International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A Study On The Privacy And Security Of Bluetooth Low Energy

Reetu Kumari Assistant Professor
Kalpna Chawala College of Educationfor Women
Hissar ,Haryana Pincode-125001

Abstract

When we say "device filtering," we're referring to a set of regulations intended to stop unwanted interaction. The energy savings achieved by using this technique are substantial. There are three broad types of filtering policies: those that target advertisers, those that target scanners, and those that target the user who makes the first connection. Various pre-connection statuses are affected by these rules, as the name suggests. When the policies are in place, a gadget may be able to lower its reaction time by tuning out the overwhelming majority of its contemporaries. This might be accomplished by having the device maintain a white list of known and safe addresses and content types. Advertisers, as an example, would be required to respond to a scan/connection request in accordance with the advertiser's advertising filter policy. When specific rules from an advertisement filter are active, devices may only allow scan/connection requests from whitelisted sources. A secondary objective of directed connectible advertisements is to protect the device's privacy and prevent unwanted scan or connection requests. These ads stand out from the others because they provide an RPA specifically tailored to the device being advertised to. If you enable this kind of marketing, your device will share information with just the persons with whom it intends to interact. Over the next several years, Bluetooth low energy (BLE) is expected to see a dramatic rise in its number of applications. Also, it serves as a magnet for would-be attackers. Because of this, BLE's security will be paramount. Over time, Bluetooth's security framework has improved. While Bluetooth is now a secure technology, that wasn't always the case. It is readily falsified and can only offer little security for the confidentiality of transmitted messages. To address this issue, the Secure Simple Pairing (SSP) protocol was developed following Version 2.1 + EDR. Because of this, Bluetooth's already impressive level of security got a big boost. In addition to these improvements, this version provides four association models that are used by a greater proportion of users. These models are as follows: Just Works, Numeric Comparison, Passkey Entry,

and Out-of-Band (OOB). The Bluetooth Special Interest Group (also known as Bluetooth SIG) placed a significant emphasis on the Low Energy security model throughout the whole of the development process for Bluetooth 4.0. However, as of right now, there are just three distinct kinds of association models (Just Works, Passkey Entry, and Out-Of-Band). Even though they are known by the same appellation as SSP, the degree of security that is given by them is far greater than that supplied by SSP. This discovery is a direct consequence of the fact that many common association models have been shown to be worthless when put into practise. In accordance with the declaration that was made by the Bluetooth Special Interest Group (SIG), version 4.1 of the Bluetooth standard includes support for the P-256 elliptic curve in addition to device authentication procedures that have been authorised by FIPS (also known as the Secure Connections feature). They assured that the information that was supplied could not be obtained by any third party by encrypting the data using the tried-and-true AES-CCM technique. This prevented any unauthorised parties from accessing the information. The protections that are now in place have not been modified in a way that would make them much more suited for the Low Energy version of the software. It is generally agreed upon by all parties involved that the significant advancement in the development of the technology represented by the enhancements to Bluetooth Low Energy's (BLE) security that were implemented in version 4.2 represents a major step forward in the development of the technology. The Secure Connections feature is an upgrade to the Low Energy protocol that integrates elliptic curve algorithms into the standard pairing procedure. The algorithms AES-CMAC and P-256 are two good examples of this kind. The Low Energy protocol was expanded to include Secure Connections. As a result of this, as we were designing Secure Connections, we kept in mind the Numeric Comparison association model as we were working on it. At the end of the day, it made use of the key-generation tools that are accessible inside Secure Connections.

Keywords: Bluetooth, *device filtering*, BLE, BR/EDR, Randomized Addresses Secure Bluetooth Devices

International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Introduction

In the 2010s, the Bluetooth Low Energy (Bluetooth LE) standard was established to improve upon the previous Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) protocol Bluetooth Low Energy (LE) devices offer a greater potential for power savings during their low-energy sleep phase since they can establish connections more rapidly and have shorter connection intervals. Low-power Bluetooth has the potential to reduce costs and space by allowing our devices to run for longer on a single charge. As a result, you may utilise a BLE-enabled gadget in a wide variety of settings, from the medical to the sports to the journalistic to the industrial. The transmission of Bluetooth Low Energy (BLE) is not compatible with that of Bluetooth Rev. 2 (BR/EDR), yet the two protocols may coexist on the same device and use the same radio for physical signalling since they adhere to different standards. This is because BLE is a low-power variant of Bluetooth that may be used over longer periods of time. Both data and sound may be sent over Bluetooth here. The BR/EDR mode of Bluetooth is used to send high-throughput audio streams (like a phone call or music stream), while the traditional Bluetooth standard is used to transmit all other communication data

Bluetooth Versions

There have been five significant Bluetooth releases, all from Bluetooth SIG. All the versions are compatible with the previous ones. The following are some of the main differences between the two versions:In May of 1998, Bluetooth protocol version 1.x became available. It was commonplace not so long ago but is no longer utilised. It's not great since its top speed is just 1 Mbit/s and it has weak pairing security. As of 2005, Bluetooth 2.0 was also available to the public. Because of its simplicity, it quickly gained traction within the featured phone market.You may send and receive data at speeds of up to 3 Mbit/s. The Bluetooth 3.x Specification was officially accepted by the Bluetooth Special Interest Group in April 2009. It is far quicker than its predecessors, being able to transport data at up to 24 Mbit/s. However, higher speeds cost more to sustain since they need more energy. Bluetooth 4.x, which was released in June of 2010, is where you'll find the most interesting Low Energy (LE) features. This is why Bluetooth Low Energy (BLE) is ideal for low-power IoT devices that nevertheless need to communicate with one another. It can connect devices up to 100 yards apart at far higher speeds and greater

distances than its predecessors. Indirect communication between Internet of Things devices is possible thanks to Bluetooth 4.1. Until recently, BLE IoT devices required a mobile phone connection to access the internet. Bluetooth 4.2 addresses this issue by incorporating an IPv6 layer into the BLE protocol stack. Consequently, the BLE protocol may provide the foundation for IPv6 communication between IoT devices. Fifth, the 2016 introduction of Bluetooth 5.x represents a significant improvement over earlier versions in terms of both speed and range. Check see Section VIII-A for a detailed discussion of the changes.

Classic Bluetooth vs. BLE

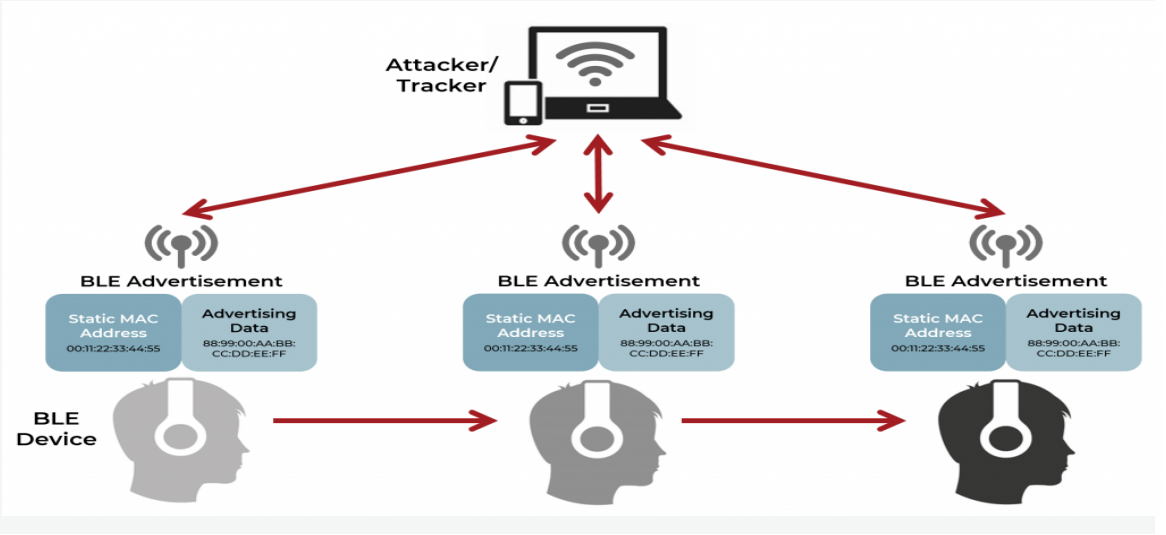
The original Bluetooth, and its successor, Bluetooth Smart, were both created with a wide range of uses in mind. Technical requirements, designs, implementations, and reported use cases are some areas where classic Bluetooth and BLE diverge. If traditional Bluetooth excels at managing large data volumes, then Bluetooth Low Energy shines in its efficiency during frequent data transfers. Which of the two options is preferable depends on the user's needs and the device's capabilities. Both regular Bluetooth and BLE use the same radio frequency range, although they use different numbers of channels. While standard Bluetooth is great for long-distance wireless communications, BLE is superior for short-distance connections due to its much lower power consumption. Due to the trade-off between data transmission rate and power consumption, BLE must reduce throughput to maintain a negligible energy footprint. However, the data rate and energy consumption of classic Bluetooth are both much higher.

Security Concerns with Bluetooth LE

BLE devices constantly "promote" themselves by broadcasting the same signals to a large number of receivers, while BR/EDR devices only "market" themselves sometimes. It is via this method that a BLE device announces its existence to other BLE devices in the vicinity. The BLE advertising data may include information on the device's manufacturer, model, and maybe even its features and specifications. The content of a

International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

BLE ad is used to determine whether or not a scanner will establish a connection with an advertising device. Among the most important aspects of a BLE advertisement is the advertised URL. The target audience member may then become aware of the ad platform and decide to interact with it. The Media Access Control (MAC) address is a 6-byte number used for networking in the same fashion as Ethernet. The owner's location may be determined by analysing the signal intensity of the always-on advertising signal in conjunction with the device's fixed MAC address.



The tracking of Bluetooth Low Energy devices through the use of static MAC address advertising

Randomized Addresses Secure Bluetooth Devices

To avoid being tracked, users of devices compliant with the BLE standard may use a Resolvable Random Private Address (RPA or RRA) as an advertising address instead of the device's Media Access Control (MAC) address (Figure). The generated random address might then be changed sporadically to elude detection. In most cases, the length of time needed to regenerate random IDs is defined by the device itself.Bluetooth Low Energy (BLE) advertising can be picked up by any device, thus it can't be used to spy on individuals. It has been shown that some of these data may still be utilised for tracking even with an RPA in place. Ad content and refresh rates need significant consideration from BLE product developers.

International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

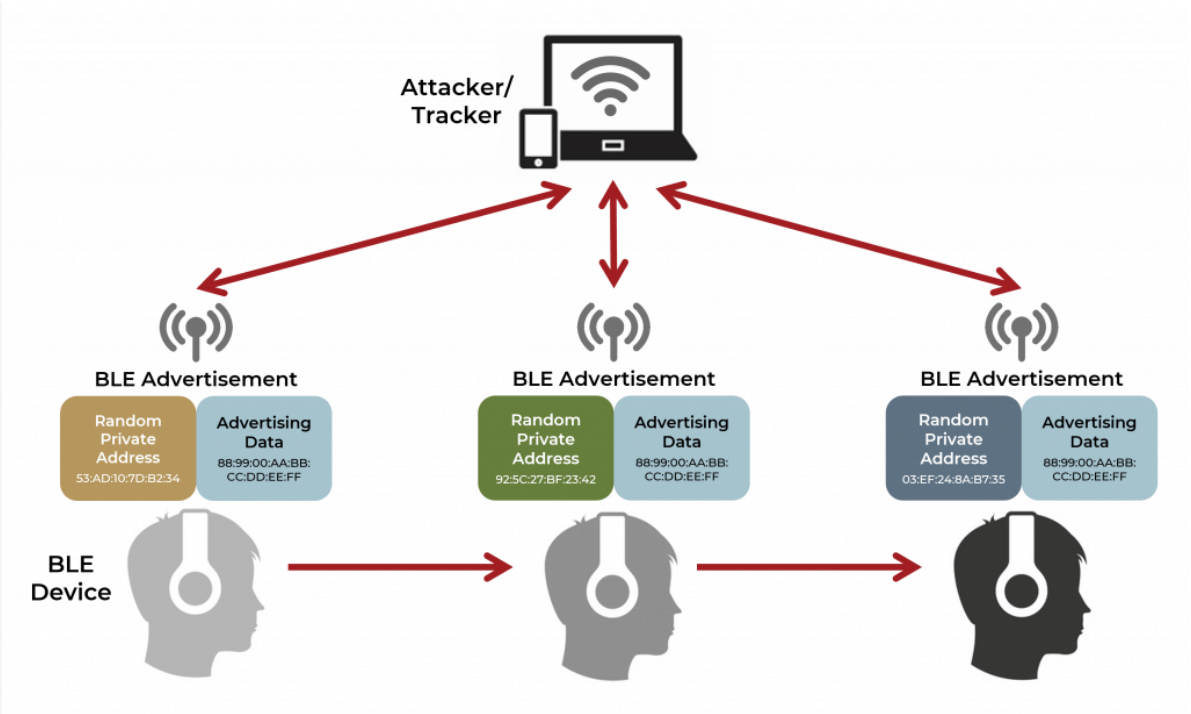


Figure : BLE device tracking protection using a Random Private Address.

Developing BLE Products That Make Use Of Randomized Addresses While Still Keeping Connectivity With Trusted Devices

How can previously connected devices determine the identity of the advertising device if the advertising device is continually changing the advertisement address in its BLE advertisements? The solution lies in strong bonds and mutual trust established between partners. As a first step, two Bluetooth Low Energy (BLE) devices establish an encrypted connection by mutually authenticating each other. As a result, devices may encrypt their communications by exchanging long-term keys (LTKs), which are established using temporary encryption keys (Figure)

International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

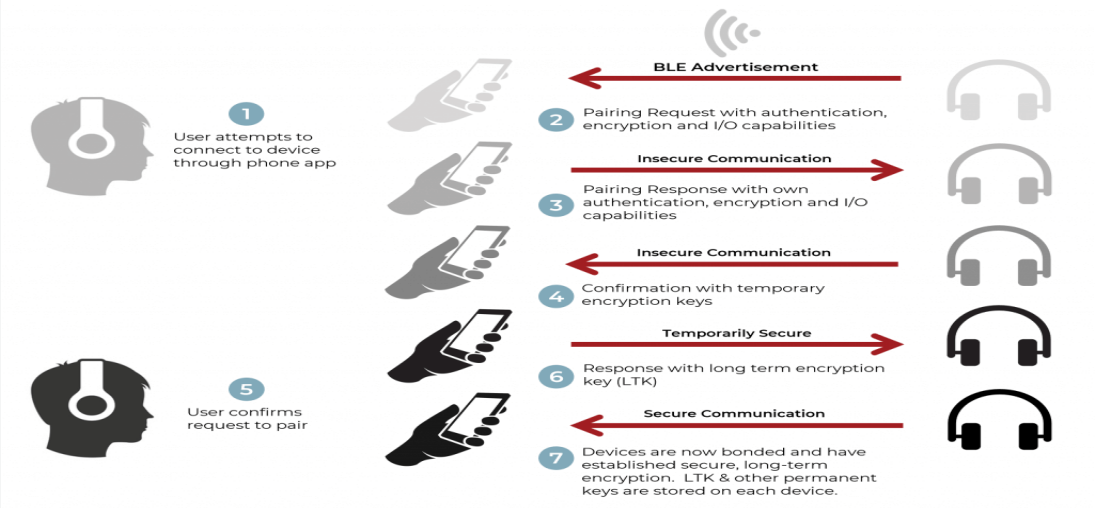
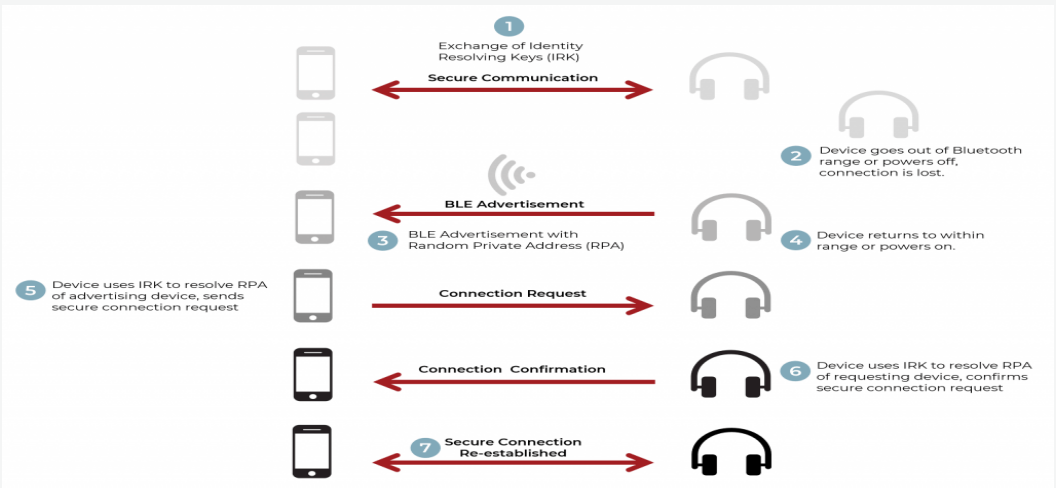


Figure:Bonding to establish a safe Bluetooth Low Energy connection. This allows for permanent encryption by exchanging a long-lived key (LTK). Bonding is the process through which two BLE devices share and store encryption keys. Devices also communicate an identity resolving key in addition to the LTK (IRK). When a BLE device comes back into range or when the random private address changes, the IRK is utilised to verify the connection (Figure). This enables trustworthy devices to stay connected via randomised address updates, while preventing tracking by unknown devices.



Secure identity-based communications over Bluetooth Low Energy by exchanging and storing a shared key (IRK). The IRK is used for device authentication whenever a BLE connection is re-established. The BLE advertisement address is 48 bits long, the same length as a MAC address (six bytes). In lieu of a typical media access control (MAC)

International Journal of Management, IT & Engineering
Vol. 8 Issue 9, September 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

address, the RPA enables a device to transmit a 22-bit random number (prand), a 24-bit hash value, and two fixed bits (Figure). Devices having RPAs may use a known encryption technique to decrypt a padded 128-bit prand (using the 2 fixed bits) and a 128-bit IRK, allowing them to validate the identification of other devices. After the address has been rectified, the verification of the device's identification is regarded as having been a fruitful endeavour. This may be accomplished by comparing the hash value that was derived from the address field of the advertising with the result of the encryption algorithm, the bit length of which has been reduced to 24 in order to accommodate the comparison. After that moment, the two devices will be able to go on with the process of sharing information with one another that is both encrypted and kept confidential.

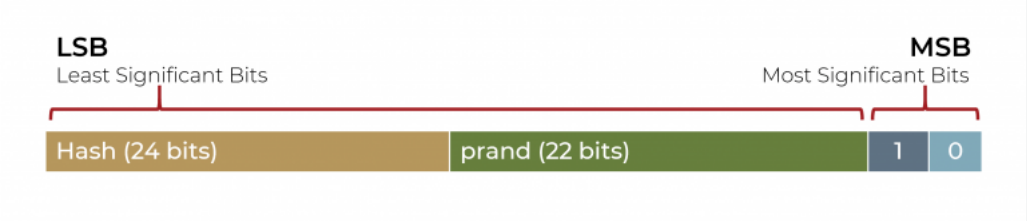


Figure : Using a Resolvable Private Address in BLE

As a result of their inexpensive price and tiny size, Bluetooth Low Energy gadgets have quickly gained in popularity. Instead of using static addresses, BLE advertisements may now utilise dynamic, randomly resolvable addresses, which safeguard users from invasive identity monitoring while still allowing trustworthy devices to communicate securely. People all throughout the globe who utilise wireless devices that support Bluetooth Low Energy may rest easy with this addition.

Conclusion

In this survey, we take a look at the security and privacy of Bluetooth Low Energy (BLE), including possible dangers and countermeasures. We recommend upgrading to BLE 4.2 or 5 due to security issues in BLE 4 and 4.1. A man-in-the-middle attack may be performed on any implementation of the BLE Just Works pairing method. Don't use it if you can help it. Since Just Works may be the only viable choice due to price and

usability constraints, it is highly recommended that encryption and authentication be implemented on an application-by-application basis.

References

1. Cross D, Hoeckle J, Lavine M, Rubin J, Snow K (2007) Detecting non-discoverable bluetooth devices. In: International conference on critical infrastructure protection. Springer, pp 281–293
2. Cyr B, Horn W, Miao D, Specter M (2014) Security analysis of wearable fitness devices (fitbit). Massachusetts Institute of Technology, p 1
3. Dunning J (2010) Taming the blue beast: a survey of Bluetooth based threats. IEEE Secur Priv 8(2):20–27
4. Gomez C, Oller J, Paradells J (2012) Overview and evaluation of Bluetooth low energy: an emerging low-power wireless technology. Sensors 12(9):11734–11753
5. Haataja KM, Hypponen K (2008) Man-in-the-middle attacks on Bluetooth: a comparative analysis, a novel attack, and countermeasures. In: 3rd international symposium on communications, control and signal processing, 2008. ISCCSP 2008. IEEE, pp 1096–1102
6. Sullivan H (2015) Security vulnerabilities of Bluetooth low energy technology (BLE). Tufts University
7. Townsend K, Cufí C, Davidson R, Davidson A (2014) Getting started with Bluetooth low energy. O'Reilly Media, Inc.
8. Uher J, Mennecke RG, Farroha BS (2016) Denial of sleep attacks in Bluetooth low energy wireless sensor networks. In: Military communications conference, MILCOM 2016-2016 IEEE. IEEE, pp 1231–1236
9. Wei X, Li Z, Chen Z, Yuan Z (2008) Commwarrior worm propagation model for smart phone networks. J China Univ Posts Telecommun 15(2):60–66
10. Whigu (2016) Change your Bluetooth device MACaddress. http://blog.petrilopia.net/linux/change-yourbluetooth-device-mac-address/.

11. Wireless World R (2016) Bluetooth vs BLE-difference between Bluetooth and BLE(bluetooth low energy). http://www.rfwireless-world.com/Terminology/Bluetooth-vs-BLE.html
12. Zegeye WK (2015) Exploiting Bluetooth low energy pairing vulnerability in telemedicine. In: International telemetering conference proceedings, international foundation for telemetering