Cybersecurity Analysis of Wearable Devices

Subjects: Computer Science, Information Systems

Contributor: Alejandra Guadalupe Silva-Trujillo , Mauricio Jacobo González González , Luis Pablo Rocha Pérez , Luis Javier García Villalba

Wearable devices are starting to gain popularity, which means that a large portion of the population is starting to acquire these products. This kind of technology comes with a lot of advantages, as it simplifies different tasks people do daily. However, as they recollect sensitive data, they are starting to be targets for cybercriminals. The number of attacks on wearable devices forces manufacturers to improve the security of these devices to protect them. Many vulnerabilities have appeared in communication protocols, specifically Bluetooth. A passive attack on six different smartwatches was performed to discover their vulnerabilities during the pairing process. Furthermore, a proposal of requirements was developed needed for maximum security of wearable devices, as well as the minimum requirements needed to have a secure pairing process between two devices via Bluetooth.

Bluetooth BLE cybersecurity secure connections sniffer wearable

1. Introduction

Internet of Things technologies are evolving and taking part in our daily routines without us even noticing [1]. The continuous growth and acceptance of these devices are going out of proportion, as the new normal shows a person owning multiple IoT devices. It is projected that by the year 2025, there will be over 75 billion connected devices [2]. Furthermore, just five years later, by 2030, it is expected that there will be 124 billion IoT devices [3].

IoT reaches different scopes; they can be medicine, education, industry, entertainment, sports, clothes, smart cities, agriculture, and many others. See **Figure 1**. Technology recollects a big amount of data, including personal information, routines, and health records, to simplify the diverse tasks that we accomplish daily. However, having that great collection of records could be counterproductive, if someone else uses it to gain something. This opens the door for cybercriminals, who understand the value of these types of sensitive data.

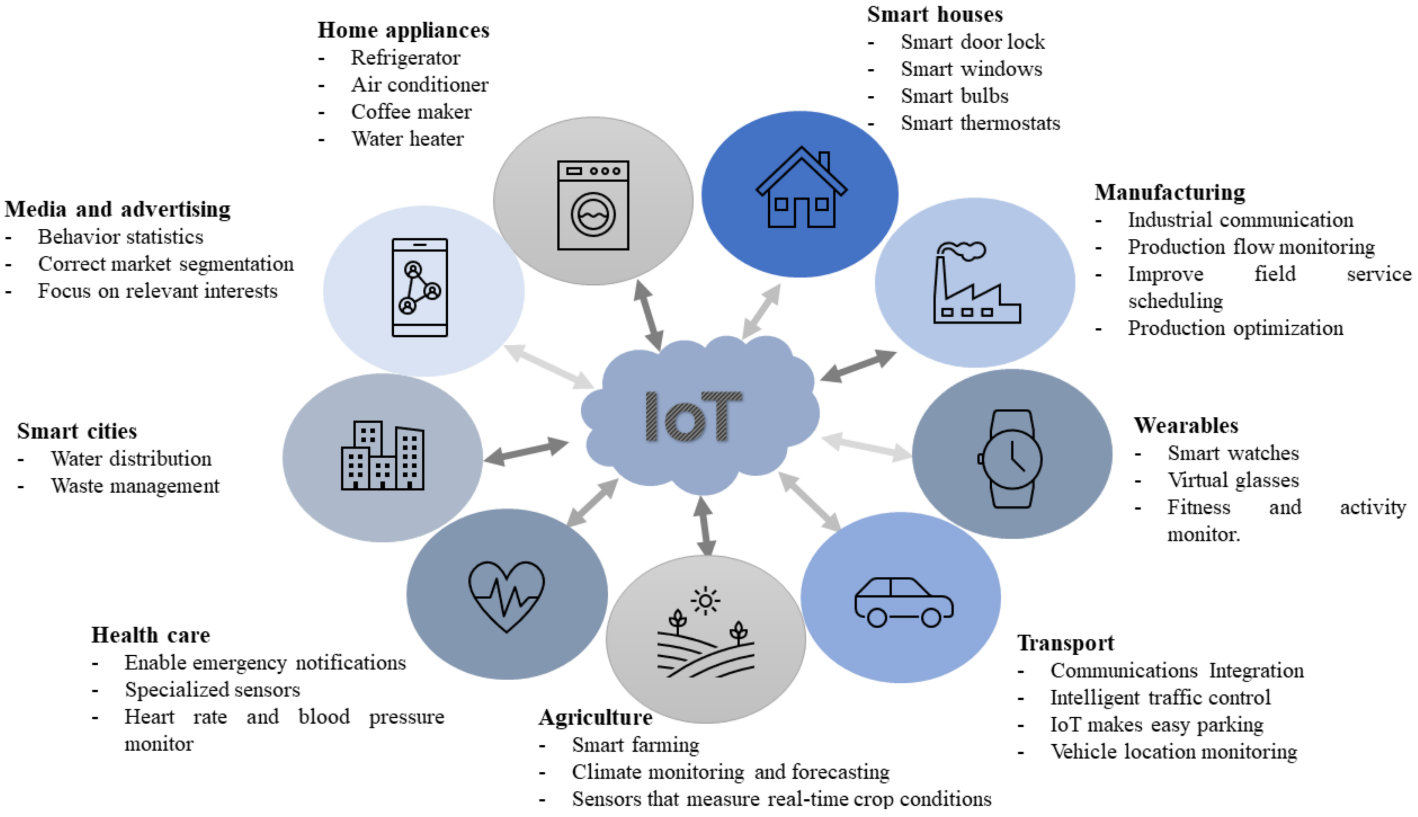
Home appliances
- Refrigerator
- Air conditioner
- Coffee maker
- Water heater
Smart houses
- Smart door lock
- Smart windows
- Smart bulbs
- Smart thermostats
Media and advertising
- Behavior statistics
- Correct market segmentation
- Focus on relevant interests
Manufacturing
- Industrial communication
- Production flow monitoring
- Improve field service scheduling
- Production optimization
IoT
Smart cities
- Water distribution
- Waste management
Wearables
- Smart watches
- Virtual glasses
- Fitness and activity monitor.
Health care
- Enable emergency notifications
- Specialized sensors
- Heart rate and blood pressure monitor
Agriculture
- Smart farming
- Climate monitoring and forecasting
- Sensors that measure real-time crop conditions
Transport
- Communications Integration
- Intelligent traffic control
- IoT makes easy parking
- Vehicle location monitoring

Figure 1. IoT Application Areas.

IoT device cyberattacks are deemed to be of high risk, particularly when handling people's health data, as they can lead to physical harm and endanger lives. Vulnerabilities not only impact device functionality, but also people's health [4]. These devices are anticipated to have high demand in the market, and manufacturers strive to optimize their components for cost reduction and focus on providing minimum functionality, disregarding fundamental security needs. Furthermore, a considerable number of device manufacturers do not provide software updates or security patches to mitigate or prevent damage after an attack.

2. IoT Vulnerabilities and Challenges

The literature shows multiple concerns already found in different IoT devices [5]. Now, to understand how big these concerns are, vulnerabilities must be covered due to the increasing use of this kind of technology and the sensitive information they gather. A key is to maintain confidentiality, integrity, and availability, also known as the CIA triad; this represents a fundamental concept in cybersecurity. There has been a lot of research, and the most common types of attacks that have been made on IoT devices can be seen in the systematic review in **Table 1**.

Table 1. Systematic Review: IoT Attacks.

IoT Attacks	Research			
	[6]	[7]	[8]	[9]
Eavesdropping	✓	✓		✓

IoT Attacks	Research			
	[6]	[7]	[8]	[9]
Traffic Analysis	✓	✓		✓
Information Gathering	✓			
Modification	✓		✓	✓
Masquerade	✓			
Denial of Service	✓	✓	✓	✓
Replay	✓	✓		✓
Based on Network Properties		✓	✓	✓
Malevolent Code				✓
Phishing				✓

The large number of attacks that exist on IoT devices gives us an idea of the importance of establishing security countermeasures against these threats [8]. The consequences that they can have on a person's lifestyle and health could be devastating. Devices' sensitive data could be at risk with a technique in which data is being sent through devices and because they have poor authentication methods for devices that handle such an important type of data, raising question marks about confidentiality.

Other types of attacks have the objective of changing data information, making the users' data that was recollected hard to trust. This way, it damages the integrity part of the IoT device. Several IoT devices are now used for medical purposes, recollecting real-time information. If they are not available at every moment of the day, not only are they not fulfilling their purpose, but they could be putting a user's life in danger by not registering, what might be, for some users, life and death cases.

As can be seen, the biggest fundamentals in cybersecurity have been exposed by these types of technologies. Correcting these problems would be the following step to take to guarantee confidentiality, integrity, and availability. However, numerous other issues appear when trying to apply new forms of security to IoT devices, as shown in **Table 2**.

Table 2. Systematic Review: Security Challenges.

Challenges	Research				
	[6]	[8]	[10]	[11]	[12]
Computational Limitations	✓	✓			
Memory Limitations		✓			
Energy Limitations	✓	✓	✓		

Challenges	Research				
	[6]	[8]	[10]	[11]	[12]
Mobility		✓	✓		
Scalability		✓		✓	
Communications Media		✓	✓	✓	
Multiplicity of Devices		✓			
Dynamic Network Topology	✓	✓			
Multi-protocol Network		✓			
Dynamic Security Updates		✓	✓		
Tamper-Resistant Packages		✓			
Design Constraints			✓		
Price				✓	✓

Bluetooth is everywhere: in speakers, headphones, refrigerators, cars, wearables, medical devices, and more. IoT is about small devices and multiple sensors. Bluetooth is a suitable technology that provides IoT features that can be applied to a wide range of potential IoT applications. Manufacturers need to understand how to implement secure architectures to protect users' sensitive information while considering the challenges and limitations of the IoT.

However, Bluetooth communication has been the target of multiple types of attacks for years as cybercriminals exploit the vulnerabilities this technology has had in earlier versions. These communication protocols have been updated to protect devices against eavesdropping and man-in-the-middle attacks.

The literature shows multiple researchers finding weaknesses in wearable devices [13][14][15][16]. They talk about different attacks on several IoT devices that communicate via Bluetooth, as well as they give countermeasures and recommendations to users for safer use of this technology. Furthermore, other research includes studies that found vulnerabilities in some devices [17]. One of them is an attack on a smartwatch, where the PIN that secures its communication with a smartphone was exploited while performing a brute-force attack. In the pairing process, this smartwatch had one of the least secure mechanisms, which shows that smartwatches are prone to attacks [18]. With respect to threats, one article divides them into two categories: passive adversary and active adversary, where the first, the attacker eavedrops on the connection and tries to find LTK or other information, but he can not manipulate the message, and in the second, the attacker can inject, modify, and block the message transmitted, enabling the ability to create his own messages and send them to the victim's device [19].

Other research focuses on wearable devices, such as a Fitbit smartwatch, and how they can be targets of man-in-the-middle attacks. The attack consists of using two fake devices, one that disguises itself as a smart device and another one as a mobile app that connects to the Fitbit device; it also adds that Fitbit collects a lot of sensitive data, and it proposes to educate the users to be aware of what happens when doing an incorrect use of the device [20]. Another research project highlights a couple of vulnerabilities in some wearable devices, such as the smartwatch Fitbit Inspire, which has a serious threat known as the Link Layer Length Overflow. It means that an attacker acting as a central device can make the peripheral devices suffer instabilities until they finally crash [21].

More studies have concluded that it is important to teach users about the correct use of this technology because most of the recommendations always go to the manufacturers. They propose some guidelines to instruct about wearable devices [22] and state the need for standards in the wearable industry [20].

Another piece of research worries about the data these devices obtain; for example, the users' location, which exposes them to different types of attacks. Furthermore, it proposes the constant change of the MAC address to avoid any type of targeting [23]. A group of researchers also mentions the vulnerabilities of the MAC address in Fitbit devices, as they recollect the MAC addresses of nearby Fitbit devices, and while Fitbit offers a reasonable level of security, they also gather extraneous data about users [24].

In one paper, they make passive attacks on wearable devices using Bluetooth sniffers and HCI snoop logs and capture an encryption key in plain text [25]. While another article shows the use of Bluetooth and describes an attack where it forces a key renegotiation using eavesdropping techniques [26]. Other works show the potential risks the devices are exposed to when manufacturers do not follow the recommendations of the Bluetooth Special Interest Group, as it happens more often than it should [27][28]. While various research projects include tests on different devices, the literature does not show a way to compare the security levels of these devices. There is no existence of measurement to identify when an IoT device is secure or what characteristics can be considered to categorize if an IoT device is safe or not.

3. Background: Bluetooth Technologies and Evolution

Bluetooth is used for short-range radio-frequency communication. As mentioned before, vulnerabilities can be found in IoT devices, and this could be discovered through the Bluetooth protocol. The most common attacks are man-in-the-middle (MITM), where an attacker can obtain the keys that are exchanged between devices and, once obtained, eavesdrop on communications [29].

The earliest days of Bluetooth introduced Bluetooth Basic Rate (BR), Enhanced Data Rate (EDR), and High Speed (HS) models. Bluetooth 1.1 and 1.2 versions could only work with BR because they are only capable of supporting up to 1 megabit per second (Mbps). EDR improves in Bluetooth version 2.0, where it gets data rates up to 3.0 Mbps. HS arrives during Bluetooth 3.0, supporting faster data rates up to 24 Mbps. However, devices that support higher data rates are also able to support lower data rates from earlier Bluetooth specifications. When referring to these versions of Bluetooth, they are commonly known as Bluetooth Classic. See **Figure 2**.

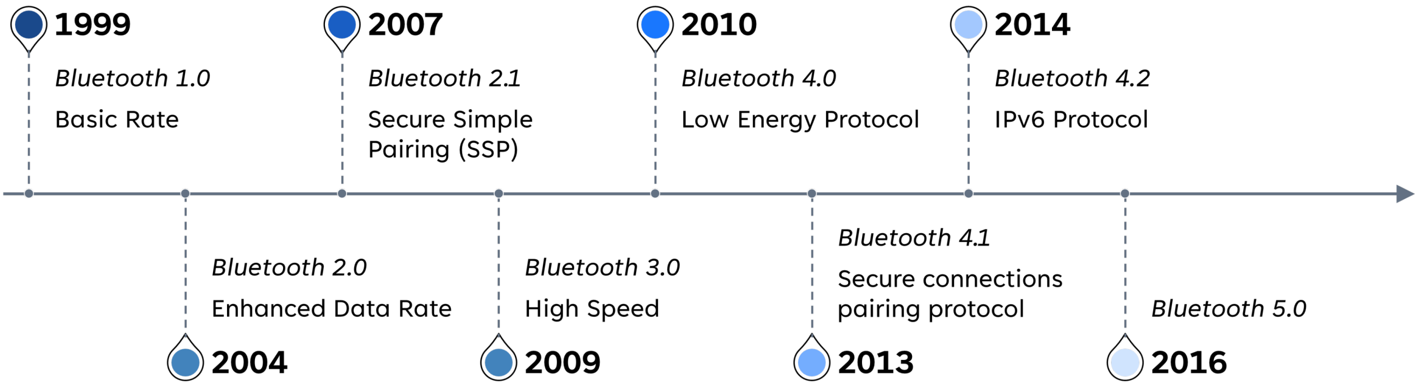

Figure 2. Bluetooth Technologies and Evolution.

Bluetooth Low-Energy (BLE) was established in the Bluetooth 4.0 specification; later, an update was made in versions 4.1 and 4.2. It is useful for wearable medical devices and sensors because it was primarily made for devices that use a coin-cell battery. It reduces power consumption and memory requirements. Basically, it is designed to operate in sleep mode and wake up only when the connection is initiated. This improves efficiency when discovering devices and during connection procedures and results in packets with shorter lengths, while services and protocols are simpler.

Since Bluetooth 4.0 devices can support both Bluetooth Classic and BLE, this is known as the dual mode. Cellphones work as a perfect example, where they might use Bluetooth Classic when connected to earphones and have the necessity to have constant data streaming while also using BLE when connected to a smart wristband that tracks your activity while doing exercises, and you only need the data exchange when you synchronize your devices to check your results.

Bluetooth has five basic security services:

(a) Authentication, using the Bluetooth address to verify the identity of each device during the communication stage.

(b) Confidentiality, guaranteeing that only authorized devices have access to data, avoiding any type of eavesdropping.

(c) Authorization, verifying that a device is authorized to use the service before allowing it to do it, guaranteeing that only this device can use the service and no other device can.

(d) Message integrity, when information is exchanged between two Bluetooth devices, it has to be secure and nothing can be modified.

(e) Pairing/bonding, the generated keys are shared and stored for future use, to create trust between two Bluetooth devices.

3.1. Bluetooth Classic

Bluetooth includes four security modes; mode 1 has no security, mode 2 has authentication and encryption in the controller, and mode 3 has it in the physical link. These three modes only existed in the prior Bluetooth 2.1 version.

Security Mode 4 is a service-level enforced security mode; it uses secure simple pairing (SSP) and it uses Elliptic-curve Diffie–Hellman (ECDH) key agreement for link key generation. This helps protect against eavesdropping and man-in-the-middle attacks. The ECDH that is used could be the elliptic curve 192 or 256. For authentication and encryption, a secret symmetric key is necessary, and it is known as the link key. Security mode 4 includes five security levels. Starting from security level 0 and ending at security level 4: (i) Level 0 has no security and is only allowed for service discovery protocols; (ii) Level 1, also does not require security; (iii) Level 2 requires an unauthenticated link key; (iv) Level 3 requires an authenticated link key, and; (v) Level 4 requires authenticating the link key using secure connections. The secure connections pairing protocol was introduced in Bluetooth 4.1 and it uses the ECDH 256, improving from the ECDH 192 that was used prior.

3.2. Bluetooth Low Energy

This section meticulously explains BLE, to understand how it is possible to protect against the most common attacks on this technology.

Bluetooth 4.0, 4.1, and 4.2 count cryptographic keys to improve security in the devices, these keys are named Identity Resolving Key (IRK), to support low-energy private device addresses, and Connections Signature Resolving Key (CSRK), to assist data signing. When pairing BLE devices, a Long-Term Key (LTK) is generated, which is important for authentication and encryption (known as the link key in Bluetooth Classic). This could result in two different methods. During the first method, one device generates the LTK and sends it to the other device in a secure manner; this is known as low-energy Legacy Pairing. Furthermore, it is important to notice that for this method, all the keys are distributed in a secure process during the pairing stage. In the second method, both devices create the key without the need to share it through the link. This method is called low-energy Secure Connections. Meanwhile, the LTK is generated, while the IRK and the CSRK are created and distributed securely. An important difference between these methods is that low-energy Legacy Pairing does not include Elliptic-curve Diffie–Hellman (ECDH) encryption, which makes it vulnerable to eavesdropping attacks and allows attackers to potentially find the LTK. In contrast, Low-energy Secure Connections can countermeasure this threat.

Low-energy Security includes two modes. Security Mode 1 has four levels related to encryption. Level 1 does not require encryption and authentication. Level 2 asks for unauthenticated pairing with encryption. Level 3 needs authenticated pairing with encryption. Level 4 uses the Secure Connections method previously discussed in this section, as it asks for an authenticated link key using low-energy Secure Connections pairing with encryption. Security Mode 2 requires data signing in both of its levels, with the sole difference that level 1 only needs unauthenticated pairing while level 2 asks for authenticated pairing. Because encryption is a great security asset, using Security Mode 1 Level 3 or 4 is strongly recommended over other options.

3.3. Bluetooth: Pairing Methods

In this section, the researchers give a more detailed explanation of the low-energy pairing methods and describe the phases that occurred during the pairing methods. Starting with low-energy Legacy Pairing. Phases:

(i) Phase 1, once explore the input/output capabilities and security requirements in the devices, they will establish an agreement on a Temporary Key (TK).

(ii) Phase 2, they proceed to create a Short Term Key (STK) using random values that are being exchanged and the TK. This STK establishes an encrypted link between devices.

(iii) Phase 3, it assures a safe key transport for all the keys mentioned earlier in this article (LTK, IRK, CSRK).

Low-energy Secure Connections work in a different manner. Even though phase 1 works the same way as legacy pairing, in phase 2, the LTK is generated without the need for the STK. This LTK is useful in phase 3, and the LTK encrypts the links, and a key agreement is made to distribute the IRK and CSRK securely instead of using a key transport.

During the pairing process between two devices, one of four different pairing processes can be applied. These pairing processes are: (a) Out of Band for Bluetooth Standard or BLE; (b) Numeric Comparison; (c) Passkey Entry 4 or 6 digits; and (d) Just Works. The input/output capabilities of devices play an important role in determining what processes can be utilized.

The out-of-band (OOB) process requires two devices that have OOB technology, such as near-field communication (NFC). One device sends the other a 128-bit number, which is the TK, using OOB technology. Using low-energy Legacy Pairing provides one-in-a-million protection against MITM attacks to guess the TK. However, this protection comes from the OOB technology that the device uses, because if someone is capable of eavesdropping on the OOB, they will obtain the TK values. For low-energy Secure Connections, the device address is sent through the OOB. Even if an eavesdropper can obtain it, this does not give them any value in decrypting the data.

Numeric comparison is an option available only for low-energy Secure Connections. This method is not available for low-energy Legacy Pairing. The process involves two devices displaying a 6-digit number on their respective screens, and the user enters one of two options: (i) YES, if both displays show the same 6-digit number; (ii) NO, if the numbers are different. The previous 6-digit number is not used to generate the link key to avoid eavesdropping. Even if an unauthorized person captures this 6-digit number, it will not be useful for any further pairing process. Additionally, it has protection against MITM attacks, as the user must confirm if the 6-digit number is or is not the same on both devices before proceeding. This guarantees that no other device can initiate the pairing process.

Another method is passkey entry, which requires that both devices have a keyboard input or at least one of them has a display output. This method works with low-energy Legacy Pairing. A passkey is given on one device and entered on the other, and then a TK is generated using the passkey. The passkey is required to have six numeric digits, which would give an entropy of twenty bits that ensures the complexity of deciphering the given key. Low-energy Secure Connections pairing works differently. After the devices exchange public keys, the six numeric digits passkey is generated, and once it is entered into the device, it starts sending a hash of each bit of the passkey. This procedure is repeated twenty times to complete the twenty bits of the passkey. Furthermore, the public keys were sent during the previous step. This method offers protection against MITM attacks. When using a passkey of six digits, it gives an attacker a one-in-a-million chance to guess the correct passkey.

The last method is the least secure one, and it is used due to the limitations in the input/output capabilities of the devices. For low-energy Legacy Pairing the key is always the same and is set to all zeros, leaving the pairing exposed to eavesdropping and MITM attacks. In the low-energy Secure Connections method, the pairing process follows the same steps as in the numeric comparison process, but the user is unable to see the 6-digit number. This is because the devices involved in this procedure cannot display the number, which in turn makes it impossible to perform the final commitment checks.

These four pairing methods are not exclusive to Bluetooth Low-Energy; they can also be found in Bluetooth Classic, working slightly differently due to the IRK and CSRK being exclusive to BLE. Only the LTK is set to be created, but it is known as the link key. The association models (out of band, numeric comparison, and passkey entry) provide authenticated link keys; meanwhile, the link key is unauthenticated during the Just Works pairing model for Bluetooth Classic. The risk of an attack is determined by the version of Bluetooth and the pairing method used. See **Figure 3**.

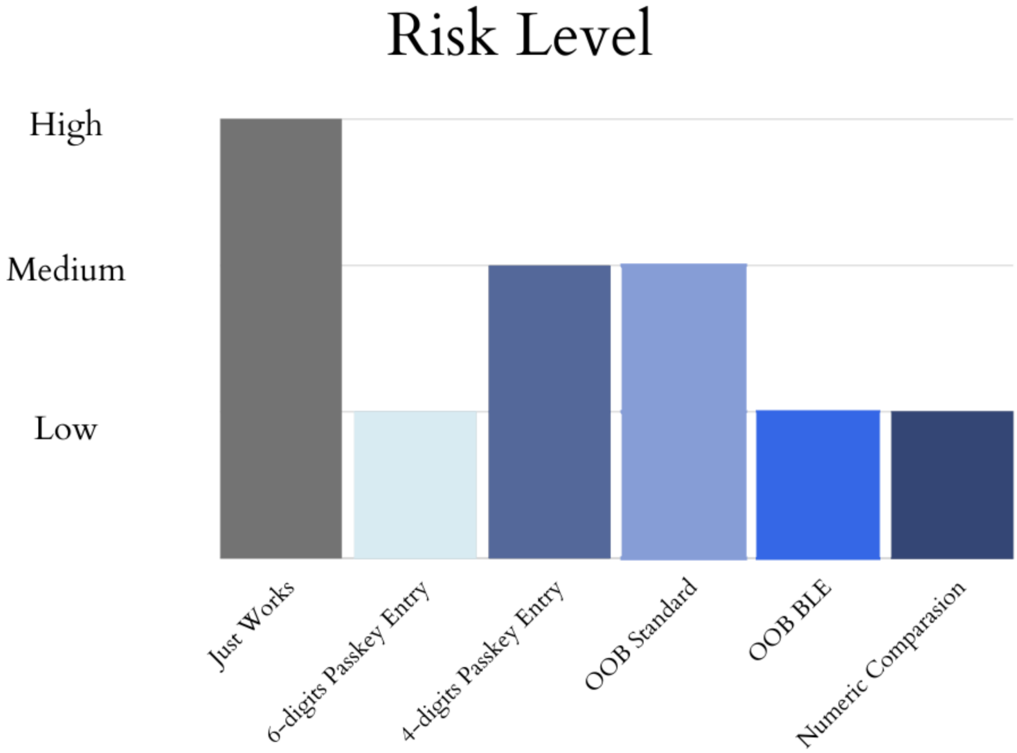

Figure 3. Risk Level on Pairing Methods.

References

1. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of Things: Evolution and technologies from a security perspective. Sustain. Cities Soc. 2020, 54, 101728.
2. Vailshery, L.S. IoT and non-IoT connections worldwide 2010–2025. Stat. March 2021. Available online: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed on 2 March 2023).
3. Alrashdi, I.; Alqazzaz, A.; Aloufi, E.; Alharthi, R.; Zohdy, M.A.; Hua, M. AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 305–310.
4. Zubair, M.; Ghubaish, A.; Unal, D.; Al-Ali, A.; Reimann, T.; Alinier, G.; Hammoudeh, M.; Qadir, J. Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System. Sensors 2022, 22, 8280.
5. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. Sensors 2022, 22, 7433.
6. Seneviratne, S.; Hu, Y.; Nguyen, T.; Lan, G.; Khalifa, S.; Thilakarathna, K.; Hassan, M.; Seneviratne, A. A survey of wearable devices and challenges. IEEE Commun. Surv. Tutor. 2017, 19, 2573–2620.
7. Sivanathan, A.; Gharakheili, H.H.; Sivaraman, V. Detecting Behavioral Change of IoT Devices Using Clustering-Based Network Traffic Modeling. IEEE Internet Things J. 2020, 7, 7295–7309.
8. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. IEEE Access 2015, 3, 678–708.
9. Rao, T.A.; Haq, E. Security challenges facing IoT layers and its protective measures. Int. J. Comput. Appl. 2018, 179, 31–35.
10. Ching, K.W.; Singh, M.M. Wearable technology devices security and privacy vulnerability analysis. Int. J. Netw. Secur. Its Appl. 2016, 8, 19–30.
11. What could derail the wearables revolution? Nature 2015, 525, 22–24.
12. Isakadze, N.; Martin, S.S. How useful is the smartwatch ECG? Trends Cardiovasc. Med. 2020, 30, 442–448.
13. Bakhshiyeva, A.; Berefelt, G. Eavesdropping Attacks on Modern-Day Connected Vehicles and Their Ramifications; KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science: Stockholm, Sweden, 2022.
14. Lee, M.; Lee, K.; Shim, J.; Cho, S.j.; Choi, J. Security threat on wearable services: Empirical study using a commercial smartband. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Seoul, Republic of Korea, 26–28 October 2016; pp. 1–5.

15. Rahman, M.; Carbunar, B.; Topkara, U. Secure Management of Low Power Fitness Trackers. IEEE Trans. Mob. Comput. 2016, 15, 447–459.
16. Singh, M.M.; Ching, K.W.; Manaf, A.A. A novel out-of-band biometrics authentication scheme for wearable devices. Int. J. Comput. Appl. 2020, 42, 589–601.
17. Khader, R.; Eleyan, D. Survey of DoS/DDoS attacks in IoT. Sustain. Eng. Innov. 2021, 3, 23–28.
18. Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security vulnerabilities in Bluetooth technology as used in IoT. J. Sens. Actuator Netw. 2018, 7, 28.
19. Sun, D.Z.; Sun, L.; Yang, Y. On secure simple pairing in Bluetooth standard v5. 0-part II: Privacy analysis and enhancement for low energy. Sensors 2019, 19, 3259.
20. Blow, F.; Hu, Y.H.; Hoppa, M. A study on vulnerabilities and threats to wearable devices. J. Colloq. Inf. Syst. Secur. Educ. 2020, 7, 7.
21. Garbelini, M.E.; Wang, C.; Chattopadhyay, S.; Sun, S.; Kurniawan, E. Sweyntooth: Unleashing mayhem over Bluetooth Low Eenergy. In Proceedings of the 2020 USENIX Conference on Usenix Annual Technical Conference, Boston, MA, USA, 15–17 July 2020; pp. 911–925.
22. Bada, M.; von Solms, B. A cybersecurity guide for using fitness devices. In The Fifth International Conference on Safety and Security with IoT; Springer: Berlin/Heidelberg, Germany, 2023; pp. 35–45.
23. Zhang, C.; Shahriar, H.; Riad, A.K. Security and Privacy Analysis of Wearable Health Device. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; pp. 1767–1772.
24. Cyr, B.; Horn, W.; Miao, D.; Specter, M. Security analysis of wearable fitness devices (fitbit). Mass. Inst. Technol. 2014. Available online: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082016/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf (accessed on 3 March 2023).
25. Cusack, B.; Antony, B.; Ward, G.; Mody, S. Assessment of Security Vulnerabilities in Wearable Devices, 2017. Available online: https://ro.ecu.edu.au/ism/207/ (accessed on 5 March 2023).
26. Ryan, M. Bluetooth: With low energy comes low security. In Proceedings of the 7th USENIX Workshop on Offensive Technologies (WOOT 13), Washington, DC, USA, 13 August 2013.
27. Kurt Peker, Y.; Bello, G.; Perez, A.J. On the Security of Bluetooth Low Energy in Two Consumer Wearable Heart Rate Monitors/Sensing Devices. Sensors 2022, 22, 988.
28. Al Kalaa, M.O.; Balid, W.; Bitar, N.; Refai, H.H. Evaluating Bluetooth Low Energy in realistic wireless environments. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; pp. 1–6.

29. Hager, C.T.; MidKiff, S.F. An analysis of Bluetooth security vulnerabilities. In Proceedings of the 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003, New Orleans, LA, USA, 16–20 March 2003; Volume 3, pp. 1825–1831.

Retrieved from https://encyclopedia.pub/entry/history/show/104438