Analyzing the Security and Safety Issues of Bluetooth Technology

Ajay Rastogi, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email Id- ajayrahi@gmail.com

ABSTRACT: With its ability to transmit wirelessly across short distances at a cheap cost and with little power consumption, Bluetooth technology has become an indispensable component of the modern world. The 2.4GHz frequency band is what Bluetooth uses. The security risks in the Bluetooth network include unauthorized access by hostile parties, the possibility of internal assaults via ad hoc transmissions, the extraction of data undetected, the possibility of data corruption on wireless devices from viruses or other susceptible attacks, etc. The security sectors are becoming more vulnerable, which might be risky for the privacy of personal data of the user. Network security for Bluetooth is proposed to address these problems. Therefore, the aim of this paper is to review the security and safety issues of the Bluetooth technology and the discussion on the basic of security methods of Bluetooth.

KEYWORDS: Data, Bluetooth, Security, Safety, Technology.

1. INTRODUCTION

The advancement of smart technology has been centers on Bluetooth devices. All smart home appliances, headphones, and practically every other gadget one can think of are all compatible with this battery-operated technology. Smartphones pair to transfer data, and as we all know, hackers are constantly present when data is exchanged. If the Bluetooth links with a malevolent person's Bluetooth, one might quickly lose the sensitive information stored in the email, social networking, or banking applications. Because of this, people need to be aware of the serious cybersecurity risk that Bluetooth presents and take steps to be safe[1].

Since its introduction to the market in 2000, Bluetooth has grown in popularity on a global scale. People may now easily connect to their gadgets and communicate data through them thanks to Bluetooth. Bluetooth safety, though? The likelihood of assaults and threats against your information shared online is rising along with the use of more modern technologies. Bluetooth technology has altered the lives of many people, yet it is also vulnerable to some assaults. Bluetooth networks therefore have a special type of vulnerability[2], [3]. Hackers continue to develop new techniques for attacking Bluetooth devices and stealing data. As a result, experts are continually searching for a solution to guarantee the security of the Bluetooth-connected devices.

1.1. Basic Concept of Bluetooth Security

Bluetooth security is crucial because devices may be attacked via a variety of wireless and network methods, such eavesdropping, man-in-the-middle attacks, signal tampering, and resources theft. The safety of Bluetooth implementation and standards also must handle more targeted Bluetooth-related threats that take use of known flaws. Attacks on Bluetooth versions that have been insufficiently protected may be one of these. Such attacks could provide intruders unauthorised access. The safety of Bluetooth might not be a concern for several users, but attackers could be able to gain access from phone numbers to more confidential material that may be stored on Bluetooth-enabled phones and other electronic devices[4], [5]. To provide Bluetooth security, there are three primary methods (Figure 1):

- Identification: The identification of the connecting devices is confirmed during the authentication procedure. The primary Bluetooth security components are not included in user authentication.
- Confidentiality: This method makes sure that only authorised devices may access and view the data, preventing information from being eavesdropped.
- Authorization: By confirming that a device is authorised to utilise a service before allowing it to do so, authorization prohibits access.

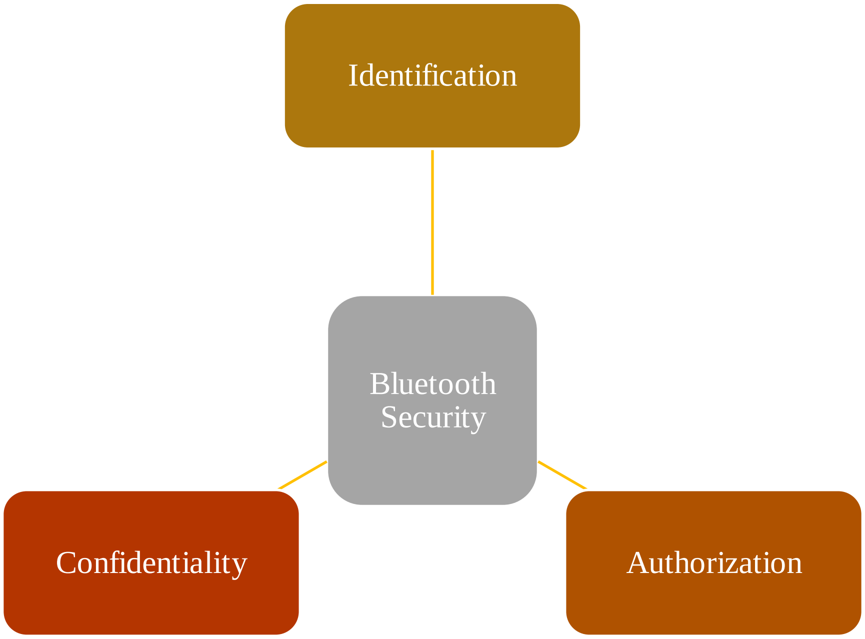

Figure 1: Illustrating the three primary methods of Bluetooth Security.

1.2. Security Issues of Bluetooth Device

Devices may connect with one another wirelessly thanks to Bluetooth technology. Any device that uses Bluetooth may communicate as long as it is within the appropriate range because it uses short-range radio frequency. The technology is frequently utilised to provide communication between two distinct kinds of devices. Because it is a "electronics standard," producers that want to include it must comply with certain specifications while creating their products. These requirements guarantee that the gadgets can identify and communicate with other Bluetooth-enabled gadgets[6]. Major four security issues of Bluetooth technology are as follows (Figure 2):

- *BlueSmacking*
- *BlueJacking*
- *BlueSnarfing*
- *BlueBugging*

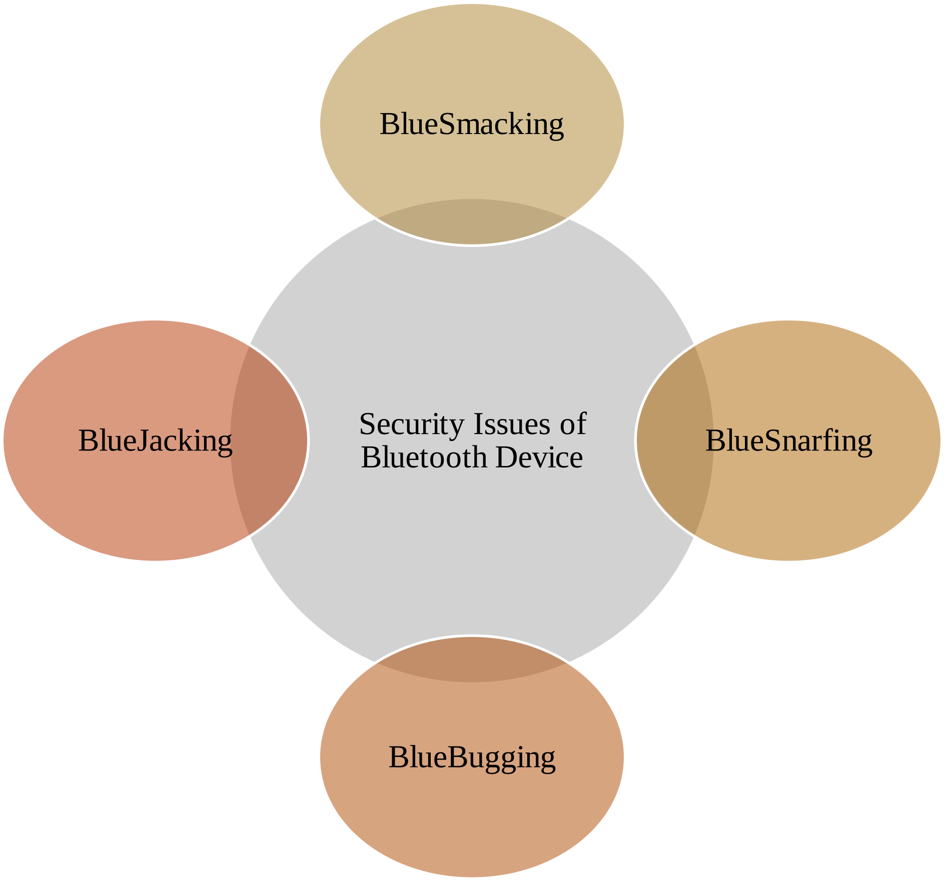

Figure 2: Illustrating the Major Security Issues of Bluetooth Devices.

1.2.1. BlueSmacking

The Denial of Service attack, which Bluetooth devices are capable of, may be implemented using this approach. The phrase "Denial of Service" is not unfamiliar if you work in the IT industry. A target, like a server, will experience this when it receives many queries or packet at once, which is more than it can handle. The system can fail and collapse as a result of being overwhelmed by the user requests. This attack, when compared to many other potential attacks, is not as serious. The server may be immediately restarted to address this issue and made accessible to users. With the use of the Bluetooth networking stack's L2CAP layer, this attack transfers a significant amount of data[7].

1.2.2. BlueJacking

It sounds like Bluetooth device hijacking. It occurs when one Bluetooth device takes control of another and floods it with spam adverts, causing some other device to operate slowly. There is a chance that the attacker remains inside the broadcasting range of bluetooth, which may potentially extend 10 metres. Another possibility is that the attacker will leave the device they are using to hijack it all within range of the device and control it from outside.

The owner will get several notifications as a result of this attack. Users are the target of a phishing attack if you are receiving text messages on the phone. It is an assault when the perpetrator poses as a reliable individual and seeks to take private sensitive information. These messages can contain a link to a malicious website that will quickly and effectively steal user personal information.

1.2.3. BlueSnarfing

All Bluetooth-specific exploits feature the term "blue" in their titles during these assaults. BlueSnarfing is somewhat analogous to BlueJacking in certain aspects, but it poses a greater risk to consumers. BlueJacking attacks cause your device to explode with junk data, whereas BlueSnarfing attacks remove data from the device, making it more susceptible. Furthermore, the attacker can access any of the sensitive data via Bluetooth-enabled devices, leading to a more damaging intrusion.

1.2.4. BlueBugging

Compared to BlueJacking and BlueSnarfing, it is a more sophisticated step. The user's Bluetooth-connected gadget receives a backdoor due to this attack. It can open up access for an adversary or outsider to obtain your insider knowledge and access. These kinds of assaults are used to hunt down someone by monitoring their phone information. Such an assault may occasionally be advantageous from a legal standpoint to obtain inside knowledge[8]–[10].

2. DISCUSSION

To address unique Bluetooth network risks and vulnerabilities, organisations should implement countermeasures. Educating employees who will work with Bluetooth-enabled devices to a sufficient degree of expertise and comprehension is the first option. The use of Bluetooth technology requires organisations to develop and publish security policies that include user obligations and the usage of Bluetooth-enabled devices. In order to help personnel in improving their understanding and expertise of Bluetooth, organisations should also include awareness-based education[11], [12].

3. CONCLUSION

More than merely replacing data cords between devices, Bluetooth is a wireless technology. Greater range, faster communication rates, and more secure security features are all supported by Bluetooth version 4.0. This study presented some historical background information regarding the Bluetooth system, its uses, and numerous security concerns related to Bluetooth. Threats against these vulnerabilities are also mentioned, as well as Bluetooth technology flaws. A few potential defences are suggested that may be applied to boost Bluetooth security. Since Bluetooth is indeed a comparatively recent wireless technology, new attacks on Bluetooth security are probably going to be discovered.

REFERENCES

[1] S. Kim and G. Garrison, "Investigating mobile wireless technology adoption: An extension of the technology acceptance model," *Inf. Syst. Front.*, 2009, doi: 10.1007/s10796-008-9073-8.

[2] M. R. Bhalla and A. V. Bhalla, "Generations of Mobile Wireless Technology: A Survey," *Int. J. Comput. Appl.*, 2010, doi: 10.5120/905-1282.

[3] C. L. Gan and V. Balakrishnan, "An empirical study of factors affecting mobile wireless technology adoption for promoting interactive lectures in higher education," *Int. Rev. Res. Open Distance Learn.*, 2016, doi: 10.19173/irrodl.v17i1.2111.

[4] A. Reyes-Muñoz, M. C. Domingo, M. A. López-Trinidad, and J. L. Delgado, "Integration of body sensor networks and vehicular Ad-hoc networks for traffic safety," *Sensors (Switzerland).* 2016. doi: 10.3390/s16010107.

[5] S. Tanwar, "Threats & Security Issues in Ad hoc network: A Survey Report," *Int. J. Soft Comput. Eng.*, 2013.

[6] U. L. M. Rijah, S. Mosharani, S. Amuthapriya, M. M. M. Mufthas, M. Hezretov, and D. Dhammearatchi, "Bluetooth Security Analysis and Solution," *Int. J. Sci. Res. Publ.*, 2016.

[7] A. M. Hainen, S. M. Remias, D. M. Bullock, and F. L. Mannering, "A hazard-based analysis of airport security transit times," *J. Air Transp. Manag.*, 2013, doi: 10.1016/j.jairtraman.2013.06.002.

[8] S. M. Babamir, R. Nowrouzi, and H. Naseri, "Mining bluetooth attacks in smart phones," 2010. doi: 10.1007/978-3-642-14292-5_26.

[9] M. Liao, "Bluetooth vulnerabilities in data security of mobile phones," 2012.

[10] G. K. Kostopoulos, "Bluetooth in mobile telephony: Privacy and security issues," 2009.

[11] R. Mehra, "Connecting & Addressing Security Concerns of Bluetooth Technology in Current Scenario," *Int. J. Emerg. Trends Sci. Technol.*, 2016, doi: 10.18535/ijetst/v3i01.05.

[12] B. K. Mandal, D. Bhattacharyya, and T. H. Kim, "A design approach for wireless communication security in bluetooth network," *Int. J. Secur. its Appl.*, 2014, doi: 10.14257/ijsia.2014.8.2.35.