Wireless Networks
https://doi.org/10.1007/s11276-022-03211-6

Analysis of security and privacy issues in wearables for minors

Jaime Fúster[1] · Sonia Solera-Cotanilla[2] · Jaime Pérez[1] · Mario Vega-Barbas[2] · Rafael Palacios[1] · Manuel Álvarez-Campana[2] · Gregorio Lopez[1]

Accepted: 13 December 2022

Abstract
The increased use of wearables in recent years has fostered a great technological development in this area, although without the appropriate supervision usability may go first than security. In addition to this, the fact that wearables have been requiring more and more personal data from the user makes them attractive devices for an attacker. In this paper we propose a set of tests for evaluating the security and privacy of wearables and we apply them to analyse the security and privacy of a set of commercial wearables that are targeted at minors, who represent a group with especially high requirements in this regard. We define the testing scenario, expose the tools to support the research, and specify the testing process to be followed. Based on the obtained results, although the considered low-end devices are broadly speaking less secure than high-end ones, most of them present security and privacy flaws, which illustrates the necessity of regulation that ensures the fulfilment of appropriate security and privacy requirements.

Keywords Cybersecurity · Internet of things · Minors · Privacy · Wearables

1 Introduction

Over the last few years, there has been a remarkable increase in the market for wearable devices (henceforth, wearables) [1]. In 2021, the global smartwatch industry was estimated at US$81.5 billion [2], with the expectation of reaching US$118.6 billion by 2028, according to Business Wire [3]. The popularity of wearable fitness devices has also grown dramatically in the past decade. Thus, the number of these devices shipped worldwide grew from 11.8 million units in 2015 to 153.5 million in 2020 [1]. Unlike wearables of the past, today's wearables collect a wide range of data that is often stored in the cloud, managed by third parties, and used to display aggregate user information on mobile devices. Such user data frequently involves sensitive information that ranges from the user's location and email address to heart rate information and other health-related data.

Even though the accelerated growth of the wearable market may favour technological progress, it poses the risk that their production grows without the adequate control and regulation required to ensure appropriate levels of privacy and security. Insufficient or ineffective oversight of the production of these devices may allow the release of insecure products that prioritise usability over security.

✉ Jaime Fúster
jaimeff@alu.comillas.edu

✉ Gregorio Lopez
gregorio.lopez@comillas.edu

Sonia Solera-Cotanilla
sonia.solera@upm.es

Jaime Pérez
jperezs@comillas.edu

Mario Vega-Barbas
mario.vega@upm.es

Rafael Palacios
rafael.palacios@iit.comillas.edu

Manuel Álvarez-Campana
manuel.alvarez-campana@upm.es

[1] Institute for Research in Technology, ICAI, Comillas Pontifical University, Madrid, Spain

[2] Escuela Técnica Superior de Ingenierios de Telecomunicación, Universidad Politécnica de Madrid, Madrid, Spain

Published online: 08 March 2023

Understandably, this threat is of particular concern in the case of wearables for minors. Thus, the Norwegian Consumer Council [4] found significant security flaws in smartwatches for minors in 2017, leading some agencies, such as the German Federal Telecommunications Agency (Bundesnetzagentur), to prohibit the sale of smartwatches for children, describing them as spying tools and going so far as to urge parents to destroy their children's devices [5]. As a token of how sensitive is to handle personal data from minors, there are specific articles dealing with this in the European Union General Data Protection Regulation (GDPR) and, in the United States, the Children's Online Privacy Protection Act (COPPA) deals specifically with it.

Although some companies have recently focused their strategies on selling products that ensure the privacy and security of their users, the results of a search on the major online marketplaces show that a significant part of the market consists of products with no such warranties. These products are often low-cost devices that generate high sales figures but prioritise price, usability, and convenience over security and privacy. Even if well-known brands such as Fitbit or Apple have usually taken up more than fifty per cent of the wearable market over the years, less-known brands seem to be on the rise [1].

On another note, recent research points towards an increasing apathy of the general public regarding data privacy and IoT security. Studies such as the one carried out in [6] showcase the prevalent lack of awareness of consumers regarding privacy and security in fitness trackers, while [7] highlights wearable users' ambivalence towards privacy versus usability. Even though some organizations and institutions such as the aforementioned Bundesnetzagentur have taken measures to protect citizen's privacy such as banning specific products, nearly 70% of American adults do not express worries about cybersecurity in their personal lives, or in their expectations for the data integrity of various public institutions, according to a 2017 study carried out in the US [8].

Given this scenario and the sensitive nature of the data in question, it seems timely to study the current market situation by analysing the security and privacy of these devices.

In this paper we propose a set of tests for evaluating security and privacy risks in wearables. Using these tests we analyse security and privacy issues in wearables currently being marketed to children and young people, considering that they are a specially sensitive group in terms of security and privacy that represents a remarkable part of the market. In addition, we identify the source of the threats, taking advantage of easily and freely accessible tools that apply to similar IoT scenarios, and we propose recommendations and countermeasures. As a result, we aim to increase transparency and user awareness on the security and privacy of wearables, as well as to encourage manufacturers to improve their security and privacy features, paying special attention to the protection of the most vulnerable groups, like children.

Other works in the literature have already addressed the cybersecurity problems of IoT and wearable devices [9–12]. In contrast to such papers, we define a series of tests for vulnerability testing of wearables that encompasses all communications scenarios involved in the operation of such devices. In addition, to support such tests, a toolkit for security and privacy vulnerabilities analysis in the context of wearables is also provided.

The rest of the paper is organised as follows. Section 2 discusses related work on the security and privacy of wearables and mobile applications. This section briefly describes the Bluetooth Low Energy (BLE) protocol, along with relevant vulnerabilities found in the literature, since BLE represents the current *de facto* standard for the communication between wearables and smartphones. In Sect. 3, we present the proposed tests and support tools, defining the attack scenario, attack categories, and testing procedures. Section 4 describes the results obtained from implementing the set of tests on a range of wearables used by and marketed to minors. In Sect. 5, we discuss those results and analyse possible mitigations to the identified risks. Finally, Sect. 6 draws the main conclusions from this research.

2 Background

In this section, we provide an overview of the background that serves as the basis for our research by describing prior works on security and privacy in wearables and mobile applications, as well as some relevant aspects of BLE. First, in Sect. 2.1 we outline some important aspects and concepts of BLE, paying special attention to security features, pairing methods, and significant vulnerabilities. Then, in Sect. 2.2, we review previous work related to wearables and their security threats. Finally, in Sect. 2.3, we review pertinent work related to privacy in mobile apps.

2.1 Overview of Bluetooth Low Energy

BLE is a Wireless Personal Area Network (WPAN) technology for applications in areas such as health, fitness, multimedia, or home. BLE is regulated by the Bluetooth Special Interest Group (SIG), which maintains and reviews the Bluetooth standard [13]. BLE operates in shorter ranges and consumes much less energy than classic Bluetooth and previous standards.

BLE is a Master-Slave protocol. This implies that the protocol distinguishes between a master or central device

that scans for other devices and initiates the communication, and slave or peripheral devices which announce themselves and connect to the master. While a master can connect to multiple slaves devices simultaneously, a slave device can only connect to one master at a time. Figure 1 illustrates two state diagrams describing the connection process between a central and a peripheral device in BLE. Peripheral devices start by announcing their characteristics, waiting for a central device to initiate the connection or request more information through a scan request. Once connected, the devices will exchange information and communicate until the master node sends a disconnect command.

The connection process used in the BLE protocol (v4.0 and v4.1) is known as BLE Legacy Pairing. In BLE Legacy Pairing a symmetric key for a master-slave link is generated during the pairing procedure, which is executed as follows:

- The devices exchange their authentication capabilities and requirements. This phase is carried out without any encryption.
- The devices generate and exchange a Temporary Key (TK) using one of the available pairing methods. Then, they exchange a series of data to check that the TK matches between the two devices, in which case a Short-Term Key STK is generated from the TK itself. This STK is used to encrypt the data stream.

A bonding phase may follow this pairing procedure, in which the devices exchange and store common link keys (*bonds*), which can be reused when re-establishing a connection between the two devices later.

Starting with the Bluetooth 4.2 specification, BLE Secure Connections was introduced, implementing an enormously more secure pairing procedure based on Elliptic Curve Cryptography (ECC). However, this type of cryptography comes with limitations: according to experimental results [14], the energy consumed during a single ECDH-ECDSA key exchange is more than 6,000 times higher than that required by symmetric encryption techniques (236 mJ versus 38 μJ).

There are four BLE pairing methods defined in the Bluetooth v5.2 standard [13]:

- *Just Works*: Automatic pairing, without a Passkey. The TK is set to 0, so it is straightforward for an attacker to brute-force the STK and decrypt the communication.
- *Numeric Comparison*: Similar to *Just Works*, but a value, generated from the public keys and nonces, is displayed on both devices and must be confirmed by the user. This pairing method is only available for BLE Secure Connections. Introduced from Bluetooth 4.2, it solves the security problem of the previous method.
- *Out of Band*: The TK is exchanged out of band, so the data security, integrity and privacy will depend on the method used.
- *Passkey*: The TK is a six-digit number defined by the user. In Bluetooth 4.1 and 4.0, the Passkey is a six-digit number entered by the user or generated by the peripheral device.

Since its first specification in 2010 and over the years, various vulnerabilities, security issues and attacks against BLE have emerged. The most relevant ones are listed in Table 1. Although some of these vulnerabilities appear only in older BLE specifications and seem to have been fixed in later versions, most devices today still implement Bluetooth 4.0, 4.1 and 4.2, so the weaknesses are still relevant.

On the other hand, smartphones tend to disconnect periodically from wearable devices to save power. This causes a large portion of wearables to be in advertisement mode most of the time, exposing their MAC address and allowing a potential attacker to easily identify any device, user, and his/her movements. This class of attack can be exploited to track a user's activity, even when communications are encrypted [11].

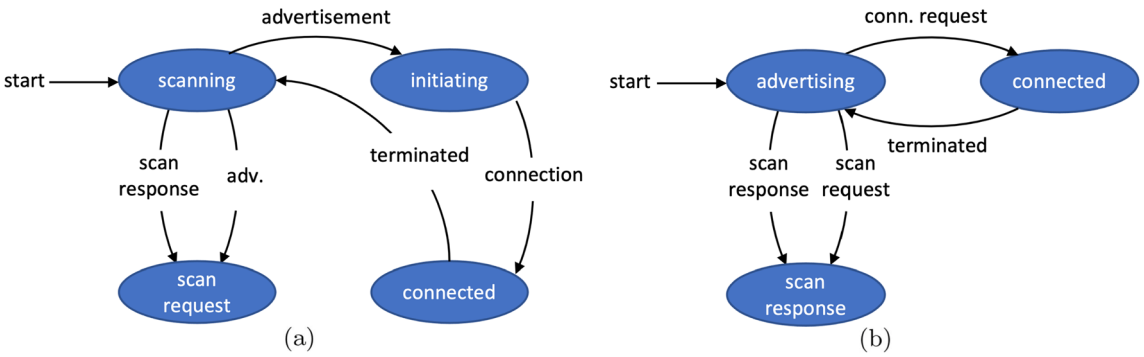


Fig. 1 BLE connection process: **a** Master or central **b** Slave or peripheral

Table 1 Summary of vulnerabilities in Bluetooth

Security issue	Remarks	BLE version
No Man-In-The-Middle (MITM) or eavesdropping protection	Attackers can capture and manipulate data exchanged between trusted devices [15]. In BLE Legacy Pairing, Just Works is vulnerable to eavesdropping and MITM since the TK is known [16].	4.0 4.1 4.2
Vulnerable key generation protocol	Passkey is vulnerable to brute force attacks [16] [17].	All
Vulnerable key exchange algorithm	In Bluetooth Secure Connections Passkey paring, since the password is transmitted bit by bit and each bit is confirmed by the peripheral each time it is received, an attacker could easily guess the password or Passkey by testing each bit from reconnections with the peripheral [18] [19].	All
No user authentication	The Bluetooth specification provides device authentication only [15].	All

2.2 Wearables

S. Seneviratne *et al.* [12] offer an exhaustive study and classification of wearables available on the market, the threats to communication security, and some solutions to these problems found in the literature. The study examines threats in terms of confidentiality, integrity, and availability of the information handled by the devices. In terms of threats to confidentiality, due to the use of BLE as the primary means of communication, most wearables are vulnerable to three types of attacks:

- *Eavesdropping*: Unauthorised real-time interception of a confidential communication.
- *Traffic analysis*: Monitoring of traffic exchanged between wearable devices and their base and/or server to make inferences from communication patterns.
- *Gathering information* transferred between the device and its base (often a smartphone).

Most of the eavesdropping and traffic analysis attacks are related to inadequate implementations of the BLE publication process or the use of static device addresses. On the other hand, information gathering attacks usually involve breaking the key exchange process during BLE pairing or gathering information about other devices, such as smartphones [12]. Although not as common as confidentiality threats, the main attacks that threaten the integrity of these devices are:

- Attacks that modify the information transmitted by the device.
- Replay attacks of packets to impersonate the user's identity or corrupt data.
- Masquerading attacks, in which the attacker impersonates an authenticated device to steal data or inject false information into the system.

All the vulnerabilities found in the context of integrity attacks are due to weak authentication methods or the absence of encryption in communications between devices. Finally, Denial of Service (DoS) attacks are the most frequent attacks against wearable devices, although they are less commonly used than other categories [12]. As with the other threats, attacks against availability are possible due to implementation deficiencies of the manufacturers.

From a vulnerability assessment point of view, M. Langone *et al.* [20] describe a methodology for performing a Vulnerability Assessment (VA) on wearable devices. This VA serves to analyse and identify security issues in three different wearable devices that communicate via BLE with a smartphone: Easy Fit by Cellular Line, Fitbit Charge and Fitbit Alta by Fitbit.

The analysis results show that the use of weak Short-Term Key (STK) encryption generation methods (such as Just Work or Passkey Entry methods) and the lack of a pairing and binding process between the device and the smartphone are the principal vulnerabilities affecting these technologies. Both Easy Fit and Fitbit Charge have issues related to these vulnerabilities, allowing a malicious actor to intercept sensitive user information exchanged between the device and the smartphone.

2.3 Applications

On the Android operating system, some applications may circumvent the permissions system by using covert channels or side channels. J. Reardon *et al.* [21] demonstrate that, with enough permissions, Android applications could use the SD card as a covert channel to share the phone's International Mobile Equipment Identity (IMEI), a numerical value that identifies mobile phones uniquely with other unauthorised apps. Furthermore, some applications utilised other channels to estimate and share user location through the device MAC address, ARP cache, or picture metadata.

Concerning parental control apps, A. Feal *et al.* [22] conducted an in-depth study of the Android parental

control app's ecosystem from a privacy and regulatory standpoints. This study distinguishes between monitoring apps, which enable parents to monitor children's behaviour (including location), and restriction apps, which enable parents to filter content and define usage rules to limit the children's actions. Regarding the use of permissions, A. Feal *et al.* [22] showed that parental control apps request 27 permissions on average, 9 of them being labelled as dangerous. These dangerous permissions were used to leak data to remote servers in many cases. Most of these data leaks required logging user actions (e.g., logging a failed/successful authentication), and some involved sensitive data like unique identifiers, such as the device's IMEI. Some apps analysed in [22] also use custom permissions to obtain functionalities exposed by other developers or handset vendors, revealing (commercial) partnerships between them. Many of the calls to dangerous permission-protected methods were invoked only by embedded third-party libraries. Only half of the apps tested clearly informed users about their data collection and processing practices. While 59% of the apps admitted third party usage of sensitive data, only 24% disclosed the complete list of third parties embedded in the software.

Regarding regulatory compliance, I. Reyes *et al.* [23] presented a framework for automatic evaluation of the privacy behaviours of Android apps. The said framework analysed the COPPA (Children's Online Privacy Protection Act) compliance of 5,855 of the most popular free children's apps. This analysis showed that most of the examined applications were potentially in violation of COPPA, mainly due to the use of third-party SDKs. Several applications sent sensitive user information to remote servers, including geolocation data and the device owner's email address and phone number. Moreover, the study found that more than half of the apps did not use TLS in at least one transmission containing identifiers or other sensitive information.

3 Testing methodology

In this section, we present a proposed set of tests, describing the testing scenario, the tools that have been used to perform the tests, the attack categories considered in the tests, and a common procedure to be followed in each test for the sake of uniformity and replicability.

3.1 Testing scenario

The communication scheme commonly used by current wearables is shown in Fig. 2. An element with higher computing capacity (e.g., smartphone) is an intermediary (hub, configurator, etc.) between the wearable device and the external servers. As it has already been mentioned, the most common communication technology between these devices is BLE.

Figure 3 shows the specific testing scenario used in this research. We can observe three potential communication areas of analysis: (i) the first one focused on the user-device interaction; (ii) the second one on the communication between the wearable and the communication hub (e.g., smartphone); (iii) and the third one on the communication between the hub and external servers or third-party applications.

In this work, we focus on the second and third communication segments. In the case of the communication between the hub (e.g., smartphone) and the external servers, we will not analyse the case of Long-Term Evolution (LTE) mobile connection. Instead, we will focus on the scenario where a Wi-Fi connection is used in this interface.

3.2 Support tools

The testing methodology focuses on analysing the information packets emitted by the devices involved. For this purpose, we have used the software tool Wireshark to analyse BLE and Wi-Fi communications, as it is also shown in Fig. 3. Wireshark is a widely-used communication packet analyser. Besides, it is an open-source and

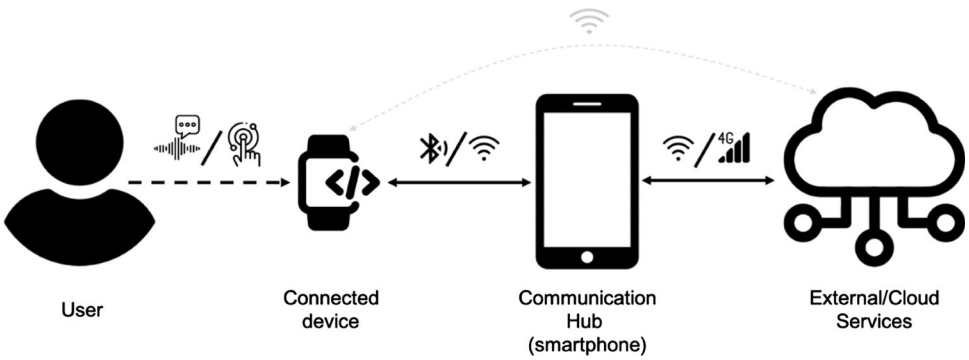


Fig. 2 Communications scenario overview

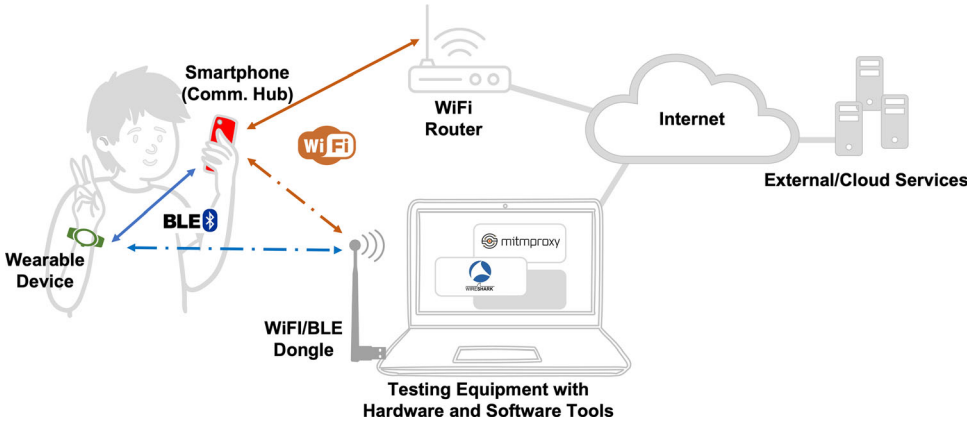


Fig. 3 Testing scenario

cross-platform tool, which facilitates its adaptation to different hardware tools and operating systems and provides us with great versatility. The following subsections describe the remaining hardware and software tools used to perform the planned tests.

To intercept the BLE communication packets, we used the Nordic Semiconductor nRF52 DK sniffer device. This device is compatible with the tool Wireshark, it is programmable, and it supports BLE, Bluetooth Mesh, Near Field Communication (NFC), and ANT communications. Furthermore, to simulate some attacks (e.g., ping of death), we have used BlueZ, the official Linux Bluetooth protocol stack software, on a Raspberry Pi 4 Model B.

To intercept the Wi-Fi communication packets, we used the antennas TP-Link TL-WN722N and Alfa AWU-S036ACH. Moreover, to trace the packets sent between the smartphone application (of the wearable device) and the external server, we have used Mitmproxy, an open-source tool that provides an interactive proxy with SSL/TLS capability to intercept HTTP/1, HTTP/2 and WebSockets, creating an HTTP proxy for the smartphone's connections.

To protect the integrity and confidentiality of transmitted data, HTTPS uses the TLS/SSL protocol to encrypt data. Therefore, to successfully intercept HTTPS traffic transmitted between a smartphone and an external server, it is necessary to install a customised root certificate on the device. Mitmproxy uses a self-created certificate that will be trusted by the smartphone being analysed, implementing a Man In The Middle (MITM) attack against the application. Thus, the encrypted content of messages exchanged can be captured in plain text.

To control the Wi-Fi-based communication environment, we created a virtual hotspot, as shown in Fig. 4. For this purpose, we have used the TP-Link TL-WN722N antenna and an Ubuntu 20.04.2.0 operating system virtualised through VirtualBox.

3.3 Attack categories

The following list shows attack categories that are considered to be relevant in the context of wearables and that need to be tested.

(1) Authentication: The application associated with the wearable device implements a method to authenticate the user's identity.
(2) Insecure pairing method: The link between the wearable device and the smartphone uses a pairing method considered insecure or ineffective against

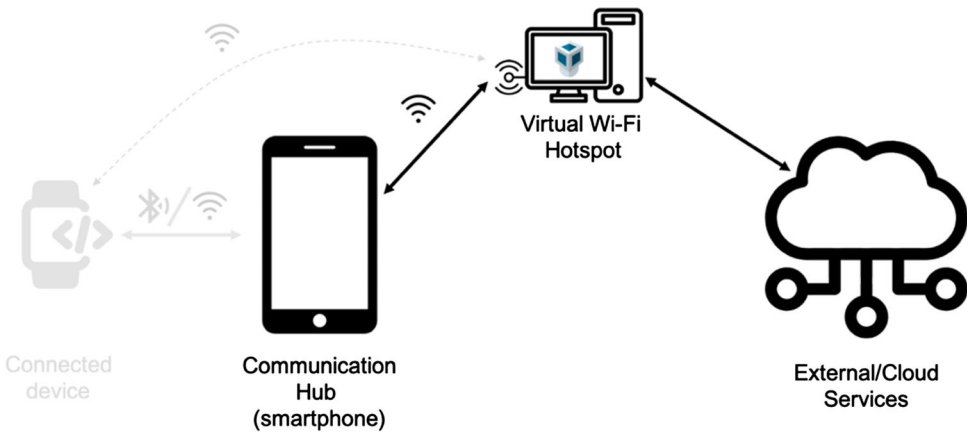


Fig. 4 Virtualised hotspot overview

MITM attacks or passive eavesdropping attacks and lacks privacy safeguards.

(3) Unencrypted Communications: BLE communications between the wearable device and smartphone are not encrypted.
(4) Encryption key capture: During the pairing process, the wearable and mobile devices exchange encryption keys in a format that the BLE sniffer can easily capture and process.
(5) Static MAC address: The wearable device uses a static MAC address (i.e., it does not change when the device is turned off or restarted and does not change periodically), exposing it to tracking and user identification attacks.
(6) Transmission of sensitive information to third-party servers: The application sends sensitive user information to third-party servers.
(7) Sending of information and firmware updates via HTTP: The application receives firmware updates and sends requests with sensitive information using HTTP without TLS encryption.

Table 2 provides a mapping of such categories with the most common security and privacy issues in connected devices used by minors identified in [24].

3.4 Testing procedure

Although each wearable may follow a different operating procedure, it can be generalised. This way, it is possible to systematise the evidence acquisition process during the execution of the defined tests. Thus, it is possible to obtain a uniform set of results and avoid excluding relevant data and evidence. In order to achieve this goal, the following procedure is defined and must be followed during test execution.

(1) Switching on the wearable and mobile device.
(2) Connection of the wearable with nRF52 DK and Wireshark.
(3) Registering/Logging into the application.
(4) Pairing process of wearable device and smartphone.
(5) BLE data collection activities:
    - Carrying out physical activities such as walking, running, etc.
    - Data Synchronization with wearable.
    - Disconnection from wearable.
    - Reconnection with wearable.
(6) HTTP data collection activities:
    - Editing the user profile.
    - Synchronization of data with cloud servers.
    - Logging out.
    - Logging in.

Table 2 Mapping of the performed tests with security and privacy issues

		Performed Tests						
		Authentication	Insecure pairing method	Unencrypted communications	Encryption keys in plain text	Static MAC address	Sharing sensitive information with third-party servers	Communications and firmware updates over HTTP
Security & Privacy Issues	Spoofing	✗		✗	✗	✗		✗
	Lack or weak encryption			✗				✗
	Lack or weak authentication	✗						
	Code Injection	✗						
	Data Interception		✗	✗	✗	✗		✗
	Takeover	✗		✗	✗	✗		
	User data compromised			✗		✗		
	Violation of privacy laws			✗			✗	
	Lack of control and understanding						✗	

(7) Disconnection.

4 Analysis of results

In this section, we describe the results obtained from the application of the tests presented in the previous section to a set of commercial wearables for minors. Thus, first we present the selected wearables, justifying why they have been chosen. In addition, the mobile apps used by such wearables are also introduced, since they will be also part of the security and privacy analysis. Then, the main results of the security and privacy analysis of such devices and their associated apps are described. Finally, such results are summarised and compared.

4.1 Device selection

For the application phase of our research, wearables were selected to include high-end brands, such as Fitbit or Garmin, as well as much less expensive albeit prevalent devices found in marketplaces such as Amazon and Alibaba, so that they can be compared. In addition, an effort was made to include models specifically designed for children. The devices selected for the analysis are shown in Table 3. To estimate the popularity of the selected devices, Table 3 includes the number of reviews in Amazon.com at due time. The average price of the selected wearables is also provided to get an idea of whether they are high-end or low-end devices. As we can see in Table 3, beside blockbuster devices such as Mi Band or Fitbit, there are also very cheap wearables from BIGGERFIVE or TOOBUR that count with thousands of reviews.

A summary of the applications used by these wearables is also shown in Table 4. As it can be seen, BIGGERFIVE and TOOBUR devices share the same application (VeryFitPro).

4.2 Results

Next, the results from the security and privacy analysis of such wearables are summarized. It should be noted that such results were obtained during a set of tests carried out during 2021, so some of the reported issues may have been fixed by the manufacturer.

4.2.1 Authentication

Most fitness tracker apps include methods for user authentication, although not all applications ensure they are used or make the user register before using the app. In this sense, Mi Band 5 and Amazfit Band 5 both require the user to connect via Huami apps: Mi Fit and Zepp, respectively. These applications require validation, using a "Mi Account" or a third-party account such as Google, Apple, Mi-Xioami or Facebook.

Similarly, other higher-end wearable devices require users to use proprietary or specific applications. Garmin Vívofit jr. 2 demands the user register the device to the Garmin Jr. app, and Fitbit Ace 3 and Fitbit Inspire 2 require the Fitbit app and a Fitbit account. Both registration procedures can be done from third-party accounts such as Google or Apple. In the case of the Fitbit Ace 3, it is necessary to create a family account. Once registered, the app allows the user to switch between different views for child/adult by validating with the account password. Honor Band 5 and Honor Watch ES use Huawei Health with a Huawei ID that requires a phone and email address for registration. Both BIGGERFIVE devices (Fitness and Vigor) and TOOBUR devices (Smart band and Smartwatch) recommend using a third-party application,

Table 3 Summary of analysed wearables

Device name	Brand	# of reviews in Amazon.com	Average price
Garmin Vívofit jr.	Garmin	11k+	$70
Fitbit ace 3	Fitbit	2k+	$80
Mi band 5	Xiaomi	51k+	$40
Amazfit band 5	Amazfit/Xiaom	13k+	$40
Honor band 5	Honor	4k+	$45
Honor watch ES	Honor	1k+	$88
TOOBUR smartwatch	TOOBUR	6.5k+	$40
BIGGERFIVE fitness	BIGGERFIVE	3.7k+	$23
BIGGERFIVE vigor	BIGGERFIVE	8.9k+	$30
Fitbit inspire 2	Fitbit	32.8k+	$100
TOOBUR smart band	TOOBUR	3.7k+	$23
Apple watch series 6	Apple	5.4k+	$400

Table 4 Summary of analysed fitness apps

App name	Version	# downloads	Developer	Wearable device
Garmin jr.	5.2.2	500k+	Garmin	Vívofit jr. 2
Fitbit	3.43.1	50M+	Fitbit	Fitbit ace 3, Fitbit inspire 2
Mi Fit	5.2.0	100M+	Huami	Mi band
Zepp	6.7.1	10M+	Huami	Amazfit band 5
Huawei health	10.1.1.312	100M+	Huawei	Honor band 5, Honor watch ES
VeryFitPro	3.3.0	10M+	Youduoyun	BIGGERFIVE fitness, BIGGERFIVE vigor, TOOBUR smartwatch, TOOBUR smart band

VeryFitPro, which does not require any authentication or registration, although a user account can be created.

4.2.2 Pairing and encryption

Huami and Honor wearable devices connect to the central smartphone device without encryption, so communications in the Bluetooth segment are unencrypted. Nevertheless, Zepp, Mi Fit and Huawei Health appear to establish a connection between the band and each company's servers, hiding communications by using the company's proprietary Services and preventing other applications from being used. The apps authenticate and pair the phone with Huami or Huawei servers and hide the Auth Key in the phone's file system so that other apps cannot use it. Examples of BLE traffic showing the use of these proprietary Services are shown in Fig. 5.

Although it is not easy to immediately identify what information is being communicated, since the communications are not encrypted, an attacker could understand the operation of Huami's or Huawei's proprietary Services and obtain the user's data. Several websites demonstrate how to circumvent this constraint [25] [26].

Garmin Vívofit jr.2 uses the *Passkey* method for pairing, whereby the user must enter the app a number that appears on the wearable screen. There is encryption, but even though the device utilises BLE version 4.2, the connection is established with LE Legacy Pairing instead of LE Secure Connections, hence allowing for a sniffer to decrypt the packets being exchanged thanks to the Long-Term Key (LTK) being sent in clear text, as shown in Fig. 6.

Fitbit Ace 3 and Fitbit Inspire 2 implement BLE Secure Connections and feature the most secure pairing procedure, encrypting communications with a public key and Elliptic Curve Cryptography (ECC). Implementing an Elliptic Curve Diffie Hellman (ECDH) key exchange algorithm, makes it impossible to decrypt the communication once the devices are paired. The pairing method used is *Passkey*, with a 4-digit key instead of 6. An example of BLE traffic showing ECDH and BLE Secure connections is shown in Fig. 7.

The TOOBUR and BIGGERFIVE wearable devices analysed paired with the smartphone directly, using the *Just Works Method* with no encryption, allowing the device to seamlessly connect to any other device once it has lost connectivity with the central communications hub (e.g., the user's smartphone). If paired from outside VeryFitPro, TOOBUR Smartwacth's LTK is sent in plain text, so that a sniffer can intercept the exchanged packets.

In the case of the information sent from the application to external servers through Wi-Fi and the Internet, it is possible to observe encrypted information (via HTTPS), but some information is also sent in plain text (HTTP). This information transmitted in plain text contains sensitive

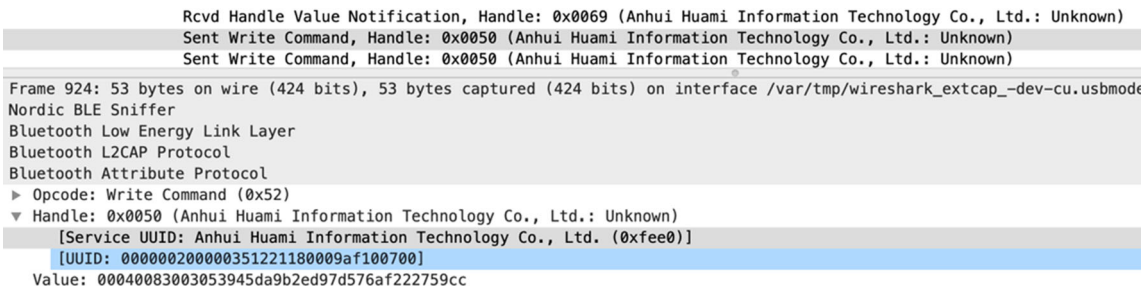


Fig. 5 Proprietary Huami BLE attributes used by Mi Fit

```
1283 45.497   Master_0xb769cac7 LE 1M   LE LL            23 36393µs              Control Opcode: LL_ENC_REQ
1287 45.535   Slave_0xb769cac7  LE 1M   LE LL            13 151µs                Control Opcode: LL_ENC_RSP
1291 45.610   Slave_0xb769cac7  LE 1M   LE LL             1 150µs                Control Opcode: LL_START_ENC_REQ
1292 45.647   Master_0xb769cac7 LE 1M   LE LL             1 37182µs              Control Opcode: LL_START_ENC_RSP
1296 45.685   Slave_0xb769cac7  LE 1M   LE LL             1 150µs                Control Opcode: LL_START_ENC_RSP
1298 45.723   Slave_0xb769cac7  LE 1M   SMP              21 150µs                Rcvd Encryption Information
1301 45.798   Slave_0xb769cac7  LE 1M   SMP              15 150µs                Rcvd Master Identification
1326 46.323   Master_0xb769cac7 LE 1M   ATT              13 37189µs              Sent Find By Type Value Request, GATT Pri

Frame 1298: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface /var/tmp/wireshark_extcap_-dev-cu.usbmodem0006823
Nordic BLE Sniffer
Bluetooth Low Energy Link Layer
Bluetooth L2CAP Protocol
Bluetooth Security Manager Protocol
   Opcode: Encryption Information (0x06)
   Long Term Key: 4723f2482fd062daa608565ae374a72b
```

Fig. 6 Wireshark capture of a LTK sent in clear text by Garmin Vívofit jr. 2

No.	Time	Source	PHY	Protocol	Length	Delta time (µs end to start)	Info
78771	404.897	Slave_0x9aa2a661	LE 1M	SMP	69	150µs	Rcvd Pairing Public Key
78773	404.937	Slave_0x9aa2a661	LE 1M	SMP	21	150µs	Rcvd Pairing Confirm
78774	404.977	Master_0x9aa2a661	LE 1M	SMP	21	39522µs	Sent Pairing Random
78779	405.016	Slave_0x9aa2a661	LE 1M	SMP	21	150µs	Rcvd Pairing Random
78989	409.336	Slave_0x9aa2a661	LE 1M	L2CAP	16	149µs	Connection Parameter Update Request
78990	409.377	Master_0x9aa2a661	LE 1M	LE LL	12	39563µs	Control Opcode: LL_CONNECTION_UPDATE_IND
78992	409.379	Master_0x9aa2a661	LE 1M	L2CAP	10	150µs	Connection Parameter Update Response (Accepted)
79010	409.829	Master_0x9aa2a661	LE 1M	LE LL	9	172191µs	Control Opcode: LL_LENGTH_REQ
79013	409.832	Slave_0x9aa2a661	LE 1M	LE LL	9	149µs	Control Opcode: LL_LENGTH_RSP
79028	411.156	Master_0x9aa2a661	LE 1M	SMP	21	150µs	Sent Pairing DHKey Check
79034	411.419	Slave_0x9aa2a661	LE 1M	SMP	21	150µs	Rcvd Pairing DHKey Check
79035	411.551	Master_0x9aa2a661	LE 1M	LE LL	23	132021µs	Control Opcode: LL_ENC_REQ
79040	411.684	Slave_0x9aa2a661	LE 1M	LE LL	13	150µs	Control Opcode: LL_ENC_RSP
79045	412.081	Slave_0x9aa2a661	LE 1M	LE LL	1	150µs	Control Opcode: LL_START_ENC_REQ
79046	412.214	Master_0x9aa2a661	LE 1M	LE LL	1	132181µs	Encrypted packet decrypted incorrectly (bad MIC)
79051	412.346	Slave_0x9aa2a661	LE 1M	LE LL	1	150µs	Encrypted packet decrypted incorrectly (bad MIC)
79055	412.612	Slave_0x9aa2a661	LE 1M	LE LL	21	149µs	Encrypted packet decrypted incorrectly (bad MIC)

Fig. 7 Capture of the ECDH key exchange when pairing the FitbitAce 3

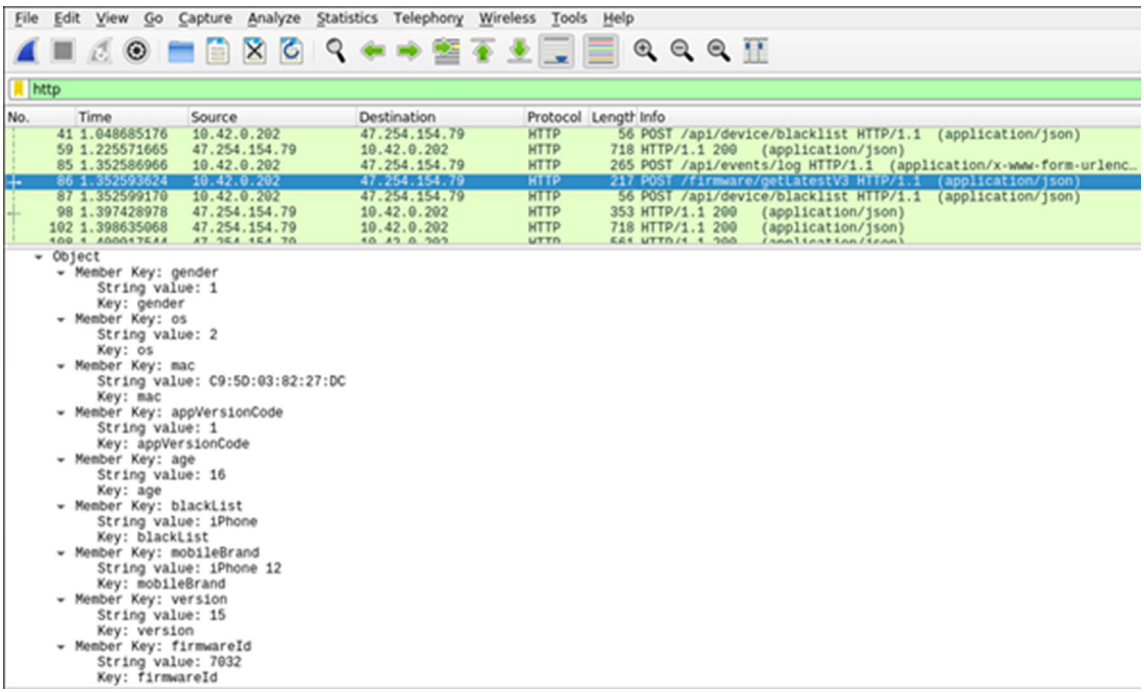


Fig. 8 Graphical description of the information exchanged by VeryFitPro and external servers

data, such as the sex of the user or the MAC address, as shown see Fig. 8. This information is sent to external servers when the user tries to update the device's firmware.

The pairing process in Apple Watch Series 6 is robust and secure (leaving aside inherent Bluetooth problems such as BIAS [27] or KNOB [28]).

4.2.3 Use of dynamic MAC addresses

At the time of our research, except for Apple Watch Series 6, none of the analysed devices used dynamic MAC addresses. If a device's MAC address is static, i.e. does not change on reboot or periodically, and is constantly announced when it is not paired, an attacker could easily identify the wearable device, entailing risk to the user's privacy.

4.2.4 Privacy

Huami's Zepp and Mi Fit apps constantly prompt the user to grant permissions for location, health data and access to the photo album, media content, and other files. Similarly, Huawei Health requests access to location, contacts, calls, notifications, photos, camera, and filesystem. Garmin Jr. must be managed from an adult-controlled account. However, the method used to identify if the user registering the account is an adult is subject to simple multiple-choice questions such as "Which of these (four) workouts is aerobic?". The application requests location permissions to use Bluetooth. The Fitbit app must be used from an account controlled by the child's parents. The application allows the user to switch between two views (minor and adult), access to which is protected by the account password. All the applications mentioned above use Certificate Pinning to prevent fraudulent certificates, so it is impossible to capture HTTPS traffic employing Mitmproxy.

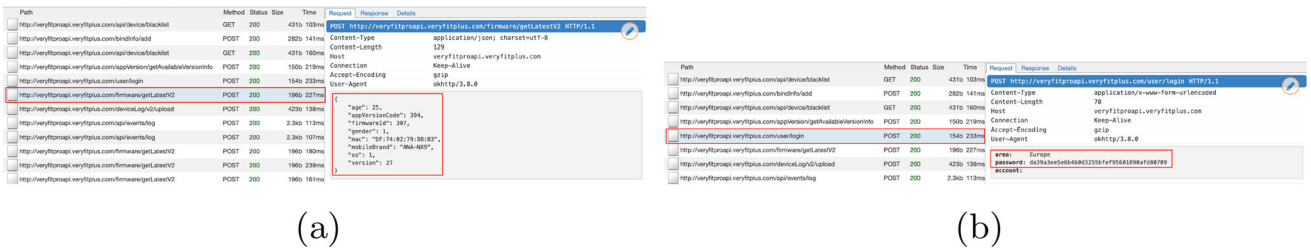
Meanwhile, VeryFitPro, used by the BIGGERFIVE and TOOBUR devices studied, requests permissions for tracking location, access to contacts and messages, and access to the photo album and camera. The privacy policy states that the app collects personal information such as the device's IMEI and exact location and that such information may be shared with third parties. Although the BIGGERFIVE and TOOBUR devices analysed are targeted at minors, the company's privacy policy specifies that the application is not intended for use by minors. Using the Mitmproxy tool, it has been possible to intercept the HTTP/HTTPS traffic of the VeryFitPro application, observing that it sends sensitive information such as the user's age, location and MAC address of the wearable over HTTP, as shown in Fig. 9a. Furthermore, the "Guest" user key is sent in clear text, unencrypted over HTTP, as shown in Fig. 9b. Regarding the privacy of the Apple Watch Series 6, the device is governed by Apple's base agreements and all sensitive information handled is processed securely.

4.3 Summary and comparison of results

Table 5 summarises the results of the tests performed on the selected wearables. The results show that devices from well-known brands such as Fitbit, Garmin or Apple implement more security and privacy measures than devices from smaller companies such as BIGGERFIVE or TOOBUR. Nevertheless, many of them do not encrypt BLE communications or implement pairing methods that do not ensure personal data privacy. This is the case with Garmin Vívofit jr. 2, Mi Band 5, Honor Band 5, and Honor Watch ES. Although they try to obfuscate their communications by using proprietary BLE services and attributes, it has been found on several occasions that these methods had been breached by reverse engineering, and there is publicly accessible information describing their operation.

Interestingly, the only wearables which can prevent MITM and eavesdropping attacks are Fitbit Ace 3 and Apple Watch Series 6 since both implement BLE Secure Connections with ECDH key exchange or secure proprietary exchange methods. All other systems use outdated legacy versions of BLE, with Legacy Pairing methods such as *Just Works* that could allow an attacker to intercept keys and access decrypted traffic. Nonetheless, all devices are susceptible to being attacked by KNOB or BIAS, due to a vulnerability in the Bluetooth architecture in version 5 or prior.

As for fitness apps and their privacy, they all seem to state that they collect sensitive user information in their privacy policies. Moreover, VeryFitPro (used by BIGGERFIVE Fitness and TOOBUR Smartwatch) sends private data over an insecure channel (HTTP), while the rest (well-known brand apps) implement Certificate Pinning on HTTPS/TLS avoiding MITM and eavesdropping attacks with tools like Mitmproxy. Only the applications used by



(a) (b)

Fig. 9 Examples of sensitive information sent by VeryFitPro via HTTP. **a** Age, MAC address, location and model of smartphone **b** Guest account password

Table 5 Comparison of all analysed wearables

		Authentication	Secure pairing method	Encrypted communications	Encryption keys sent encrypted	Dynamic MAC address	Communications and firmware updates over HTTP
High-end devices	Amazfit band 5	✔	✔	✗	No Encryption	✗	✔
	Apple watch series 6	✔	✔	✔	✔	✔	✔
	Fitbit ace 3	✔	✔	✔	✔	✗	✔
	Fitbit inspire 2	✔	✔	✔	✔	✗	✔
	Garmin vívofit jr. 2	✔	✔	✔	✗	✗	✔
	Honor band 5	✔	✗	✗	No Encryption	✗	✔
	Honor watch ES	✔	✗	✗	No Encryption	✗	✔
	Mi band 5	✔	✔	✗	No Encryption	✗	✔
Low-end devices	BIGGERFIVE fitness	✗	✗	✗	No Encryption	✗	✗
	BIGGERFIVE vigor	✗	✗	✗	No Encryption	✗	✗
	TOOBUR smartwatch	✗	✗	✗	✗	✗	✗
	TOOBUR smart band	✗	✗	✗	✗	✗	✗

high-end wearables require user authentication, and in the case of devices specifically designed for minors, only Garmin Jr. and Fitbit apply specific measures to protect minor's data.

By not encrypting either the BLE connection or requests sent over HTTP, VeryFitPro is the most insecure and least private application among those analysed. By inspecting the BLE traffic exchanged between VeryFitPro and the wearable devices connected, we found out that its operation is vulnerable to reverse engineering attacks, regardless of the connected device. Of particular concern is that BIGGERFIVE and TOOBUR Smartwatch devices, designed specifically for minors, indicate in their boxes and manuals that the bands must be used with the VeryFitPro app.

One particularly relevant finding from this research is that all the devices analysed used static MAC addresses, except for the Apple Watch Series 6. The MAC address of a BLE peripheral device is constantly advertised unencrypted when it is disconnected from its central controller, making it vulnerable to being tracked and identified by an attacker.

5 Discussion and recommendations

Considering the results obtained and their analysis, we have found that most low-cost devices carry more security and privacy vulnerabilities. From a security point of view, these low-cost devices lack the authentication and/or encryption means or tools necessary to guarantee the integrity of the devices themselves or the data they handle. For this reason, the privacy of its users is compromised, both due to possible access to sensitive information handled by these devices or because said information is transferred through insecure connections with cloud servers and shared with third-party companies. Thus, low-income families using those low-end devices may be more exposed to security and privacy risks, even more if they are not familiar with technology. In order to avoid this, it should exist regulation that ensures that this kind of devices meet minimum security and privacy requirements.

As mentioned in the introduction to this paper, the precedence of protecting children's privacy has already been enshrined in various regulations around the world. Although most of them show similarities with each other, some present differences in their approach. For instance, it is important to note that while the COPPA, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the UK GDPR allow children as young as 13 to approve the disclosure of their own personal information, the GDPR sets the general age of consent at 16. Other regulations, such as Australia's Privacy Act 1988, do not specify an age after which an individual can make their own privacy decision.

Beside this, it is interesting to offer recommendations with the aim of avoiding or mitigating the effects of the detected vulnerabilities. Furthermore, these recommendations are defined with a general application purpose,

without discerning the device's type, price, manufacturer, or origin. First, users must be aware of the information (personal data) that each device captures during its use. For this purpose, it is necessary to read and understand the privacy policy set by the device or the underlying management application. In addition, it is essential to limit the information shared with the applications, giving access only to the data necessary for their operation, which should be data collected by the wearable device and nothing stored in the smartphone (e.g., location, contacts, pictures, etc.). From the companies' side, concise and easy to understand information must be given to the user, especially when data is being shared with third parties or used for a purpose that the user has not approved.

Second, it is critical to use well-configured profiles to interact with the devices and management applications. For example, using a different username and password is highly recommended than the defaults for each application (using key rings to safeguard more complex keys).

From the point of view of configuring the devices, it is essential to give them an identifying name and hide their MAC address whenever possible. A representative name facilitates unequivocal identification for pairing with the right device on the local network. Furthermore, since the definition of BLE in the Bluetooth 4.0 core specification, privacy capabilities have been defined to safeguard user and peripheral privacy. The BLE Privacy feature allows for the MAC address within the advertising packets to be replaced with a random value that changes at timing intervals determined by the manufacturer and permits hiding the device's actual MAC address. A cryptographic Identity Resolution Key (IRK) will allow explicitly trusted devices to find and connect to the peripheral.

The importance of protecting devices against user tracking through BLE connections is reflected by the existence of several techniques and attacks that can allow for an attacker to gain private information by passively observing the communication between smartphone and wearable device [11]. These include user tracking as well as user activity detection techniques [29]. On the one hand, an attacker can pretend to be a peripheral device by looking for UUIDs or spoofing GATT profiles, and track a user whenever the smartphone application tries to connect with it. This can be used to track users in crowded places or in their homes, as well as cross-app tracking [30]. On the other hand, an attacker can detect a user's activity such as walking or running by sniffing BLE traffic between their wearable and smartphone, even when communications are encrypted [11]. In some cases it is also possible to determine the heart rate sensor data by observing the Received Signal Strength Indicator (RSSI) [31].

Another crucial factor necessary to guarantee the security and privacy of wearable devices is the implementation of up-to-date protocols that incorporate secure methods aimed to safeguard user information. As presented in this paper, although Bluetooth core specification defines secure pairing methods and features such as LE Secure Connections since version 4.2, most vulnerabilities were related to outdated or inadequate configurations of the BLE protocol. In this regard, devices that use outdated versions of BLE or LE legacy pairing methods should improve privacy and security by using LE Secure Connections and ECDH cryptography.

As shown in the previous section, it is also possible to prevent sensitive data interception via HTTP by implementing HTTPS and other defenses such as Certificate Pinning or by warning the user about new and untrusted certificates. These countermeasures are not effective against MITM attacks, however, as some techniques exist that can circumvent them. Such is the case of the Rogue Access-Point (RAP) or Evil Twin attack, that allows an attacker to impersonate legitimate Wi-Fi networks and can be carried out with low cost devices such as a Raspberry Pi and open source tools like the Kali Linux distribution. As a token of its importance, RAP attack detection has been and are still a source of concern [32–34]. In cellular networks, MITM attacks can be carried out via analogous attacks to hijack communication such as the IMSI Catcher or false base station attack [35, 36].

6 Conclusions

In this paper, we presented a set of tests for analysing security and privacy risks in wearable devices. Using such set of tests, we evaluated the vulnerability problems associated with prevalent wearable devices, especially those targeting children and young people. We also provided some recommendations for risk avoidance and mitigation.

The results obtained during the tests show that, although devices from well-known brands tend to apply more security and privacy measures than devices from smaller companies, such as BIGGERFIVE or TOOBUR, many of them were found not to encrypt BLE communications or implement pairing methods that do not ensure the privacy of user data.

The only wearable devices found to successfully encrypt BLE traffic using BLE Secure Connections with ECDH key exchange are Fitbit Ace 3 and Apple Watch Series 6. All other systems use outdated legacy versions of BLE, with Legacy Pairing methods such as Just Works, allowing an attacker to intercept the cryptographic keys and access the unencrypted traffic. Some of these devices, such as the Garmin Vívofit jr. 2 or the Mi Band 5, were found to rely on obfuscation methods using proprietary BLE services and attributes to mitigate eavesdropping attacks and allow

the user to use third-party apps. It has been noted that these methods have been breached through reverse engineering on several occasions and that there is publicly available information describing how they work.

Regarding the applications used by the wearable devices, the higher-end devices connect to a proprietary application of its company, while lower-end devices can be linked to third-party applications. All applications designed by high-end companies use Certificate Pinning on HTTPS/TLS to avoid MITM and eavesdropping attacks with Mitmproxy. Lower-end devices use third-party applications such as VeryFitPro that send sensitive information over HTTP and are neither secure nor private. Of the devices studied that are designed specifically for children, Garmin's Vívofit jr. 2 is vulnerable to active and passive eavesdropping and MITM attacks. Furthermore, low-end devices, such as the TOOBUR Smartwatch and the BIGGERFIVE Fitness, are targeted at minors while being the most vulnerable among the systems analysed.

Another particularly relevant finding of this research is the use of static MAC addresses by all the devices analysed in the tests, except for the Apple Watch Series 6. Given that one of the objectives of this research is the analysis of wearable devices targeted at minors, this vulnerability is particularly worrying. As mentioned in this paper, specific measures are defined in the BLE specification that allows for the use of private and random addresses that change periodically, so manufacturers can easily avoid this vulnerability.

All in all, the results obtained in this research illustrate that, as cybersecurity guru Bruce Scheneier brilliantly exposed in the keynote he delivered in RSA2017 entitled "Regulating the Internet of Things" [37], IoT manufacturers do not have clear incentives to include security and privacy features, so regulation and law enforcement are needed to guarantee that commercial IoT devices meet appropriate security and privacy requirements, being especially important when such devices are targeted at vulnerable groups such as minors.

Finally, we would like to emphasize that, while only applied to wearable devices used by minors for the purposes of our research, the set of tests proposed in this paper, including the testing methodology and tools, have been designed and chosen to be general enough as to be able to be applied to any kind of IoT device used in a similar scenario as the one described in sect. 3.1. Even though the analysis side of our research has focused on devices aimed to minors, the application of the testing methodology to other IoT devices as those found in the home, vehicle, building, and industrial facilities, as well as to products used by adults, could yield a far larger crop of issues beyond those found in wearables.

Acknowledgements This work has been funded by the Horizon 2020 program of the European Union through the RAYUELA project (contract no. 882828). The content of the article reflects the views only of the authors. The European Commission is not responsible for any use that may be made of the information contained therein. The authors have no relation with the manufacturers of the analysed wearables. The analysed wearables were bought and have been exclusively used for research purposes. No human beings have been involved in the experiments except from the researchers who carried out the experiments themselves, so the data managed by the wearables is fake data and thus does not represent sensitive data at all. The manufacturers of the analysed devices have been duly informed about the findings and their publication as a scientific paper in Wireless Networks. At the time of the publication of the paper, we have received answer to such a communication from two manufacturers (Apple and Huawei). We would like to acknowledge their interest and commitment to security and privacy.

Data availability The manuscript has no associated data.

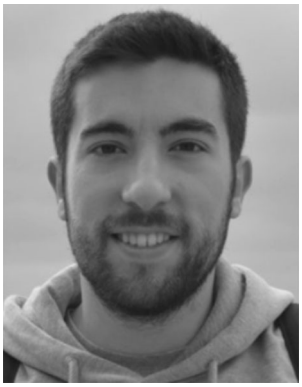
References

1. Laricchia, F. (2022). Wearables unit shipments worldwide by vendor from 1st quarter 2014 to 3rd quarter 2021. https://www.statista.com/statistics/435933/quarterly-wearables-shipments-worldwide-by-vendor/, February 2022.
2. Gartner. (2021). Gartner forecasts global spending on wearable devices to total \$81.5 billion in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-01-11-gartner-forecasts-global-spending-on-wearable-devices-to-total-81-5-billion-in-2021/, January 2021.
3. BusinessWire. (2022). Global wearable technology market trends & analysis report 2021-2028: Adoption of fitness trackers and health-based wearables is anticipated to propel growth, 2022.
4. WatchOut: Analysis of smartwatches for children. Technical report, Forbrukerrådet, 2017.
5. Bundesnetzagentur (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway). Bundesnetzagentur takes action against children's watches with "eavesdropping" function, 2017. Press Release.
6. Velykoivanenko, L., Niksirat, K.S., Zufferey, N., Humbert, M., Huguenin, K., & Cherubini, M. (dec 2022). Are those steps worth your privacy? fitness-tracker users' perceptions of privacy and utility. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, *5*(4).
7. Kang, H., & Jung, E. H. (2021). The smart wearables-privacy paradox: A cluster analysis of smartwatch users. *Behaviour & Information Technology, 40*(16), 1755–1768.

8. Olmstead, K., & Smith, A. (2017). *Americans and Cybersecurity*. Technical report, Pew Research Center.
9. Hilts, A., Parsons, C., & Knockel J., (2016). Every step you fake: A comparative analysis of fitness tracker privacy and security. Technical report, Open effect.
10. Zuo, C., Wen, H., Lin, Z., & Zhang, Y. (2019). Automatic fingerprinting of vulnerable ble iot devices with static uuids from mobile apps. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pp. 1469-1483, New York, NY, USA. Association for Computing Machinery.
11. Das, A.K., Pathak, P.H., Chuah, C.-N., & Mohapatra, P. (2016) Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, HotMobile '16, pp. 99-104, New York, NY, USA, 2016. Association for Computing Machinery.
12. Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., et al. (2017). A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials, 19*(4), 2573–2620.
13. Bluetooth SIG. *Bluetooth core specification*, 12 2019. Rev. 5.2.
14. Snader, R., Kravets, R., & Harris, A.F. (2016). Cryptocop: Lightweight, energy-efficient encryption and privacy for wearable devices. In *Proceedings of the 2016 Workshop on Wearable Systems and Applications*, WearSys '16, pp. 7–12, New York, NY, USA. Association for Computing Machinery.
15. Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2017). Guide to bluetooth security, 2017-05-08 00:05:00.
16. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal, 6*(5), 8182–8201.
17. Ryan, M. (2013). Bluetooth: With low energy comes low security. In *7th USENIX Workshop on offensive technologies (WOOT 13)*, Washington, D.C. USENIX Association.
18. Zegeye, W.K. (2015). Exploiting bluetooth low energy pairing vulnerability in telemedicine. In *International Telemetering Conference Proceedings. International Foundation for Telemetering*.
19. Rosa, T. (2013). Bypassing passkey authentication in bluetooth low energy. Cryptology ePrint archive, Paper 2013/309. https://eprint.iacr.org/2013/309.
20. Langone, M., Setola, R., & Lopez, J. (2017). Cybersecurity of wearable devices: An experimental analysis and a vulnerability assessment method. In *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 2, pp. 304–309.
21. Reardon, J., Feal, Á., Wijesekera, P., On, A.E.B., Vallina-Rodriguez, N., & Egelman, S. (2019). 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *28th USENIX Security Symposium (USENIX Security 19)*, pp. 603–620, Santa Clara, CA. USENIX Association.
22. Feal, Á., Calciati, P., Vallina-Rodriguez, N., Troncoso, C., Gorla, A., et al. (2020). Angel or devil? a privacy study of mobile parental control apps. In *Proceedings of Privacy Enhancing Technologies (PoPETS)*.
23. Reyes, I., Wijesekera, P., Reardon, J., Elazari Bar On, A., Razaghpanah, A., Vallina-Rodriguez, N., Egelman, S. et al. (2018). "Won't somebody think of the children?" examining coppa compliance at scale. In *Proceedings of Privacy Enhancing Technologies Symposium (PETS)*.
24. Solera-Cotanilla, S., Vega-Barbas, M., Pérez, J., López, G., Matanza, J., & Álvarez Campana, M. (2022). Security and privacy analysis of youth-oriented connected devices. *Sensors, 22*(11), 3967.
25. Ojha, Y. (2018). I hacked MiBand 3, and here is how I did it. Part I. https://medium.com/@yogeshojha/i-hacked-xiaomi-miband-3-and-here-is-how-i-did-it-43d68c272391. Medium Blog.
26. Rai, P. (2020). How To use Mi band 5 without The Mi fit app, 2020. TechWiser Blog.
27. Antonioli, D., Tippenhauer, N.O., & Rasmussen, K. (2020). Bias: Bluetooth impersonation attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 549–562.
28. Antonioli, D., Tippenhauer, N.O., & Rasmussen, K.B. (2019). The KNOB is broken: Exploiting low entropy in the encryption key negotiation of bluetooth BR/EDR. In *28th USENIX Security Symposium (USENIX Security 19)*, pp. 1047–1061, Santa Clara, CA, Aug. 2019. USENIX Association.
29. Barua, A., Al Alamin, M. A., Hossain, M. S., & Hossain, E. (2022). Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society, 3,* 251–281.
30. Korolova, A., & Sharma, V. (2018). Cross-app tracking via nearby bluetooth low energy devices. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, CODASPY '18, pp. 43-52, New York, NY, USA. Association for Computing Machinery.
31. Soderi, S. (2019). Cybersecurity assessment of the polar bluetooth low energy heart-rate sensor. In L. Mucchi, M. Hämäläinen, S. Jayousi, & S. Morosi (Eds.), *Body area networks: Smart IoT and big data for intelligent health management* (pp. 252–265). Cham: Springer International Publishing.
32. Beyah, R., & Venkataraman, A. (2011). Rogue-access-point detection: Challenges, solutions, and future directions. *IEEE Security & Privacy, 9*(5), 56–61.
33. Lin, Y., Gao, Y., Li, B., & Dong, W. (2020). Accurate and robust rogue access point detection with client-agnostic wireless fingerprinting. In *2020 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 1–10.
34. Igarashi, K., Kato, H., & Sasase, I. (2021). Rogue access point detection by using arp failure under the mac address duplication. In *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1469–1474.
35. Palamà, I., Gringoli, F., Bianchi, G., & Blefari-Melazzi, N. (2021). Imsi catchers in the wild: A real world 4g/5g assessment. *Computer Networks, 194,* 108137.
36. Piqueras Jover, R., & Marojevic, V. (2019). Security and protocol exploit analysis of the 5g specifications. *IEEE Access, 7,* 24956–24963.
37. Schneier, B. (2017). Regulating the internet of things. https://www.youtube.com/watch?v=b05ksqy9F7k. RSA Conference.

Jaime Fúster received the double M.Sc. in Telecommunications Engineering and Cybersecurity from the ICAI Engineering School of Universidad Pontificia Comillas in 2021. During his Master's studies, he conducted research within the framework of the EU H2020 project RAYUELA. During 2021-2022, he enjoyed a prestigious "Vulcanus in Japan" scholarship working for Rakuten on security in 5G networks.

Sonia Solera-Cotanilla was born in Cuenca, Spain, in 1996. She received the B.S. and M.Sc. in Telecommunication Technologies and Services Engineering from Universidad Politécnica de Madrid (UPM), Spain, in 2018 and 2020, respectively. Currently, she is pursuing a Ph.D. in Telecommunications Engineering at UPM. During her Master's studies, she obtained a research grant in the Telecommunications and Internet Networks and Services research group at the UPM. She is currently a researcher within this research group, working in the field of the Internet of Things, Smart Cities, and Cybersecurity. Her areas of interest are Mobile Communication Networks, Big Data, Smart Cities, Data Analytics and Visualization, the Internet of Things, and Network Monitoring.



Jaime Pérez received the B.S. and the M.Sc. degree in Telecommunications Engineering from Universidad Politécnica de Madrid (UPM), Spain, in 2018 and 2021, respectively. During his Master's studies (2018-2020), he worked as research assistant in the Laboratory of Integrated Systems at the ETSIT UPM developing research about energy optimization in data centers using Machine Learning and Deep Learning techniques. Currently, he is pursuing a Ph.D. in Engineering Systems Modeling at Universidad Pontificia Comillas. He is a member of the Institute for Research in Technology of the ICAI Engineering School, researching in the intersection between Artificial Intelligence and Serious Games within the framework of the EU H2020 project RAYUELA. His areas of interest are Serious Games, Machine Learning, Deep Learning, and Applied Artificial Intelligence.

Mario Vega-Barbas was born in Guadalajara, Spain, in 1984. He received the B.S. and M.Sc. degrees in Computer Science from Universidad de Alcalá (UAH), Spain, in 2009, and the Ph.D. in telematics and in applied medical technology from Universidad Politécnica de Madrid (UPM), Spain, and the KTH-Royal Institute of Technology, Sweden, in 2016. He is currently an Associate Professor and a Senior Researcher within the Telecommunication and Internet Networks and Services research group at UPM. Previously, he has been a Postdoctoral Researcher with the Institute of Environmental Medicine, Karolinska Institute, and Medical Sensors, Signals and Systems, KTH, Sweden. Assoc. Prof. Vega-Barbas has authored or co-authored more than 30 publications, including books, book chapters, journal articles, and conference papers. His research interests include data analysis and visualization, ubicomp, pervasive sensitive services, cybersecurity, user-oriented security, and the development of the IoT.

Rafael Palacios was born in Madrid, Spain, in 1966. He received the B.S. and M.S. degrees in mechanical engineering from the ICAI School of Engineering, Comillas Pontifical University, Madrid, in 1990, and the Ph.D. degree from Comillas Pontifical University, in 1998. He joined the Department of Electronics, ICAI School of Engineering, as an Assistant Professor, and the Institute for Research in Technology, as a Researcher, in 1998. He obtained, a Tenure, in 2004, and became a Full Professor, in 2020. He has been the Head of the Programs in telecommunications engineering and computer science since 2012. He also helped to create the master's program in cybersecurity and was the coordinator from 2019 to 2021. From 2001 to 2002, from 2009 to 2010, and from 2017 to 2018, he was a Visiting Professor with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA. He carried out research with the Department of Aeronautics and Astronautics, Sloan School of Management, and the MIT Energy Initiative.

Manuel Álvarez-Campana is an Associate Professor at Universidad Politécnica de Madrid (UPM). He received a Telecommunication Engineer degree in 1989 and a PhD in Telecommunication Engineering in 1995, both from UPM. He has participated in several projects within the framework of European and Spanish public funded R &D programs, as well as in consultancy contracts for private companies and public organizations. His professional interests cover a broad spectrum of aspects related to communication networks and services. His main current lines of work are Mobile Communication Networks, Cybersecurity, the Internet of Things and Smart Cities. He is author of more than 70 technical publications in journals and conferences, and three books.

Gregorio Lopez received his Ph.D. in Telecommunications Engineering from Universidad Carlos III de Madrid (UC3M) in 2014. He currently works as Assistant Professor in the ICAI Engineering School of Comillas Pontifical University, where he also serves as the coordinator of the Cybersecurity MSc, and as Senior Researcher in the Institute for Research in Technology. He gathers wide experience in close-to-market research gained through his participation in more than ten national and European research projects. As a result of his research activity, he holds an European Patent and has published more than twenty papers in top-tier conferences and journals. His current research interests revolve around the optimization of Machine-to-Machine (M2M) communications networks based on analysis and simulation, cybersecurity, and data analytics for the Internet of Things (IoT), and the use of technology and the Internet, being currently the coordinator of the European H2020 project RAYUELA (empoweRing and educAting YoUng pEople for the Internet by pLAying), which addresses this latter topic.