ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 6, June 2017

ANALYSING BLUETOOTH SECURITY SYSTEM

[1] Baibaswata Mohapatra

[1] Department of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1] bmohapatra@Galgotiasuniversity.edu.in

Abstract: Bluetooth is considered to be an essential part in the modern era which provides a short distance wireless communication between multiple devices and networks that consumes low power which makes it convenient for users. The technology uses the free frequency of 2.4 GHz signal range. The challenges in Bluetooth network are mischievous data can be accessed without any authorization, internal attacks can be carried out using ad hoc communication technology, data can be extracted without any virus or attacks. The attacks in the security system are increasing which could be dangerous and could hamper the privacy of the personal data of the user. To overcome the issues of network security in Bluetooth is introduced. There are numerous risks that are created using the Bluetooth, susceptible risks is associated, network securities related to the Bluetooth. The paper focuses on the solution of the above mentioned problem that can be solved by giving safety tips and solutions like conducting seminars, workshops, etc. Due to the increasing security issues, users will be aware of Bluetooth attacks.

Keywords: Bluetooth, communication, Free frequency, Internal attacks, Security, Wireless transmission.

INTRODUCTION

Bluetooth innovation is considered to be a wireless option in contrast to information links by exchanging information utilizing radio transmissions. The name Bluetooth is taken from a tenth century Danish King, “Harald Blatant” or, in English, “Harold Bluetooth”. Bluetooth innovation was made as an open standard to give network and relationship between divergent items and businesses. The Bluetooth Special Interest Group (SIG) is the administrator and maker of the center detail and administrations [1]. That working groups ensure the determination and administrations work to the most elevated exchangeability gauges so clients can recognize, with certainty, their Bluetooth items essentially work. In this 21st century every one of the gadgets are installed with the Bluetooth innovation. Bluetooth is a wireless innovation where it is interface inside the short separation with the low power and minimal effort. Bluetooth uses the standard 2.4GHz sign range. Bluetooth is associated with the gadgets with radio waves rather than links [2].

This wireless system link between the gadgets makes it helpful to move the information between gadgets. Bluetooth is low in cost as they are implanted with a little chip into the gadgets. This wireless link need to ensure that the signs are not hindered to verify the link. To verify the link, there are a few security techniques are accessible. Bluetooth can play out a confided in link that can trade information without asking the authorizations. At the point when the other gadget sets up the link the client needs to conclude it to permit it. While moving the information starting with one gadget then onto the next gadgets. So the security issue emerges. Security is one of the significant difficulties looked by this time of wireless innovation.

BLUETOOTH OVERVIEW

Bluetooth is great for short-run “radio frequency” (RF) communication. Bluetooth is utilized principally to set up “wireless personal area network” (WPAN) [3]. Bluetooth innovation has been coordinated into numerous assortment of business and purchaser gadgets comprise of phones, workstations, printer, car, console, mouse and headsets. This offers clients to frame AD hoc systems between a wide scope of gadgets to transmit voice and information. Bluetooth is lower cost, low force innovation that gives a component to making little wireless systems on an AD hoc premise acknowledged as piconets. A piconet is gathered of at least two Bluetooth gadgets in closest physical closeness that work on a similar channel utilizing a similar frequency hopping grouping [4]. Bluetooth based link between a mobile phones and headset are a case of piconet. Bluetooth piconets are frequently perceived on an impermanent and changing premise which offers interchanges adaptability and versatility between cell phones.

Some principle advantages of Bluetooth innovation

Cable substitution: Bluetooth innovation recoup an assortment of links, for example, those regularly utilized for fringe gadgets (e.g., mouse, console, printers, wireless headsets and ear buds that interface with work areas, workstations, mobile phones, and so forth.)

Simplicity of document dissemination: A Bluetooth-empowered gadget can shape a piconet to help document circulating capacities with other Bluetooth gadgets, for example, workstations, and telephones [5].

Wireless synchronization: Bluetooth can give programmed synchronization between Bluetooth-empowered gadgets. For instance, Bluetooth permits synchronization of contact data comprise of electronic location books and schedules.

Web network. A Bluetooth gadget utilizing Internet network can impart that link with other Bluetooth gadgets. For instance, a workstation will utilize a Bluetooth link with direct a mobile phone to build up a dial-up link so the PC can authorize the Internet through the phone.

HOW DOES BLUETOOTH WORK

Reported by Bluetooth site, the innovation "works in the unlicensed modern, logical and therapeutic (ISM) band at 2.4 to 2.485GHz, utilizing a development range, frequency bouncing, full-duplex sign at a basic pace of 1600 hops/sec". On the off chance that you dropped snoozing part path through that, how about separating it to discover completely how your headset knows to decision a calls from your telephone [6]. Bluetooth chips produce wavelengths that are imperative to frequencies working inside a range explicitly put in a safe spot for this kind of short-extend communication. Different gadgets may get that utilization frequency incorporate cordless phones and infant screens. Nonetheless, there is an issue with continually utilizing a similar frequency. Different gadgets working at the equivalent, or closest, frequencies will cause breaks in the sign. To keep this from being an issue, the sign is grow over a more extensive scope of frequencies. So as to deal with this, the sign hops around the frequency, and on account of Bluetooth that come into 1600 times each second. The regular change in wavelength implies that even a steady sign won't intrude, and won't be interfered, for longer than 1/1600th of a second. Bluetooth headsets can recognize in two unique styles, utilizing a full or part duplex link [7]. A full-duplex sign implies that every single associated gadget are competent to send and get signals – for this situation a two-way discussion – all the while, rather than a half-duplex sign, the same is a walkie-talkie, where each side can at present speak and tune in, but not simultaneously.

Bluetooth Security Methods

There are a few techniques for security to verify the Bluetooth. These security is partitioned into administration level security and gadget level security. These both together secure the gadgets from the unapproved authorization/information transmission. Bluetooth secure strategies quickly clarified underneath.

- Authorization in Bluetooth is the manner in which that depicts authorize control the data by and large .For instance, information in a gadget ordinarily approved to authorize different gadgets data is generally formalized as access control runs in a gadget system. During activity, the system utilizes the entrance control rules to pick whether access demands from verified the gadget client will be affirmed or dismissed. Assets incorporate individual records and the individual information, gave by applications or gadget. In basic term it permits just the allowed gadgets [8].
- Authentication is the way toward choosing the character of the other client. For that authorization it utilizes the key that as of now in the gadgets so it is no reason to produce new key for each new link with a similar gadget associated as of now.
- In the key administration they have various kinds of key administration they are connect key, Pin, encoded key. The connection key are now and then permanent or provisional. This lasting key may store in a non-unstable memory, this can be utilized in the current circumstance and it will be ended, yet the brief key is restricted by lifetime in the current circumstance. In the pin key it is chosen by the utilization of a fixed number. Encoded key will be get from the present connection key in that encryption is actuated.

These Bluetooth protections are partitioned into 3 modes.

Mode 1: A Bluetooth gadget won't start any security. This is a non-secure mode. Fundamentally the validation and encryption security techniques to enable any Bluetooth device associate with it.

Mode 2: A Bluetooth gadget doesn't start security systems before link connection. This mode permits extraordinary and adaptable arrangements for applications, particularly running applications with various security necessities in the equivalent. This is an application level implemented security mode. The idea of a security administrator is acquainted in this mode with control access to administrations. The incorporated security director keeps up authorize control arrangements and is liable for interfacing with different conventions and gadget clients. Validation, classification, and approval are bolstered in this mode [6].

Mode 3: A Bluetooth gadget starts security techniques before the connection set-up is finished. This is a connection level authorized security mode and is fixed. Since this security mode is fixed it doesn't know about any application layer security. Validation and encryption are bolstered in this mode. Validation and encryption are acknowledged utilizing a common mystery interface key that is determined during the matching procedure.

BLUETOOTH SECURITY

1. Bluetooth Security and Vulnerabilities

Bluetooth innovation is a wireless substitute to information links by trading information utilizing radio - transmissions. Bluetooth innovation was made as an open standard to approve network and joint effort between divergent items and ventures. Like any wireless innovation, Bluetooth additionally has various security vulnerabilities. These vulnerabilities may contain the gadget or the systems that the gadget associates with. In any case if the basic Bluetooth security highlights are utilized appropriately, it ought to give sufficient security [9].

2. Technology of Bluetooth Security

When gadgets associate with one another, Bluetooth makes a connection which utilizes open pre-shared key confirmation and calculations which is viewed as solid when utilized accurately. The quality of the Bluetooth security for the most part depends on the arbitrariness and the length of the passkey utilized at the time of their first link. Discoverability and connect ability settings likewise assume a significant job in deciding the security quality. These settings control whether the gadget can looked by other Bluetooth gadgets and how it tends to be associated. Likewise discretionary client approval for link demands gives additional security[10].

3. Bluetooth Vulnerabilities

Through structure, Bluetooth utilizes distributed innovation. Bluetooth has an intricate particular and offers help for a great deal of administrations. A portion of these administrations incorporate information yield gadgets like keypad and mouse, earphones, speakers, networking, document move and printing. All together for these administration to work and speak with gadgets, planners and developers executes Bluetooth for a wide assortment for working systems, chipsets and gadgets. Settings like discoverability, association inclinations and security of the interface are not generally the equivalent and rely upon the software engineer. Because of this, Bluetooth is available to a great deal of security vulnerabilities. A portion of the known Bluetooth assaults incorporate the accompanying:

1. Character identification;
2. Location following;
3. Denial of administration;
4. Unintended control and access of information and voice channels;
5. Unauthorized gadget control and information access.

For instance, specialists have indicated that Bluetooth headset can utilize gadgets in a few different ways. This trade-off is because of the headset profiles' help for amazing communication flagging directions and the very normal utilization of powerless built up passkeys (regularly "0000").

4. Types Bluetooth Attacks

Since there are billions of Bluetooth gadgets being used, vindictive security infringement are general occasions now and it is relied upon to ascend sooner. In actuality, the ascent use of Bluetooth gadgets makes security stresses considerably additionally upsetting. From this point forward, Bluetooth security engineering needs a consistent advancement to keep away from new unidentified dangers. Like any further wireless communication system Bluetooth transmission can be purposely jammed or restricted. Fake or changed data can be conveyed to the gadgets by the digital criminals [11]. Security dangers in Bluetooth can be expanded into three significant classifications as follows:

- **Disclosure risk**: The data can spill out of the objective system to a meddler that is unapproved to get to the data.
- **Integrity risk:** The data can be purposely remedied to delude the beneficiary.
- **Denial of Service (DoS) risk**: The clients can be hindered to get associate with an assistance by making it either inaccessible or seriously constraining its accessibility to an approved client. Bluetooth security is directly a functioning exploration region in both scholarly community and industry. Security dangers like profession and uprightness assaults normally bargain some delicate data and accordingly, can be risky. Then again, DoS assaults generally

upset Bluetooth arrange clients and are viewed as less risky. Amazing directional receiving wires can be utilized to extraordinarily expand the examining, spying and assaulting scope of practically all sort of Bluetooth gadget. One extraordinary case of a long-separation assaulting apparatus is the Blue Sniper Rifle. It is a rifle stock with a prevailing directional reception apparatus required to a little Bluetooth-perfect PC. The examining, spying and assaulting can be finished over a mile missing from the objective gadgets. Along these lines, the likelihood that an assailant is utilizing range improvement apparatus for exposure, respectability and DoS assaults ought to be taken extremely [12].

CONCLUSION

This paper gives a diagram of a portion of the large assaults that Bluetooth has tested throughout the years alongside some potential arrangements. Some security tips for the clients have likewise been provided for in a split second make mindfulness among them to be progressively cautious about their significant individual data. Even though all larger part of gadgets presently convey utilizing this innovation, the dangers are profound more prominent if the security dangers are dismissed by our companions in this industry. Bluetooth security experts should give programmed updates to its security conventions and client security insurance techniques for each new security open up so assurance of the gadget client's close to home data turns into the essential goal. Because of constraints in time and assets, just a general writing review has been introduced in this paper. Developing gadgets all have Bluetooth as a fundamental element and its potential applications are expanding, so its future vulnerabilities should be broke down through further research in this field.

REFERENCES

[1] Bluetooth Special Interest Group (SIG), ‘Bluetooth Core Specification Version 5.0’, 2016.

[2] J. Decuir, ‘Introducing bluetooth smart: Part 1: A look at both classic and new technologies’, *IEEE Consumer Electronics Magazine*. 2014.

[3] R. Mitchell and I. R. Chen, ‘A survey of intrusion detection in wireless network applications’, *Computer Communications*. 2014.

[4] I. Howitt and G. Jore A., ‘IEEE 802.15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)’, *Wirel. Commun. Netw.*, 2011.

[5] M. Verma, S. Singh, and B. Kaur, ‘An Overview of Bluetooth Technology and its Communication Applications’, *Int. J. Curr. Eng. Technol. E Int. J. Curr. Eng. Technol.*, 2015.

[6] W. Ren and Z. Miao, ‘A hybrid encryption algorithm based on DES and RSA in Bluetooth communication’, in *Proceedings - 2010 2nd International Conference on Modeling, Simulation, and Visualization Methods, WMSVM 2010*, 2010.

[7] M. Duarte, C. Dick, and A. Sabharwal, ‘Experiment-driven characterization of full-duplex wireless systems’, *IEEE Trans. Wirel. Commun.*, 2012.

[8] M. Denis, C. Zena, and T. Hayajneh, ‘Penetration testing: Concepts, attack methods, and defense strategies’, in *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*, 2016.

[9] M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, ‘Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption’, *J. Inf. Secur.*, vol. 09, no. 02, pp. 168–176, 2018.

[10] M. Ghallali, D. El Ouadghiri, M. Essaaidi, and M. Boulmalf, ‘Mobile phones security: The spread of malware via MMS and Bluetooth, prevention methods’, in *ACM International Conference Proceeding Series*, 2011.

[11] M. La Polla, F. Martinelli, and D. Sgandurra, ‘A survey on security for mobile devices’, *IEEE Commun. Surv. Tutorials*, 2013.

[12] D. Mani and A. Mahendran, ‘DDOS detection and mitigation for managed security of cloud resources’, *Int. J. Pharm. Technol.*, 2016.

[13] Nisha Pandey, B. S. Chowdhary , Bhagwan Das , D. M. Akbar Husain , Vishal Jain , Tanesh Kumar, “Design of Data Processing Device on Low Power SPARTAN6 FPGA”, International Journal of Control and Automation (IJCA).

[14] Sujeet Pandey, Puneet Tomar, Lubna Luxmi Dhirani, D. M. Akbar Hussain, Vishal Jain, Nisha Pandey, “Design of Energy Efficient Sinusoidal PWM Waveform Generator on FPGA”, International Journal of Signal Processing, Image Processing and Pattern Recognition (IJSIP), Vol. 10 No. 10, October, 2017, page no. 49-58 having ISSN No. 2005-4254.

[15] B.Powmeya , Nikita Mary Ablett ,V.Mohanapriya,S.Balamurugan,”An Object Oriented approach to Model the secure Health care Database systems,”In proceedings of International conference on computer , communication & signal processing(IC3 SP)in association with IETE students forum and the society of digital information and wireless communication,SDIWC,2011,pp.2-3, 2011