v-descs/lasco_a.shtml
17. Shaked Y, Wool A. Cracking the Bluetooth PIN. 2015. Available from: http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05
18. Going Around with Bluetooth in Full Safety. 2015. Available from: http://www.securenetwork.it/ricerca/whitepaper/download/ bluebag_brochure.pdf
19. F-Secure Article on Lasco. A Worm. 2015. Available from: http://www.f-secure.com/v-descs/lasco_a.shtml
20. Dnyanoba BA, Nagajayanthi B, Ramachandran P. Development of an embedded system to track the movement of bluetooth devices based on RSSI. Indian Journal of Science and Technology. 2015; 8(19):1–7.
21. Nagajayanthi B, Radhakrishnan R, Vijayakaumari V. Healthcare IoT - A multilayer security mechanism using linear programmable pre-coded matrix decomposition method. International Journal of Applied Engineering Research. 2015; 10(24):44554–63.
22. Park J-K, Lee H-S, Kim S-J, Park J-P. A study on secure authentication system using integrated user authentication service. Indian Journal of Science and Technology. 2015; 8(23):1–6.
23. Priyalakshmi B, Kirthi J. Mini UWB-Bluetooth antenna design with band-notched characteristics. Indian Journal of Science and Technology. 2016; 9(1):1–5.