Challenges in Medical Device Communication: A Review of Security and Privacy Concerns in Bluetooth Low Energy (BLE)

Michail Terzidis
CERTH - ITI
Thessaloniki, Greece
email : terzmich@iti.gr

Notis Mengidis
CERTH - ITI
Thessaloniki, Greece
email : nmengidis@iti.gr

Georgios Rizos
CERTH - ITI
Thessaloniki, Greece
email : grizos@iti.gr

Mariana S. Mazi
CERTH - ITI
Thessaloniki, Greece
email : msmazi@iti.gr

Konstantina Milousi
CERTH - ITI
Thessaloniki, Greece
email : kmilousi@iti.gr

Antonis Voulgaridis
CERTH - ITI
Thessaloniki, Greece
email : antonismv@iti.gr

Konstantinos Votis
CERTH - ITI
Thessaloniki, Greece
email : kvotis@iti.gr

***Abstract*—The employment of medical devices and sensors in healthcare is growing rapidly each year, as their contribution in diagnosis and treatment is immeasurable. Given the paramount importance of security and privacy in the healthcare sector, the increasing number of devices in the industry also brings a rise in potential targets for exploitation and security misconfigurations. Most of these devices communicate using Bluetooth Low Energy (BLE), and despite BLE's advantage in providing a communication protocol characterized by low energy consumption, an indispensable requirement for medical applications, its simplified protocol stack and general architecture render it susceptible to various security and privacy flaws. Consequently, a comprehensive analysis of the BLE protocol becomes imperative in order to assess the security aspects of medical devices thoroughly. Furthermore, this analysis aims to identify the most critical vulnerabilities and specific attacks targeting the Bluetooth protocol that necessitate mitigation and remediation.**

Keywords-Bluetooth; BLE; Internet of Things; IoT; Cybersecurity; Medical Devices.

I. INTRODUCTION

The development and widespread adoption of the Internet of Things (IoT) have given rise to a significant proliferation of smart medical devices and sensors designed to record, store, and transmit data. These technological advancements find diverse applications, with a notable emphasis on their integration into the medical field. Within the healthcare sector, such medical devices and sensors are deployed to enhance the quality of patient care, encompassing a range of examples such as heart rate monitors, blood pressure monitors, blood glucose monitors, insulin pumps, and implantable cardiac devices.

In order to achieve seamless interoperability, many of these medical devices and sensors rely on wireless communication protocols. Among the key considerations in choosing a communication technology that enables interconnection in IoT applications is low power consumption, making Bluetooth Low Energy (BLE) an increasingly favored option, as stated in the Bluetooth Marker Research report of 2020 [4]. However, as mentioned in [9], [13] and [14] the simplicity of Bluetooth's protocol stack also gives rise to certain inherent security and privacy vulnerabilities.

The issue of medical device security has garnered significant concern within the healthcare sector, particularly in the wake of several incidents involving malicious attacks. R. Horton in [1] shared his research, which uncovered plenty of cases where, Bluetooth was the reason for the recall of thousands of medical devices, which raised a lot of concerns in the patients that were in need of these devices. BLE, has potential security risks, which in turn can impact the security of the interconnected devices. Consequently, a more robust security and vulnerability assessment process becomes imperative to identify flaws in BLE's security architecture, delineate specific Bluetooth-related attack vectors, and propose effective mitigation strategies. These measures are essential to uphold security and privacy standards within healthcare IoT environments.

In Section 2, we provide a background for medical devices and the Bluetooth protocol followed by a presentation of the security issues of the BLE protocol and an overview of various attacks against it in Section 3. In the concluding section, a detailed examination of Bluetooth attack incidents in healthcare is presented along with an analysis of pertinent mitigation techniques.

II. BACKGROUND

Medical devices have changed from the once non-networked and isolated equipment to devices with one-way vendor monitoring, to fully networked equipment with bi-directional communications, remote access, wireless connectivity, and software. Thus, with software increasingly embedded into medical devices, the transition to Software-as-a-Medical-Device (SaMD) has occurred [2]. The global wearable medical devices market size was estimated at USD 28.15 billion in 2022

 ISBN: 978-1-68558-113-8

and is expected to hit over USD 169.58 billion by 2030 with a registered Compound Annual Growth Rate (CAGR) of 25.6% from 2022 to 2030 [3]. Further accentuating the expansion of wearable medical devices, the 2020 Bluetooth Market Research report highlights the significant impact of the COVID-19 pandemic on this sector. Consequently, the healthcare wearable market, encompassing connected blood pressure monitors, continuous glucose monitors, pulse oximeters, and electrocardiogram monitors, witnessed a surge in demand, resulting in 12 million shipments in 2020 alone. This upward trajectory is anticipated to continue, with projected shipments reaching 52 million in 2025 [4]. BLE is currently used in many types of medical devices that have been approved and cleared by the Food and Drug Administration (FDA), including Blood pressure, Blood Glucose Meter, Continuous Glucose Meter, Pulse oximeter, Thermometer, Weight scale, Insulin pump, Cardiac implant, Electrocardiogram and Prosthetics [12].

A. Security and privacy in healthcare

Many consumers and clinicians are eager to adopt and use medical devices and health-related technologies to promote health and well-being. Nevertheless, despite the potential benefits in terms of enhanced efficiency and cost, the integration of such technologies also necessitates the careful examination and resolution of concerns pertaining to security and privacy.

Vulnerabilities identified in the Bluetooth protocol have rendered certain Bluetooth-enabled medical devices susceptible to exploitation. This concern has been further underscored by reported incidents of Bluetooth attacks against defibrillators, according to a recent report by WIRED [5]. The study, conducted by security experts affiliated with a Midwestern medical facility chain over a span of two years, revealed critical security weaknesses in medical devices utilizing Bluetooth technology. Despite the fact that Bluetooth technology has given diabetes patients a more efficient and effective way to manage their diabetes by providing them with the ability to easily monitor their blood glucose levels, it is crucial to acknowledge the potential risks associated with its usage. As presented in [6], individuals in close proximity can potentially exploit this technology through Man-in-the-Middle and eavesdropping attacks. Notably, even seemingly innocuous wearable devices like smartwatches and smart bracelets, which also employ Bluetooth communication channels, are not exempt from vulnerability to Bluetooth-based attacks, as demonstrated by the findings of Bitdefender experts [7], [8].

B. Basic architecture of Bluetooth Low Energy protocol

BLE was first introduced in the Bluetooth 4.x version, released in June 2010. Bluetooth, specifically BLE, has become the preferred technology for IoT devices [9]. Bluetooth Low Energy is regarded as a different technology that specifically targets markets where the demand is for ultra-low power rather than high throughput [48]. This low energy version of Bluetooth could positively affect IoT technology, by giving devices the ability to exist and successfully function in a wide variety of application scenarios [9].

The main building blocks of the BLE protocol stack [13] are the controller, which includes the hardware to transmit and receive data and the host, which enables applications to scan, discover, connect, and exchange information with peer devices. The communication between those two parts is done through the Host Controller Interface (HCI). The BLE Protocol Stack has the following functionalities [48]:

- ATT (Attribute Control Protocol) : is a client-server-based stateless low-level protocol that defines data exchange between a client and a server.
- GAP (Generic Access Profile): specifies device roles, modes and procedures for the discovery of devices and services, the management of connection establishment and security.
- SM (Security Manager): controls the pairing mechanism, key distribution and key management of a device. It is also responsible to encrypt and decrypt data.
- GATT (Generic Attribute Profile): defines a framework that uses the ATT for the discovery of services, and the exchange of characteristics from one device to another.

The security properties of a BLE connection are defined primarily through the selected security mode, security level and the used pairing method. BLE protocol was introduced in version 4.0 and was later developed through versions 4.1, 4.2, and 5.0x.

III. Problem Statement

A. Inherent security issues of the BLE protocol

The pairing process in Bluetooth and BLE has been identified as a significant contributor to security issues, as highlighted in [14]. Attacks can be executed at various stages, both prior to its completion and after successful device pairing.

Notably, the authentication challenge requests during pairing are unrestricted in number, thereby providing a potential attack surface for adversaries to accumulate challenge responses, which may reveal information about the secret link key [14].

Furthermore, if the storage of link keys is poorly implemented, then an adversary can view or even modify them. An additional vulnerability derives from the encryption key's minimum length, which can be as short as a single byte. This relatively limited key length could undermine the overall security of the system. Additionally, it is crucial to acknowledge that the Bluetooth standard incorporates only device authentication, lacking the additional layer of user authentication. Finally, another vulnerability lies in the indefinite duration of a device's discoverable/connectable mode. This opens a window of opportunity for potential attackers to exploit the device's accessibility over an extended period [14].

B. BLE attacks

In this section, we describe attacks like Man in The Middle (MiTM), Denial of Service (DOS), Eavesdropping and how to implement them against the BLE protocol, but also some BLE-specific attacks like the treacherous attacks, distortion

 ISBN: 978-1-68558-113-8

and others that can be implemented because of specific BLE vulnerabilities.

Passive Eavesdropping attacks

This type of attack as mentioned in [15], refers to the unauthorized access and monitoring of Bluetooth communications and involves the use of specialized software and hardware tools capable of intercepting and analyzing Bluetooth traffic. Within this context, attackers can execute a passive sniffing attack, wherein they position themselves along the data transmission path. The susceptibility of BLE to this attack is particularly pronounced due to its simplified and predictable channel hopping design.

Active Eavesdropping attacks

In addition to the previous type of attack, where an attacker monitors Bluetooth communication, in this attack he also tries to steal sensitive data. MiTM and Replay are two variations of active eavesdropping attacks.

- In the context of BLE, a conventional MiTM approach faces a limitation, as it cannot establish simultaneous connections to both communication endpoints. Hence, executing a BLE MiTM attack necessitates the utilization of two components with the capability to act in unison. For instance, in a scenario involving a mobile app attempting to communicate with a smart device, one of the components can be employed to establish a connection with the mobile app while posing as the smart device, while the other component simultaneously connects to the smart device while posing as the mobile app. This dual-component approach enables the MiTM attacker to intercept and manipulate the data being exchanged between the communication parties [8].
- Replay attack is a common form of attack for wireless communications where the attacker captures legit communication packets and then re-transmits those packets at a later time. After intercepting the packets, the attacker can simply re-transmit the whole intercepted packet; an example of such attack, performed on a smart lock, is described in [16].

Device Cloning

In this type of attack, the attacker tries to deceive the target by assuming the identity of a trusted device, thereby misleading them into establishing a connection. Afterwards, in the case of successful connection, he tries to actively steal the victim's data and cause notable damage to the victim's devices. To perform this type of attack, an attacker should spoof his MAC address, name, and GATT characteristics to confuse the victim.

- MAC spoofing : The attacker spoofs the MAC address as well as GATT services. By employing specialized software tools like Gattacker, the attacker effectively replicates the GATT services of the original peripheral device, thereby assuming the role of a counterfeit peripheral entity [17].
- Forced Repairing : BLE devices, upon their initial connection, undergo a process of pairing and bonding, wherein a Long-Term Key (LTK) is generated. In this attack, the attacker tricks the paired devices to undergo the unpairing process and initiate a new connection. Unpairing two connected devices itself is not an inherently malicious act, however after successfully carrying out this attack, the malicious actor has the ability to launch more severe attacks such as eavesdropping passively or even actively performing a MiTM attack.

Cryptographic Vulnerabilities

In these type of attacks, the attackers try to compromise the encryption of the communication protocol, exploiting inherent cryptographic weaknesses and flawed key exchange mechanisms within the BLE protocol. Some of the most prominent attacks in the aforementioned category are the following:

- Offline PIN cracking attack : PIN Cracking attack can be done in many ways, such as using brute force to crack the PIN, another way is to use a dictionary with a set of possible given PINs, also known as dictionary attack. The security vulnerability of BLE is that the length of the Temporary Key (TK) to generate the encryption key is too short, as described in [18].
- Device Authentication attack : This attack is feasible because of a cryptographic weakness of the passkey-based pairing of BLE. The authors of [19] describe how an active fraudulent Responder can bypass passkey authentication, despite it being based on a one-time generated PIN.
- BlueMirror attacks : BlueMirror is a collection of seven attacks published in May 2021 [29] of which three affect BLE pairing. During a reflection attack an intruder collects a message in the authentication protocol, then sends it without modification to the original sender.
- BLUR attacks : The Bluetooth standard (v4.2) introduced Cross-Transport Key Derivation (CTKD). CTKD allows establishing BT and BLE pairing keys just by pairing over one of the two transports. The authors in [30] present the first complete description of CTKD obtained by merging the information from the Bluetooth standard with the results from their reverse-engineering experiments. These attacks allow to impersonate, MiTM, and establish connectins with arbitrary devices.

Denial of Service

Similarly to traditional DoS attacks, the goal is to make the resources of the system unavailable to the intended users. In BLE, the attacker primarily targets the master, so that the slave cannot get proper services in the BLE mesh network. Some of the most prominent attacks in the literature are:

- Battery Exhaustion Attack : One of the main features of BLE is its brief wake period, during which it facilitates data transfers before returning to its sleep mode once more. [20]. This attack targets this unique feature of BLE by keeping the device awake. Bluetooth piconet is subject to this form of attack [21].
- Denial of Sleep : When data from the base sensing layer is provided by low power technologies, such as BLE, a

 ISBN: 978-1-68558-113-8

class of vulnerabilities called Denial of Sleep attacks can be especially damaging to the network. These attacks can reduce the lifespan of the sensing nodes by several orders of magnitude, rendering the network unusable [22].

- Jamming : Jamming describes the deliberate blocking, and therefore suppression of specific parts of a communication or the target medium as a whole [13]. By jamming only packets sent by the peripheral to the central device, an attacker can trigger the timeout in the central device. Since the timeout was triggered only in the central device the attacker can step in as central device and hijack the BLE connection. This attack was published in 2018 by Damien Cauquil and implemented in the tool BtleJack [23].

Treacherous

The authors of [36] describe the treacherous attacks, as the type of attacks that are based on establishing a trusted relation between the devices and then breaking the trust. That way, the attacker can gain full access to the system and exploit it. There are two different attacks mentioned:

- The Backdoor Attack is the method of gaining trust of the victim device through the pairing mechanism. It ensures that the attacker's device does not appear on the victims list of paired devices. In this way, the attacker can monitor the activities of the victim device.
- Blue-Bump is a social engineering technique [47]. First, the attacker sends a file and gains the trust of the victim. Then the attacker persuades the victim to delete the link key that was established during the transaction by keeping the connection open. While the victim is unaware of the open connection, the attacker requests the victim to initiate another link-key. Now, the attacker device remains concealed in the paired list of the victim device and remains connected with the victim. To the victim the attacker device seems like a complete new device.

Distortion

Here, the attacker exploits the vulnerability of BLE protocol services like GATT, L2CAP (Logical Link Control and Adaptation Layer Protocol) or BLE data packets and tries to disrupt the services of the BLE devices.

- Fuzzing : Fuzzing involves writing invalid values to characteristics [24]. Characteristics are data fields which hold atomic values. As a consequence of fuzzing, the BLE server can start behaving abnormally, and in severe cases, it can even lead to the crashing of the GATT server. Prior to commencing the attack, a comprehensive understanding of the characteristics present in the victim's GATT server is required. This can be easily done by an active scan, but once the characteristic handle is obtained and is writable, then the attacker can write random values to it.
- Blue Smack : Both Bluetooth classic and BLE use L2CAP for data transmission services. In this attack, the attacker targets L2CAP protocol and disrupts its services. This is also known as the ping of death attack [25].

Surveillance

Due to the architectural design issues of the protocol and lack of proper security enforcement, attackers can gather information about a person's identity as well as personal data.

- Fingerprinting : Device fingerprinting is a technique of identifying a device uniquely using different device-specific features, such as MAC Addresses, Universal Unique Identifier (UUID), advertisement packets, GATT services, etc. [26].
- Blue Printing : Blue Printing is a technique to collect detailed information, such as device model, manufacturer, International Mobile Equipment Identity (IMEI), and software versions. It is not a severe attack, but it results in privacy leakage issues, as shown in [27].
- Blue-stumbling : It is the method of randomly searching for Bluetooth devices to find suitable targets to attack. It is mostly done in crowded places where a large number of Bluetooth devices are available. In this case, attackers mainly search for victims, marking the devices with more security flaws that could be potentially be exploited. This process, even though does not cause any harm to the victims directly, serves as the initial step to initiate an attack [36].
- Blue-Tracking is the method of tracing the location of a victim by following the signal of their Bluetooth Device. It is not meant to steal information from the victim. The attacker has no access to any content of the victim device [28].

IV. Challenges and Countermeasures

The Sweyn-Tooth vulnerabilities [31], one of the most recent sets of vulnerabilities, have the potential to affect devices using the BLE protocol. The vulnerabilities expose flaws in particular BLE SoC implementations, which enable an attacker within radio range to initiate deadlocks, crashes, buffer overflows, or completely bypass security.

One of the earliest works showing the vulnerabilities of medical devices is the seminal study by Halperinet al. [32], which introduced attacks on an Implantable Cardiac Defibrillator (ICD), compromising the confidentiality, integrity, and availability of the device. Similar attacks were also later shown in insulin pumps [33], Fitbit trackers [34], medical infusion pumps [35]. Several studies have also explored information disclosure vulnerabilities in Bluetooth-enabled wearable devices [36].

A proof-of-concept attack, executed by experts at Bitdefender [46], targeted a Samsung smartwatch that was paired with a Google Nexus smartphone. Exploiting sniffing tools, researchers were able to uncover the PIN used to protect the smartwatch and the smartphone connection. In this case, an attacker could easily perform a brute-force attack on the PIN, as the "key space" is composed of only 1 million possible key combinations. The vulnerability is in the Link Manager Protocol and can be remediated by the manufacturer by requiring a password for Bluetooth pairing, as well as implementing encryption for the data communication.

 ISBN: 978-1-68558-113-8

Concerning BLE fitness bands [40] and health devices [34], it has been shown that an attacker can very easily access a lot of personal data, read the various health sensor data [41] or even guess what the user is typing by analyzing the motion sensors data from wearable wrist devices [42].

Glucose monitors can be connected to companion smart apps on smartphones, which not only capture data, but also send alerts to patients. The technology can be exploited by individuals in close range, and MiTM and eavesdropping attacks can be executed [43]. During these attacks, data being communicated between the devices could be intercepted, decrypted, and captured.

A. Mitigation strategies

Given the open nature of wireless technologies, preventing all attacks and guaranteeing security is a very challenging task, however, there are several countermeasures that can be applied to provide a reasonable security level.

Several mitigation strategies designed specifically for BLE applications have been proposed over the years. Notably, in reference to [37], the authors present various sets of rules for users to help them perform actions safely, thereby minimizing the susceptibility to potential attacks. They describe how to use your BLE devices in your environment as well as underscore the significance of regularly updating the firmware of such devices. Of particular importance is the usage of a lengthy PIN during the authentication phase when establishing connections with other devices. Ensuring that this PIN is not only lengthy but also randomly generated enhances its resilience against brute-force attacks, akin to the practice employed in altering phone passwords, as also mentioned in [14]. The authors also suggest the adoption of link encryption for all data transmissions as a means to prevent eavesdropping, while the utilization of the maximum encryption key size is emphasized to fortify protection against brute-force attacks.

In recent times, there has been a notable emergence of BLE security testing frameworks aimed at evaluating the security of applications. One such framework, as described in [24], encompasses various software components designed to carry out attacks like MiTM, DoS by flooding, and fuzzing. The principal objective of this particular BLE security testing framework is to present an integrated approach for assessing the security of BLE networks through the execution of multiple attacks on the network and its associated devices.

Additionally, [38] introduces an innovative framework, known as MARC, which is specifically tailored to identifying MiTM attacks in HealthCare BLE systems. The primary purpose of this framework is to detect, analyze, and mitigate Bluetooth security vulnerabilities, with a specific focus on MiTM attacks targeting NiNo devices. To achieve this, a comprehensive solution has been proposed which utilizes four novel anomaly detection metrics for detecting MiTM signatures. These metrics involve the analysis of malicious scan requests, advertisement intervals, Received Signal Strength Indicator (RSSI) levels, and cloned node addresses.

The authors in [39] present an automated security assessment framework designed specifically for Wearable BLE-enabled Health Monitoring Devices. This framework encompasses four distinct stages, beginning with the initial phase of information gathering. During this stage, the focus is on identifying the assets, their interactions, and comprehending the overall system workflow. Subsequently, the threat modelling phase is executed, followed by a thorough vulnerability analysis, and ultimately, the exploitation phase.

The efficiency of this framework has been empirically evaluated by conducting tests on a variety of medical devices, such as the Athos Smart Apparel. This particular wearable system seamlessly integrates surface electromyography (sEMG) technology, Smart Fitness Trackers, and Electrocardiogram (ECG) trackers. The outcomes of these assessments have revealed interesting findings, underscoring the framework's value in enhancing the security posture of such health monitoring devices.

V. Conclusion

Maintaining a balance between security and design goals remains a challenging task and requires closer collaboration between manufacturers, security researchers, and clinicians. As the popularity of Bluetooth continues to grow and it is incorporated into more aspects of everyday life, it's very important that users understand the risks involved with using Bluetooth. Even more important is that they work to mitigate those risks by following the recommended security guidelines.

Both academia and industry researchers and practitioners are presently collaborating to address certain open research challenges aiming to enhance the performance of BLE, like the improvement and design of the physical layer, specifically the radio or PHY mode introduced in BLE v5.x. [44]. Additionally, the investigation of adaptive parameter settings [48] and the utilization of random back-off mechanisms to retry channel sensing for more efficient device discovery appears to be quite promising in identifying devices within crowded environments. Finally, research topics such as the role switching between central and peripheral devices based on events, the coexistence of BLE with other wireless technologies, as well as adaptive frequency hopping techniques to avoid interference, are expected to enrich our understanding, inform practical applications, and stimulate further research.

Acknowledgment

This research has been co-financed by the European Regional Development Fund of the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH – CREATE - INNOVATE (project code:T2EDK-03093)

References

[1] R. Horton, "What We Can Learn From Bluetooth Medical Device Recalls," orthogonal.io/bluetooth [retrieved: August, 2023]

[2] P. A. Williams and A. J. Woodward, “Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem,” Med Devices (Auckl), vol. 8, pp. 305—316, 20 Jul 2015. Doi: https://doi.org/10.2147/MDER.S50048

[3] ”Medical devices market”, www.fortunebusinessinsights.com [retrieved: August, 2023]

[4] ”How bluetooth technology is enabling safe return strategies in a COVID-19 era”, www.bluetooth.com [retrieved: August, 2023]

[5] K. Zetter, ”It is insanely easy to hack hospital equipment”. Available online: www.wired.com [retrieved: August, 2023]

[6] M. Kijewski, ”Medical devices most vulnerable to hackers”. Available online: www.medtechintelligence.com [retrieved: August, 2023]

[7] P. Paganini, Smartwatch Hacked, ”How to access data exchanged with smartphone”. Available online: www.securityaffairs.com [retrieved: August, 2023]

[8] T. Melamed, “An active man-in-the-middle attack on bluetooth smart devices”. International Journal of Safety and Security Engineering, vol. 8, pp. 200-211, 2018. Doi: https://doi.org/10.2495/SAFE-V8-N2-200-211

[9] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, ”Security vulnerabilities in bluetooth technology as used in IoT,” J. Sens Actuator Netw, 2018. Doi: https://doi.org/10.3390/jsan7030028

[10] ”Bluetooth Low Energy A Complete Guide”, www.novelbits.io [retrieved: August, 2023]

[11] A. Barua, M. A. Al Alamin, M. S. Hossain and E. Hossain, ”Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey,” in IEEE Open Journal of the Communications Society, vol. 3, pp. 251-281, 2022, doi: 10.1109/OJCOMS.2022.3149732

[12] W. Saltzstein, “Bluetooth wireless technology cybersecurity and diabetes technology devices,” Journal of Diabetes Science and Technology, vol. 14, no. 6, pp. 1111-1115, 2020. Doi: 10.1177/1932296819864416

[13] M. Cäsar, T. Pawelke, J. Steffan, and G. Terhorst, “A survey on bluetooth low energy security and privacy,” Computer Networks, vol. 205, p. 108712, 2022. Doi: https://doi.org/10.1016/j.comnet.2021.108712

[14] P. Cope, J. Campbell, and T. Hayajneh, “An investigation of bluetooth security vulnerabilities,” IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 1-7, 2017. Doi: 10.1109/CCWC.2017.7868416

[15] F.R. Maruf and A. Nasr, “Eavesdropping in bluetooth networks,” International Journal of Current Engineering and Technology.www.researchgate.net [retrieved: August, 2023]

[16] S. Jasek, ”GATTacking bluetooth smart devices,” Tech. rep., SecuRing, p. 15, www.paper.bobylive.com [retrieved: August, 2023]

[17] Gattacker, ”A Node.js package for BLE (Bluetooth Low Energy) Man-in-the-Middle & more”. www.github.com/gattacker [retrieved: August, 2023]

[18] G. Kwon, J. Kim, J. Noh, and S. Cho, “Bluetooth low energy security vulnerability and improvement method,” IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Seoul, Korea (South), pp. 1-4, 2016. Doi: 10.1109/ICCE-Asia.2016.7804832

[19] Rosa, ”Bypassing passkey authentication in Bluetooth low energy”, 2013, www.eprint.iacr.org [retrieved: August, 2023]

[20] C. Gomez, J. Oller, and J. Paradells, ”Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology Sensors,” Sensors 12, no. 9, pp. 11734-11753, 2012 Doi: https://doi.org/10.3390/s120911734

[21] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, “Denial-of-service attacks on battery-powered mobile computers,” Second IEEE Annual Conference on Pervasive Computing and Communications, pp. 309-318, 2004. Doi: 10.1109/PERCOM.2004.1276868

[22] J. Uher, R. G. Mennecke and B. S. Farroha, “Denial of Sleep attacks in Bluetooth Low Energy wireless sensor networks,” MILCOM IEEE Military Communications Conference, Baltimore, MD, USA, pp. 1231-1236, 2016, Doi: 10.1109/MILCOM.2016.7795499

[23] D. Cauquil, “You’d better secure your BLE devices, or we’ll kick your butts!,” www.virtuallabs.fr [retrieved: August, 2023]

[24] A. Ray, V. Raj, M. Oriol, A. Monot and S. Obermeier, “Bluetooth Low Energy Devices Security Testing Framework,” IEEE 11th International Conference on Software Testing, Verification and Validation (ICST), Västerås, Sweden, pp. 384-393, 2018. doi: 10.1109/ICST.2018.00045

[25] R. Nasim, ”Security threats analysis in bluetooth-enabled mobile devices”. arXiv:1206.1482

[26] C. Zuo, H. Wen, Z. Lin, and Y. Zhang, “Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps,” in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 1469–1483, 2019. Doi: https://doi.org/10.1145/3319535.3354240

[27] C. Herfurt, C. Martin and C. Mulliner, ”Remote Device Identification based on Bluetooth Fingerprinting Techniques”.www.researchgate.net [retrieved: August, 2023]

[28] P. Lloyd, ”Blue Tracking”. www.scribd.com/Blue-Tracking. [retrieved: August, 2023]

[29] T. Claverie and J. L. Esteves, ”BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols,” 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2021, pp. 339-351, Doi: 10.1109/SPW53761.2021.00054

[30] BLURtooth: “Exploiting cross-transport key derivation in Bluetooth Classic and Bluetooth Low Energy”, arXiv:2009.11776

[31] Swentooth, Unleashing Mayhem over Bluetooth Low Energy, www.github.com/sweyntooth [retrieved: August, 2023]

[32] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, ”Security and privacy for implantable medical devices,” in IEEE Pervasive Computing, vol. 7, no. 1, pp. 30-39, 2008. Doi : 10.1109/MPRV.2008.16

[33] J. Radcliffe, “Hacking medical devices for fun and insulin: Breaking the human SCADA system,” in Black Hat Conference Presentation Slides. www.media.blackhat.com [retrieved: August, 2023]

[34] M. Rahman, B. Carbunar, and M. Banik, ”Fit and vulnerable: Attacks and defenses for a health monitoring device,” in Proceedings of the 6th Workshop on Hot Topics in Privacy Enhancing Technologies. arXiv 2013, arXiv:1304.5672

[35] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, ”This ain’t your dose: Sensor spoofing attack on medical infusion pump,” in Proceedings of the 10th USENIX Workshop on Offensive Technologies.www.usenix.org/ [retrieved: August, 2023]

[36] S. S. Hassan, S. D. Bibon, M. S. Hossain, and M. Atiquzzaman, ”Security threats in bluetooth technology,” Comput. Secur. pp. 308–322, 2018. Doi: 10.1016/j.cose.2017.03.008

[37] S. Shrestha, E. Irby, R. Thapa, and S. Das, “A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures,” in Computer and Information Science, vol. 1403, pp. 108–127, 2022. Doi: https://doi.org/10.1007/978-3-030-93956-4_7

[38] M. Yaseen et al. “A Novel Framework for Detecting MiTM Attacks in eHealthcare BLE Systems,” Journal of Medical Systems vol. 43, p. 324, 2019. Doi: https://doi.org/10.1007/s10916-019-1440-0

[39] G. A. Zendehdel, R. Kaur, I. Chopra, N. Stakhanova, and E. Scheme, ”Automated Security Assessment Framework for Wearable BLE-enabled Health Monitoring Devices,” ACM Trans. Internet Technol, vol. 22, no. 14, pp. 1-31, 2021. Doi: https://doi.org/10.1145/3448649

[40] W. Zhou and S. Piramuthu, “Security/privacy of wearable fitness tracking IoT devices,” Proc. 9th Iberian Conf. Inf. Syst. Technol. (CISTI), pp. 1-5, 2014. Doi: 10.1109/CISTI.2014.6877073

[41] O. Arias, J. Wurm, K. Hoang and Y. Jin, ”Privacy and security in Internet of Things and wearable devices,” IEEE Trans. Multi-Scale Comput. Syst., vol. 1, no. 2, pp. 99-109, 2015. Doi: 10.1109/TMSCS.2015.2498605

[42] H. Wang, T. T.-T. Lai and R. R. Choudhury, “MoLe: Motion leaks through smartwatch sensors,” Proc. 21st Annu. Int. Conf. Mobile Comput. Netw., pp. 155-166, 2015. Doi: https://doi.org/10.1145/2789168.2790121

[43] M. Kijewski, ”The Medical Devices Most Vulnerable to Hackers”. www.medtechintelligence.com [retrieved: August, 2023]

[44] J. Seo, K. Cho, W. Cho, G. Park, and K. Han, “A discovery scheme based on carrier sensing in self-organizing Bluetooth Low Energy networks,” Journal of Network and Computer Applications, vol. 65, pp. 72-83, 2016. Doi: https://doi.org/10.1016/j.jnca.2015.09.015

[45] J. Yang, C. Poellabauer, P. Mitra, and C. Neubecker, ”Emerging applications and challenges of BLE,” vol. 97, 2020. Doi: https://doi.org/10.1016/j.adhoc.2019.102015

[46] ”PoC hack on data sent between phones and smartwatches”,www.arstechnica.com [retrieved: August, 2023]

[47] ”BlueBump Attack”,bluebump-attack [retrieved: August, 2023]

[48] E. Park, M. S. Lee, H. S. Kim, and S. Bahk, ”AdaptaBLE: Adaptive control of data rate, transmission power, and connection interval in bluetooth low energy,” Computer Networks, vol. 181, 2020. Doi: https://doi.org/10.1016/j.comnet.2020.107520

 ISBN: 978-1-68558-113-8