RAYUELA
a fun way to fight cybercrime

Deliverable Report

D2.3 Open Report on Methodology, tools and results of testing security and privacy risks of connected devices

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 882828. The sole responsibility for the content of this document lies with the author and in no way reflects the views of the European Union.

Document Contributors

Deliverable No.	2.3	Work Package No.	2	Task/s No.	T2.2, T2.3, T2.4
Work Package Title	Technology assessment and IT threat landscape				
Linked Task/s Title	Vulnerability tests and risk assessment of security issues linked to connected devices (T2.2.), IT threat landscape: identification of most common online threats for children and young adults (T2.3.), and Accounting for the rise of Cybercrime-as-a-Service models exploiting IoT vulnerabilities (T2.4.)				
Status	Final	(Draft/Draft Final/Final)			
Dissemination level	PU	(PU-Public, PP, RE-Restricted, CO-Confidential)			
Due date deliverable	31/03/2022	Submission date		31/03/2022	
Deliverable version	3.0				

Deliverable responsible	Universidad Politécnica de Madrid		
Contributors	Organization	Reviewers	Organization
Mario Vega	UPM	Lynne Henderson	PSNI
Sonia Solera	UPM	Aivars Bērziņš	TILDE
Manuel Álvarez-Campana	UPM	Violeta Vázquez	ZABALA
Gregorio López	COMILLAS		
Jaime Pérez	COMILLAS		
Javier Matanza	COMILLAS		
Carlos Rodríguez-Morcillo	COMILLAS		
Francisco Javier Herraiz	COMILLAS		
Rafael Palacios	COMILLAS		
Ruben Fernández Bleda	PLV		
José Ángel Olivares	PLV		
Ingrid Borarosova	BPI		

Pedro Vicente	PJ		
Lynne Henderson	PSNI		
Lauri Tamm	EPGB		

Document History

Version	Date	Comment
1.0	15/10/2021	Document skeleton
2.0	11/03/2022	Final version before external review
3.0	24/03/2022	Final version ready for submission

TABLE OF CONTENT

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Description
BIAS	Bluetooth Impersonation Attacks
BLE	Bluetooth Low Energy
CaaS	Cybercrime-as-a-Service
COPPA	Children’s Online Privacy Protection Act
DDos	Distributed Denial of Service
DoS	Denial of Service
EUROPOL	European Union Agency for Police Cooperation
GDPR	General Data Protection Regulation
GSM	Global System for Mobile communication
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICT	Information and Communication Technology
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
KNOB	Key Negotiation of Bluetooth
LEA	Law Enforcement Agency
LTE	Long Term Evolution
MitM	Man-in-the-Middle
NFC	Near Field Communication
SPA	Smart Personal Assistant
SQL	Structured Query Language

Abbreviation	**Description**
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SWOT	Strengths, Weaknesses, Opportunities and Threats analysis
TLS	Transport Layer Security
WPA	Wi-Fi Protected Access

Disclaimer

This document is part of an internal deliverable of the RAYUELA project, funded by the European Union's Horizon 2020 research and innovation program under grant agreement No 882828.

The sole responsibility for the content of this document lies with the authors and in no way reflects the views of the European Union. In particular, the tests performed in the context of this document have taken place in the project partners' own laboratories, always under the necessary expert supervision and in a controlled and prepared environment. It is therefore impossible to identify real end users in any of our test results.

No personal comments or opinions of the researchers are included in this document, only the results obtained from a set of tests are presented and compared. And in no way has any kind of benefit been obtained from any brand of connected device to expose beneficial or detrimental results to that or other brands. The reader is encouraged to understand the exposed tests as the result of research in controlled environments. In the event of wishing to replicate any of the tests performed, the researchers are not responsible for any misuse of the information provided.

Executive Summary

This deliverable is included in WP2, which is focused on technology assessment and IT threat landscape. Specifically, this deliverable is the result of the work carried out in tasks T2.2, T2.3, and T2.4. These tasks are mainly related to three aspects:

- Conducting vulnerability tests and risk assessment of security issues linked to connected devices (T2.3);
- Study of the IT threat landscape, focusing on the identification of most common online threats for children and young adults, and, in particular for this case, on how human factors may influence the impact of technological risks and threats (T2.3);
- Accounting for the rise of CaaS models exploiting IoT vulnerabilities. (T2.4)

Thus, the main objective of this document is to describe and explain a methodology for the evaluation of security and privacy risks in IoT devices, as well as a catalogue of vulnerabilities in IoT devices frequently used by children and young people and some recommendations for risk mitigation. In addition, to support the methodology, this document exposes a set of interesting tools for testing security and privacy vulnerabilities in the context of the IoT. As an additional source of data, the paper includes a dedicated section for the analysis of attacker behaviour by designing and deploying an IoT honeypot. The methodology developed, the tests performed, and the results obtained along with the recommendations offered are stored in an open access platform for public consultation. Furthermore, next to purely technological aspects, the work done also consider human factors affecting such technological vulnerabilities and their exploitation in new CaaS models.

The results show that generic and more affordable devices are more prone to attack due to security and privacy vulnerabilities. The fact that these devices are cheaper is also, partly, because they use third-party applications to manage the information collected. These applications are often hosted in countries with dubious or less restrictive data protection policies. This, together with the human factors that have the highest correlation with possible cybersecurity attack vectors (External locus of control, Learned Helplessness, Careless Privacy Attitude or Low Perception of Risk), has been reflected in the creation of a socioeconomic framework for the provision of tools and applications to offer personalized services for taking advantage of CaaS.

Introduction

As a starting point for this project, an analysis of security and privacy of connected devices has been carried out as part of previous tasks outside this development. This analysis concludes with the top ten security and privacy issues associated with the use of IoT technology and connected devices by minors. As experts, we must address and analyse these problems from a technological or engineering perspective and by studying human and socio-economic factors that influence the appearance, development and establishment of these problems and the underlying threats. Therefore, it is necessary to analyse these problems from three specific points of view: technological, psychological, and socio-economic.

This document is organised into three well-differentiated sections. Section 1 focuses on outlining the testing methodology developed to assess the security and privacy problems of connected devices commonly used by minors. It also offers a series of recommendations to try to mitigate the impact of those threats. As an additional source of information about how attackers behave, a computer security mechanism, i.e., honeypot, has been included in addition to the tests performed following the proposed methodology. All the information is presented on an Open Access Platform where access is also provided to a tool developed for testing devices. For its part, section 2 analyses the human factors involved in supporting the security and privacy problems identified. Finally, section 3 focusses on the CaaS issue, analysing how services are developed to exploit socio-economically the vulnerabilities associated with the security and privacy problems of IoT devices analysed before.

1 Vulnerability tests and risk assessment of security issues linked to connected devices

1.1 Design testing method

From the results obtained in previous tasks and already mentioned in the document, there is a categorization of the devices most used by young people and on which the associated security and privacy problems have been investigated. This document includes a list of specific devices of interest to the project on which the tests described here have been performed. The following sections describe the testing methodology for the security and privacy analysis applied to the selected devices.

1.1.1 Test scenario

The operating and communication scheme commonly used by all current IoT devices underlies the evaluation scenario. An element with high computing capacity acts as an intermediary (hub, configurator, etc.) with external servers. Depending on the IoT device, BLE or the user's Wi-Fi hotspot, supports the communication with the master or hub. For its part, this scenario uses a wireless link to implement the communication between the master element or. Finally, special attention has been paid to the user interaction with specific devices when they use voice commands. Figure 1 shows the organization of the test scenario used in the proposed security and privacy assessment.

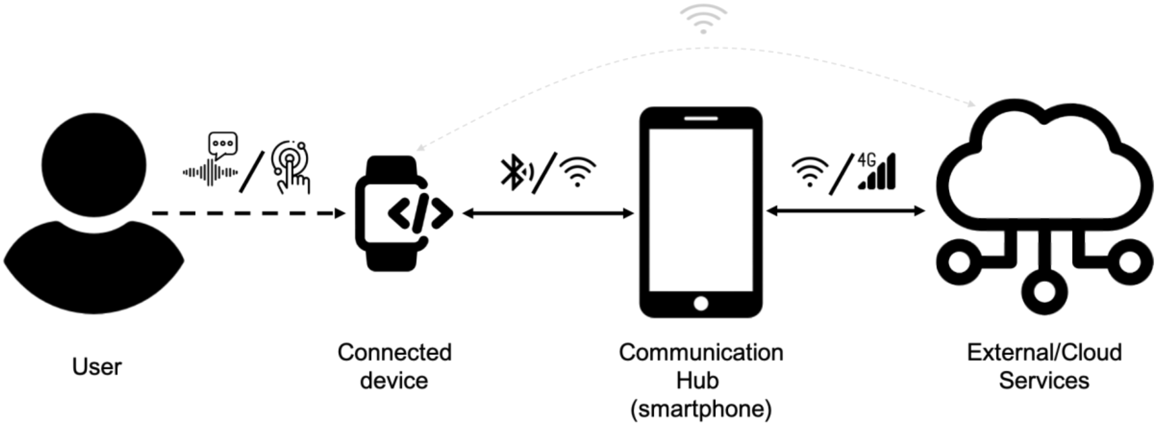


Figure 1. Testing scenario overview.

This scenario shows three areas of analysis: one focused on user-connected device interaction, a second one on communication between the connected device and the communications hub, and a third one on studying the communication process between external servers or third-party applications and the hub system. Each analysis area will define a case study to examine the security and privacy issues by defining specific tests. In the case of LTE communication between the communication hub and external/cloud servers is out of the scope of this analysis due to the cost associated with the LTE/GSM monitoring tools and the underlying legal aspects.

1.1.2 Testing tools

The analysis of the communications carried out within the defined scenario focuses on studying all the information packets emitted by the devices involved in each test. Thus, Wireshark was used as the default software tool, both for the analysis of BLE and Wi-Fi packets. Wireshark is a communications packet analyser widely used in telecommunications, both academically and for research. In addition, it is an open-source and cross-platform tool, which facilitates its adaptation to the finally selected hardware tools (plug-ins and addons) as well as to different operating systems. The next sections describe the remaining hardware and software tools used to perform the planned tests.

1.1.2.1 Bluetooth

To be able to intercept the BLE communication between the peripheral device and the master, a tool capable of correctly capturing and interpreting the exchanged packets was required. Among the main sniffer devices available on the market and shown in Figure 2, the Nordic Semiconductor nRF52 DK was chosen due to its radio characteristics, ease of use and versatility, as it is programmable and can be used as a development kit as well as a sniffer.

Table 1. Bluetooth sniffing and analysers tools: a comparative.

Device	**Characteristics**	
	Pros	Cons
Bluefruit LE Sniffer	Wireshark compatible Easy to use	BLE only 1 listening channel
nRF52 DK	Wireshark compatible Programmable Debugging BLE, Bluetooth mesh, NFC, and ANT	1 listening channel
nRF52840 DK	Wireshark Compatible Programmable Debugging Bluetooth LE, Bluetooth mesh, NFC, Thread and Zigbee	1 listening channel
nRF52840 Dongle	Wireshark Compatible Low-cost Small Easy to use	Low range Fewer functionalities compared to nRF52840 and nRF52

	Bluetooth 5, Bluetooth mesh, Thread and Zigbee	1 listening channel
CC2540EMK-USB	Wireshark Compatible	1 listening channel
Ubertooth One	Wireshark Compatible Programmable Open Source Long Range	Hard to configure Packet loss 1 listening channel
HackRF One	Generic SDR: Bluetooth and more protocols	Can sniff BLE traffic, but it is hard to implement due to frequency hopping

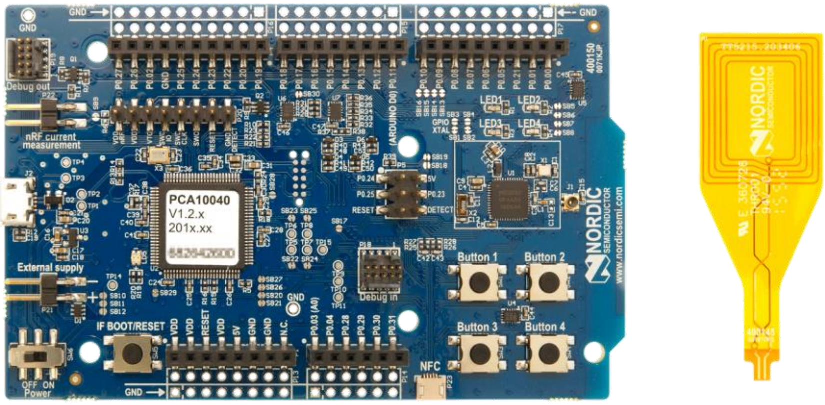


Figure 2. Nordic Semiconductor's nRF52 DK.

Finally, to implement the "BLE ping of death" attack we have used Bluez, the Linux's Bluetooth stack. Specifically, we have used the L2ping tool to ping a Bluetooth device. To support the L2ping request system, an Ubuntu 20.04.2.0 operating system (Canonical Ltd., London, UK) installed on a RaspberryPi 4 model B (Raspberry Pi Foundation, London, UK) was used.

1.1.2.2 Wi-Fi

The hardware tools used to sniff and analyse the Wi-Fi signal are the TP-Link TL-WN722N (TP-Link Technologies CO. LTD, Shenzhen, PRC) antenna and the Alfa AWUS036ACH (Alfa network Inc., Taiwan, PRC) antenna. To trace out what data is sent between the fitness wristband application and the servers of each company, the packets emitted by the mobile applications were captured using *mitmproxy*.

mitmproxy is an open-source tool that provides an interactive proxy with SSL/TLS capability to intercept HTTP/1, HTTP/2 and WebSockets. It allows for real-time interception and analysis of HTTP and HTTPS requests and responses sent from a mobile device or an external server, making the computer where it is installed function as an HTTP proxy for the smartphone's connections. Figure 3 and Figure 4 illustrate how *mitmproxy* works.

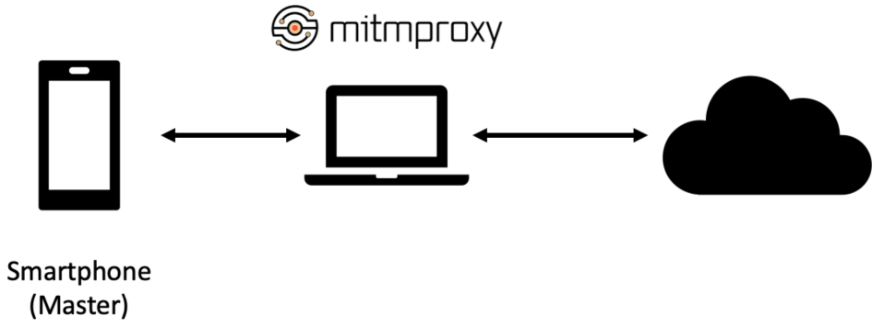


Figure 3. System overview with *mitmproxy* as middle proxy between the communication hub and external servers.

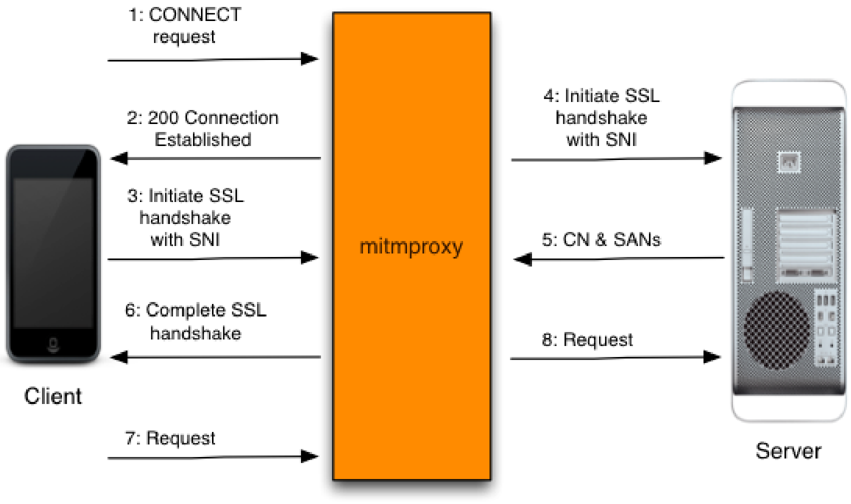

1: CONNECT request
2: 200 Connection Established
3: Initiate SSL handshake with SNI
6: Complete SSL handshake
7: Request
Client
mitmproxy
4: Initiate SSL handshake with SNI
5: CN & SANs
8: Request
Server

Figure 4. Behaviour of *mitmproxy*.

To protect the integrity and confidentiality of transmitted data, HTTPS uses TLS/SSL to encrypt data end-to-end. Therefore, to successfully intercept HTTPS traffic transmitted between a mobile and an external server, it is necessary to install a customized root certificate on the device. *mitmproxy* uses a self-created certificate that will be trusted by the mobile being analysed. In this way, it implements MitM attack against the application and the encrypted content of messages exchanged can be captured in clear text.

1.1.2.3 Hotspot virtualization

One way to control a Wi-Fi-based communication environment is by creating a virtual hotspot, as shown in Figure 5. In this sense, we have created an environment composed of a TP-Link TL-WN722N antenna (TP-Link Technologies CO. LTD, Shenzhen, PRC) and an Ubuntu 20.04.2.0 operating system (Canonical Ltd., London, UK) virtualized through VirtualBox (Oracle Co., CA, USA). Finally, the Wireshark tool was the tool selected to perform the Wi-Fi traffic analysis.

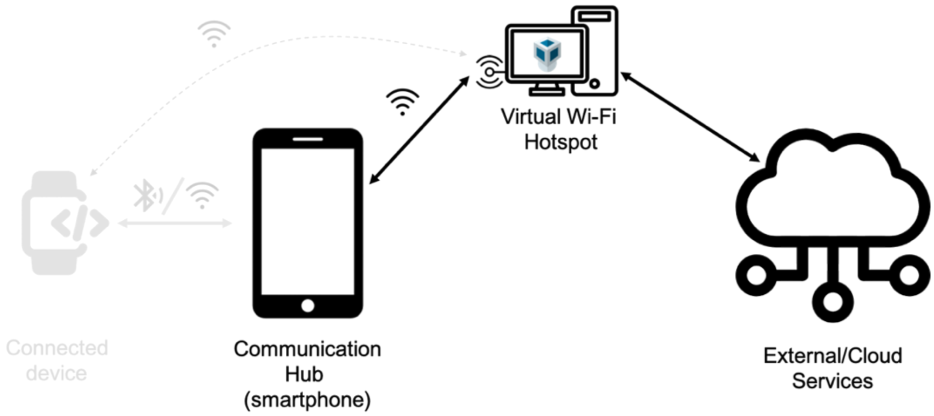


Figure 5. Virtualized hotspot overview.

1.1.3 List of tests

1.1.3.1 Wearables

An overview of the range of tests chosen for the analysis of the devices is given below, with a brief description of each one, as the Table 2 shows:

- Authentication: the application associated with the wearable implements a method to authenticate the user's identity.
- Insecure pairing method: the link between the wearable and the mobile device uses a pairing method considered insecure or ineffective against MitM or passive eavesdropping attacks and lacks privacy safeguards:
  - "Just Works" does not provide any protection against MitM and eavesdropping attacks[1].
  - "Numeric Comparison" does not protect against eavesdropping.
  - "Passkey" does not protect a device against eavesdropping in BLE v 4.2 [1], [2].
- Unencrypted Communications: the BLE communication between the wearable device and smartphone is not encrypted.
- Encryption keys sent in plain text: during the pairing process, the wearable and mobile devices exchange encryption keys in a format that can be easily captured and processed by the BLE sniffer.
- Static MAC address: the wearable uses a static MAC address (i.e., it does not change when the device is turned off or restarted), exposing it to tracking and user identification attacks.

[1] https://www.bluetooth.com/specifications/specs/core-specification/

- Transmission of sensitive information to third-party servers: the fitness application sends sensitive user information to third-party servers.
- Sending of information and firmware updates via HTTP: The application receives firmware updates and sends requests with sensitive information using HTTP without TLS.

Table 2. Security and privacy issues and tests mapping. (1) Authentication, (2) Insecure pairing method, (3) Unencrypted communications, (4) Encryption keys sent in clear text, (5) Static MAC address, (6), Transmission of sensitive information to third-party servers, (7) Sending information and firmware updates over HTTP.

WEARABLES	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Spoofing	x		x	x	x		x
Lack or weak encryption			x				x
Lack or weak authentication	x						
Uncontrolled voice interaction							
Code injection	x						
Data interception		x	x	x	x		x
Takeover	x		x	x	x		
User data being compromised			x		x		
Violation of privacy laws			x			x	
Lack of Control and Understanding						x	

1.1.3.2 Smart Personal Assistants

The feature tests were divided into four categories, covering the different stages of the interaction of a user with the device and the possible security and privacy adjustments that can be made. With these domains, the aim was to obtain a global overview about security and privacy in SPA, focusing the study on common configuration aspects, and actions that a person can perform on the devices.

- Installation. These tests cover both the installation of the device with the SPA itself and the registration of new accessories and third-party skills.
    - Installation process of the SPA. It was studied how the installation of the personal assistant was carried out, which additional devices and applications are necessary, and what configurations can be performed.

  - Installation of new connected devices. The installation process of accessories connected to the assistant is examined and which permissions or configurations can be set to restrict their use.
  - Installation of third-party skills. The installation process of third-party skills or developments to be invoked from the assistant was analysed if the SPA had this functionality available.
- Interaction. Analyses that cover the possible options that a user has for managing the interaction with the SPA, with connected devices and third-party skills.
  - Interaction with the SPA and connected devices. Checks how a user can control the interaction with the assistant and the connected accessories.
  - Interaction with third-party skills. It is analysed if there are controls that allow to define use profiles for third-party skills incorporated to the assistant.
- Functionality. Tests covering options to control assistant functionalities, such as payments or multimedia content playback.
  - Payments and transactions. The possibility of making payments from the assistant is studied, verifying the configurations and restrictions that a user can define.
  - Possibility of creating "safe" profiles for minors. It was checked if the assistants have options to create restricted profiles for minors in an easy manner, therefore allowing for control of multimedia content that is played by the assistant, the accessories with which it can interact, payments that can be made, etc.
- Privacy and security. This category includes tests that evaluate the security features of the assistant, as well as the options that a person has to control the use of his/her personal information.
  - Control of answers containing personal information. Assistants can include users' personal information as responses to some of the requests. This test evaluates if a user can control the sharing options of his personal information.
  - Authentication methods. The authentication methods available in the assistants are analysed, as well as their real effectiveness.
  - Non-human voice filtering. It is checked whether the assistant is susceptible to be activated by voices of artificial origin, such as a recorded message or a *Text To Speech* system.
  - Interaction with the conversation history. These tests cover the options provided to the user to control and display information about the conversation history with the assistant.

1.1.3.3 Smart home IoT

The security and privacy tests performed to the home IoT devices and a brief description of each one are detailed below as the Table 3 shows:

- Authentication: the application associated with the smart home IoT device implements a method to authenticate the user's identity.
- Insecure pairing method: the link between the smart home IoT device and the mobile app uses a pairing method considered insecure or ineffective against MitM or passive eavesdropping attacks and lacks privacy safeguards.
- Unencrypted Communications: the Wi-Fi communication between the smart home IoT device and mobile app is not encrypted.
- Static MAC address: the smart home IoT device uses a static MAC address (i.e., it does not change when the device is turned off or restarted), exposing it to tracking and user identification attacks.
- Transmission of sensitive information to third-party servers: the managing smart home IoT device application sends sensitive user information to third-party servers.
- Sending of information and firmware updates via HTTP: The mobile app receives firmware updates and sends requests with sensitive information using HTTP without TLS.

Table 3. Security and privacy issues and Smart Home IoT devices tests mapping. (1) Authentication, (2) Insecure pairing method, (3) Unencrypted communications, (4) Static MAC address, (5) Transmission of sensitive information to third-party servers, (6) Sending information and firmware updates over HTTP.

Smart Home IoT	(1)	(2)	(3)	(4)	(5)	(6)
Spoofing	x		x	x		
Lack or weak encryption			x			x
Lack or weak authentication	x					
Uncontrolled voice interaction						
Code injection	x		x	x		
Data interception		x	x	x		x
Takeover	x	x	x	x		
User data being compromised					x	
Violation of privacy laws					x	
Lack of Control and Understanding					x	

1.1.4 List of devices

1.1.4.1 Wearable devices

Wearable devices were selected to include high-end brands such as Fitbit or Garmin, and popular devices (much less expensive) with doubtful reputation. In additions an effort was made to include models specifically designed for children.

The selection of wearables analysed is the following (see Figure 6):

- Mi Band 5
- Garmin vívofit jr. 2
- Fitbit Ace 3
- Honor Band 5
- Honor Watch ES
- BIGGERFIVE Fitness
- TOOBUR Smartwatch
- Amazfit Band 5
- BIGGERFIVE Vigor
- Fitbit Inspire 2
- TOOBUR Smart band

Figure 6. Example of the wearable catalogue analysed.

1.1.4.2 Smart Personal Assistants and Wireless Speakers

The most popular home assistants, from the four leading brands were included in this research. The selection of SPA analysed is the following:

- Apple HomePod Mini (see Figure 7).
- Google Home Mini (see Figure 8).
- Google Nest Audio (see Figure 9).
- Amazon Echo Show 5 (see Figure 10).
- Amazon Echo Dot 4 (see Figure 11)
- Facebook Portal (see Figure 12)

All features of each SPA are detailed in Table 4. For its part, the wireless speaker (BLE speaker) selected to be analysed is the JBL Charge 4, which uses Bluetooth v4.2. to pair with the communication hub (smartphone).

Table 4. Description of SPAs' features.

Features	*Apple HomePod Mini*	*Google Home Mini*	*Google Nest Audio*	*Amazon Echo Show 5*	*Amazon Echo Dot 4*	*Facebook Portal*
Model and release date	1st Generation (November 2020)	1st Generation (October 2017)	-	1st Generation (June 2019)	4th Generation (October 2020)	2nd Generation (October 2019)
Built-in SPA	*Siri*	*Google Assistant*	*Google Assistant*	*Amazon Alexa*	*Amazon Alexa*	*Amazon Alexa*
Companion application	*Home* Application	*Google Home* Application	*Google Home* Application	*Amazon Alexa* Application	*Amazon Alexa* Application	*Amazon Alexa* Application
Supported OS	iOS	iOS and Android	iOS and Android	iOS and Android	iOS and Android	iOS and Android
Wake-up word activation	It can be turned off, but the wake-up word cannot be changed	It cannot be deactivated, and the wake-up word cannot be modified	It cannot be deactivated, and the wake-up work cannot be modified	It cannot be deactivated, but the wake-up word can be selected from a set of three	It cannot be deactivated, but the wake-up word can be selected from a set of three	It cannot be deactivated, but the wake-up word can be selected from a set of three
Microphone	It cannot be deactivated	It can be turned off	It can be turned off	It can be turned off	It can be turned off	It can be turned off
Camera	No	No	No	Yes. It can be deactivated	No	Yes. It can be deactivated
Voice recognition	Yes	Yes	Yes	Yes	Yes	Yes

Figure 7. HomePod Mini

Figure 8. Google Home Mini

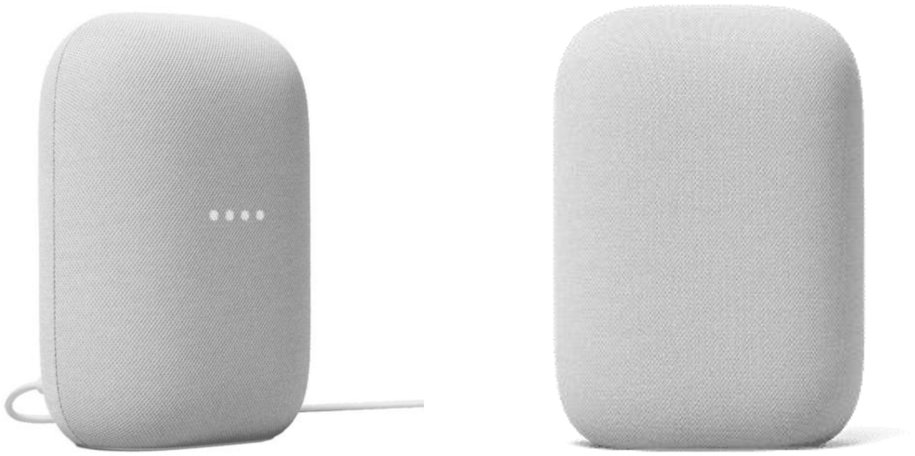


Figure 9. Google Nest Audio.

Figure 10. Amazon Echo Show 5

Figure 11. Amazon Echo Dot 4

Figure 12. Facebook Portal

1.1.4.3 Smart Home IoT

The selection of smart home IoT devices analysed is the following:

- Sonoff devices family.
  - Sonoff smart plug.
  - Sonoff smart lamp holder.
  - Sonoff cable device.
- NiteBird smart led light strip.

1.2 Test implementation and results

1.2.1 Wearables

1.2.1.1 Operation process

Each category of connected device follows a different operating procedure but can be generalized. In this way, it is possible to systematize the evidence acquisition process during the execution of each test defined for each device, depending on the category to which it belongs. In this way, it is possible to obtain a uniform set of results and avoid excluding relevant data and evidence.

- Switching on the wearable and mobile device.
- Connection of the wearable with nRF52 DK and Wireshark.
- Registering/Logging in to the application.
- Pairing process of wearable device and smartphone.
- BLE data collection activities:
  - Carrying out physical activities such as walking, running, etc.
  - Data Synchronization with wearable.
  - Disconnection from wearable.
  - Reconnection with wearable.
- HTTP data collection activities:
  - Editing the user profile.
  - Synchronization of data with cloud server.
  - Logging off.
  - Logging in.
- Disconnection.

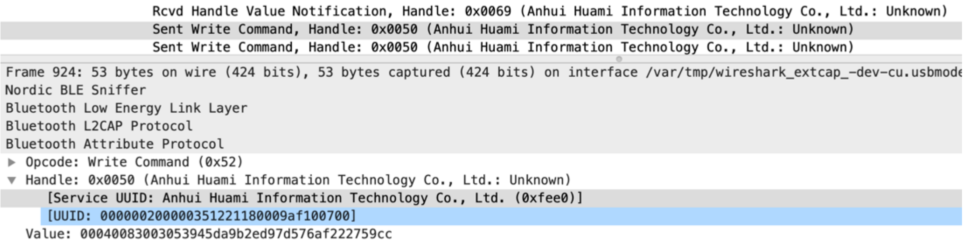
1.2.1.2 Test results

For each device, the tests performed, and the results obtained are briefly summarized below.

1.2.1.2.1 Mi Band 5

- Authentication: the device requires the user to connect via Huami's Mi Fit app. To use it, a Mi Account is required to log in, although it is possible to create one from a third-party account such as Google.
- Pairing and Encryption: Pairing in BLE is immediate and unencrypted, so the packets exchanged are visible to the sniffer. The application appears to establish a connection between the band/app and Huami's servers, which hides its operation using the company's proprietary methods (see Figure 13) and prevents the use of other

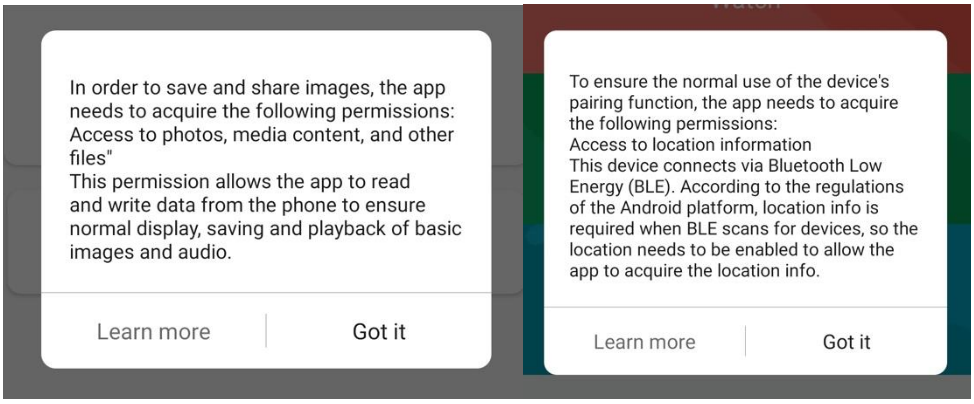
applications. The app authenticates/pairs the phone with Huami's servers and hides the Auth Key in the phone's file system so that it cannot be used by other apps.



```
                    Rcvd Handle Value Notification, Handle: 0x0069 (Anhui Huami Information Technology Co., Ltd.: Unknown)
                    Sent Write Command, Handle: 0x0050 (Anhui Huami Information Technology Co., Ltd.: Unknown)
                    Sent Write Command, Handle: 0x0050 (Anhui Huami Information Technology Co., Ltd.: Unknown)
Frame 924: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface /var/tmp/wireshark_extcap_-dev-cu.usbmode
Nordic BLE Sniffer
Bluetooth Low Energy Link Layer
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
▶ Opcode: Write Command (0x52)
▼ Handle: 0x0050 (Anhui Huami Information Technology Co., Ltd.: Unknown)
     [Service UUID: Anhui Huami Information Technology Co., Ltd. (0xfee0)]
     [UUID: 000000200000351221180009af100700]
  Value: 00040083003053945da9b2ed97d576af222759cc
```

Figure 13. Proprietary Huami BLE attributes used by Mi Fit.

- Although it is not easy to identify what information is being communicated immediately, since the communications are not encrypted, an attacker could understand the operation of Huami's proprietary Services and obtain user's data. That is why there are ways to circumvent this limitation [3], [4], already accessible online.
- <u>MAC Address</u>: The device's MAC does not change on reboot and is constantly announced when the device is not paired, making it easily identifiable.
- <u>Privacy</u>: The application constantly prompts the user to grant permissions for location, health data and access to the photo album, media content and other files (see Figure 14).



In order to save and share images, the app needs to acquire the following permissions: Access to photos, media content, and other files"
This permission allows the app to read and write data from the phone to ensure normal display, saving and playback of basic images and audio.

To ensure the normal use of the device's pairing function, the app needs to acquire the following permissions:
Access to location information
This device connects via Bluetooth Low Energy (BLE). According to the regulations of the Android platform, location info is required when BLE scans for devices, so the location needs to be enabled to allow the app to acquire the location info.

Figure 14. Example of permissions requested by the Mi Fit application (left: images and media; right: location).

1.2.1.2.2 Amazfit Band 5

- <u>Authentication</u>: the device requires the user to connect via Huami's Zepp app. This app requires a Zepp account to log in, although it is possible to create one from a third-party account such as Google, Apple, Mi-Xioami or Facebook.

- Pairing and Encryption: Pairing in BLE is immediate and unencrypted, so the packets exchanged are visible to the sniffer. This process is like the one described in the section 0.

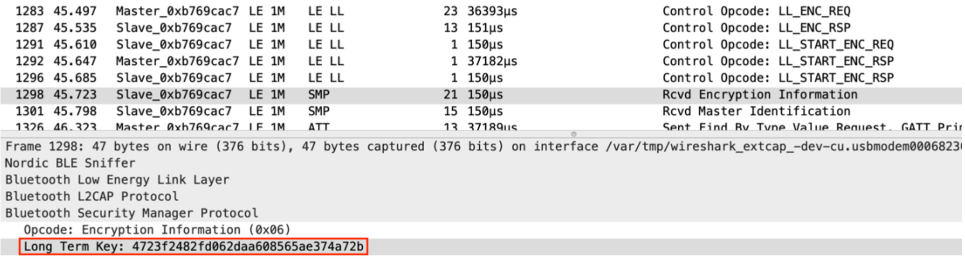
- MAC Address: The device's MAC is visible unless otherwise indicated and it does not change on reboot. In addition, it is constantly announced when the device is not paired, making it easily identifiable.

- Privacy: The application constantly prompts the user to grant permissions for location, health data and access to the photo album, media content and other files, as the section 0 pointed out.

1.2.1.2.3 Garmin vívofit jr. 2

- Authentication: It is necessary to register the device in the Garmin app (Garmin Jr.) which can be done from third party accounts, such as Google.

- Pairing and Encryption: It uses a more secure pairing method than the previous devices. Vivofit uses Passkey, whereby the user must enter the app a number that appears on the wearable's screen. There is encryption, but the Long-Term Key is sent in clear text, so the sniffer can decrypt the packets being sent (see Figure 15).

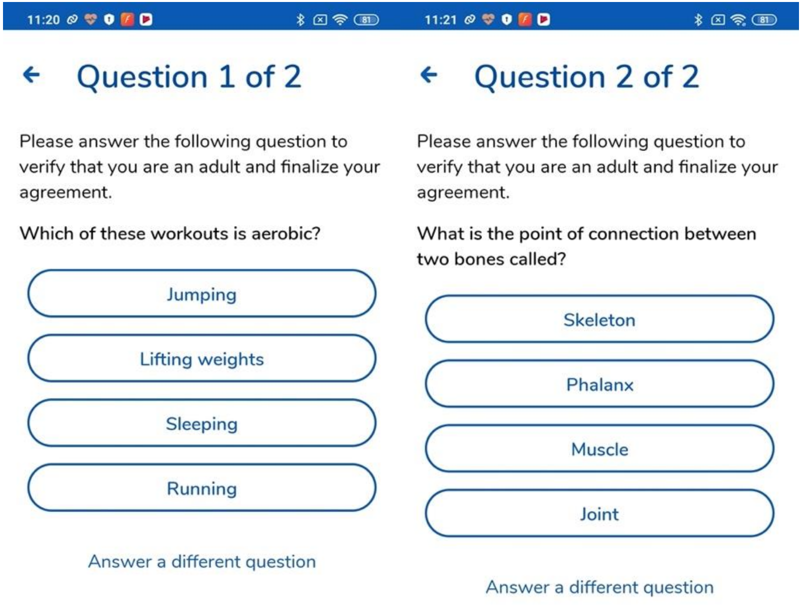


```
1283  45.497   Master_0xb769cac7  LE 1M    LE LL              23  36393µs                   Control Opcode: LL_ENC_REQ
1287  45.535   Slave_0xb769cac7   LE 1M    LE LL              13  151µs                     Control Opcode: LL_ENC_RSP
1291  45.610   Slave_0xb769cac7   LE 1M    LE LL               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
```

Figure 15. LTK sent in clear text by vivofit jr. 2.

- MAC Address: The MAC address does not change when the wearable is rebooted and is announced when it is not paired.

- Privacy: The Garmin application must be managed from an account that must be controlled by a parent. However, the method used to identify whether it is an adult who is registering the account is subject to simple questions (see Figure 16). The application requests location permissions to use Bluetooth.



11:20

← Question 1 of 2

Please answer the following question to verify that you are an adult and finalize your agreement.

Which of these workouts is aerobic?

Jumping

Lifting weights

Sleeping

Running

Answer a different question

11:21

← Question 2 of 2

Please answer the following question to verify that you are an adult and finalize your agreement.

What is the point of connection between two bones called?

Skeleton

Phalanx

Muscle

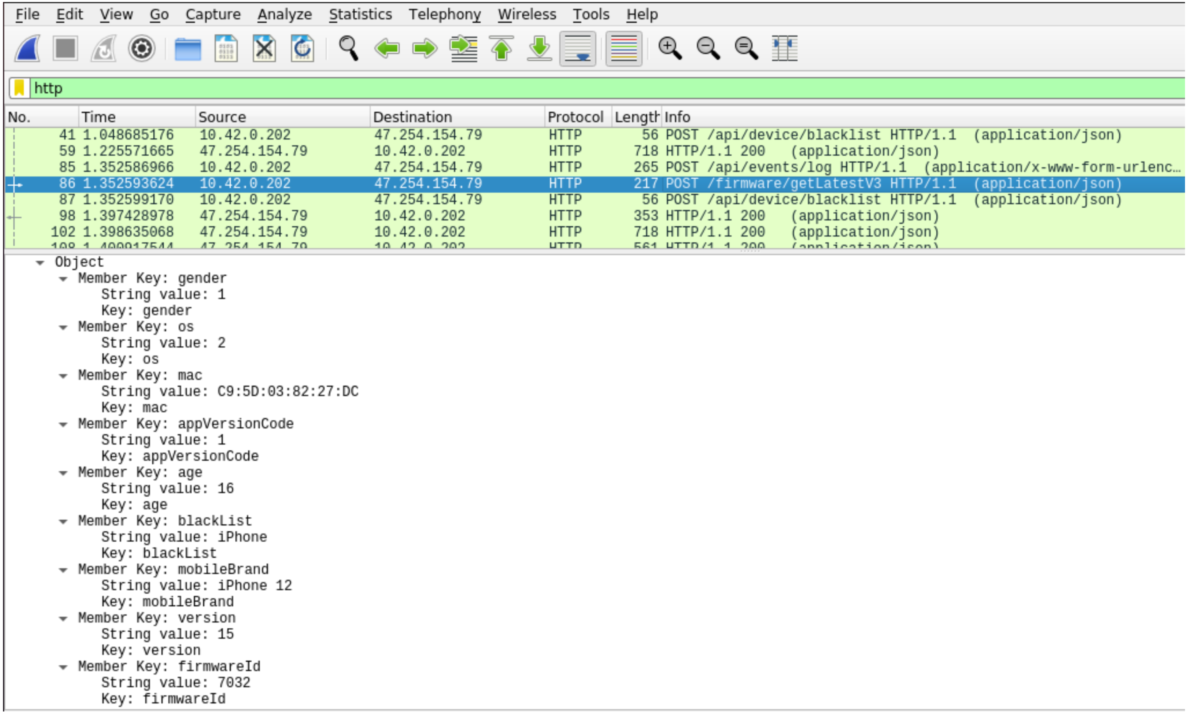
Joint

Answer a different question

Figure 16. Questions asked by Garmin Jr. for adult authentication.

1.2.1.2.4 BIGGERFIVE Fitness and Vigor

- Authentication: A third-party application, VeryFitPro, which does not require any type of authentication or registration, must be used. Also, it is possible to create a user account.
- Pairing and Encryption: The device pairs with the smartphone directly, so it uses Just Works method. There is no packet encryption. This allows the device to seamlessly connect to any other device once it has lost connectivity with the main communications hub (the user's smartphone).
- In the case of the information that is sent from the application to external servers through Wi-Fi, it is possible to observe encrypted information (via HTTPS), but some information is also sent in clear (HTTP). This information transmitted in clear contains sensitive data such as the sex of the user or the MAC address (see Figure 17). This information is sent to external servers when the user tries to update the firmware of the device.

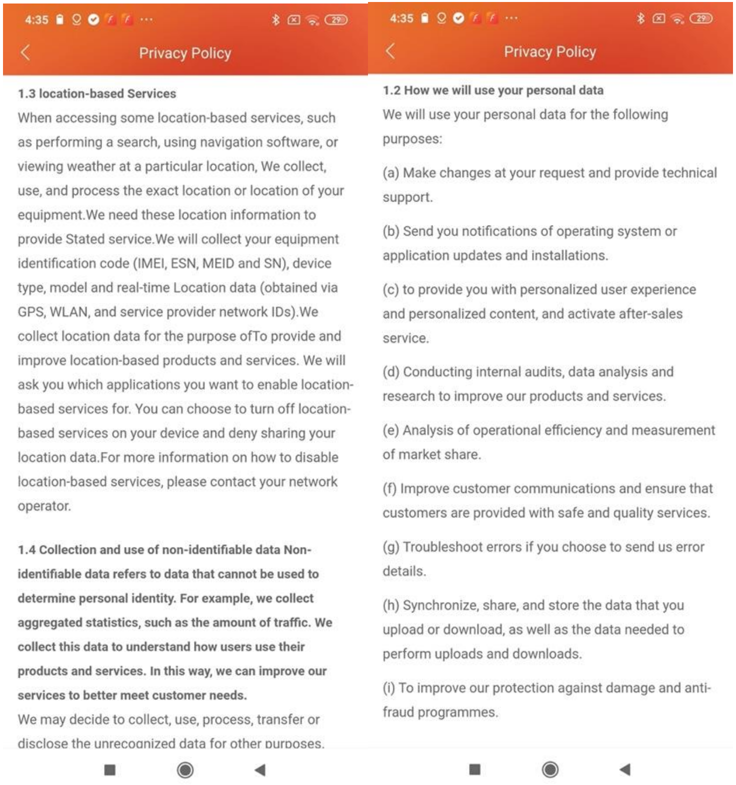

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time         Source          Destination     Protocol Length Info
   41 1.048685176  10.42.0.202     47.254.154.79   HTTP       56 POST /api/device/blacklist HTTP/1.1  (application/json)
   59 1.225571665  47.254.154.79   10.42.0.202     HTTP      718 HTTP/1.1 200   (application/json)
   85 1.352586966  10.42.0.202     47.254.154.79   HTTP      265 POST /api/events/log HTTP/1.1  (application/x-www-form-urlenc…
   86 1.352593624  10.42.0.202     47.254.154.79   HTTP      217 POST /firmware/getLatestV3 HTTP/1.1  (application/json)
   87 1.352599170  10.42.0.202     47.254.154.79   HTTP       56 POST /api/device/blacklist HTTP/1.1  (application/json)
   98 1.397428978  47.254.154.79   10.42.0.202     HTTP      353 HTTP/1.1 200   (application/json)
  102 1.398635068  47.254.154.79   10.42.0.202     HTTP      718 HTTP/1.1 200   (application/json)
  108 1.400917544  47.254.154.79   10.42.0.202     HTTP      561 HTTP/1.1 200   (application/json)

    Object
      Member Key: gender
          String value: 1
          Key: gender
      Member Key: os
          String value: 2
          Key: os
      Member Key: mac
          String value: C9:5D:03:82:27:DC
          Key: mac
      Member Key: appVersionCode
          String value: 1
          Key: appVersionCode
      Member Key: age
          String value: 16
          Key: age
      Member Key: blackList
          String value: iPhone
          Key: blackList
      Member Key: mobileBrand
          String value: iPhone 12
          Key: mobileBrand
      Member Key: version
          String value: 15
          Key: version
      Member Key: firmwareId
          String value: 7032
          Key: firmwareId
```

Figure 17. Graphical description of the information exchanged by VeryFitPro and external servers.

- MAC Address: The MAC address is static, does not change when the device is rebooted and is announced when it is not paired.

- Privacy: The application requests permissions for location, access to contacts and messages, as well as access to the photo album and camera. The app's privacy policy states that the app collects personal information such as the device's IMEI (unique phone identifier) and exact location. It is also stated that this information may be shared with third parties. Although the wristband is targeted at minors, the company's privacy policy specifies that the application is not intended for use by minors (see Figure 18).



4:35

Privacy Policy

1.3 location-based Services

When accessing some location-based services, such as performing a search, using navigation software, or viewing weather at a particular location, We collect, use, and process the exact location or location of your equipment.We need these location information to provide Stated service.We will collect your equipment identification code (IMEI, ESN, MEID and SN), device type, model and real-time Location data (obtained via GPS, WLAN, and service provider network IDs).We collect location data for the purpose ofTo provide and improve location-based products and services. We will ask you which applications you want to enable location-based services for. You can choose to turn off location-based services on your device and deny sharing your location data.For more information on how to disable location-based services, please contact your network operator.

1.4 Collection and use of non-identifiable data Non-identifiable data refers to data that cannot be used to determine personal identity. For example, we collect aggregated statistics, such as the amount of traffic. We collect this data to understand how users use their products and services. In this way, we can improve our services to better meet customer needs.

We may decide to collect, use, process, transfer or disclose the unrecognized data for other purposes.

4:35

Privacy Policy

1.2 How we will use your personal data

We will use your personal data for the following purposes:

(a) Make changes at your request and provide technical support.

(b) Send you notifications of operating system or application updates and installations.

(c) to provide you with personalized user experience and personalized content, and activate after-sales service.

(d) Conducting internal audits, data analysis and research to improve our products and services.

(e) Analysis of operational efficiency and measurement of market share.

(f) Improve customer communications and ensure that customers are provided with safe and quality services.

(g) Troubleshoot errors if you choose to send us error details.

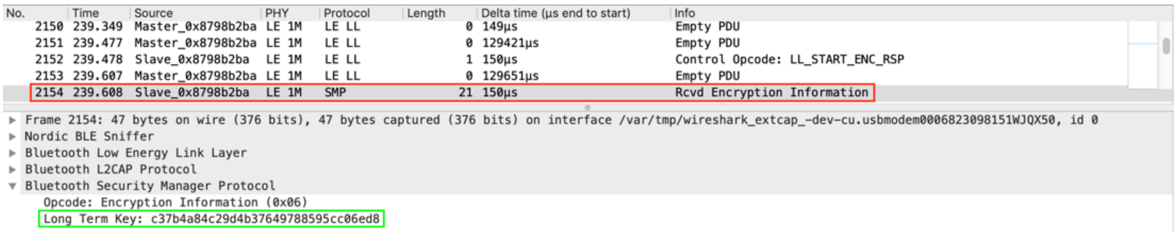
(h) Synchronize, share, and store the data that you upload or download, as well as the data needed to perform uploads and downloads.

(i) To improve our protection against damage and anti-fraud programmes.

Figure 18. Data collected by VeryFitPro.

1.2.1.2.5 TOOBUR Smartwatch and TOOBUR Smart band

- Authentication: No authentication required. The wearable uses VeryFitPro.
- Pairing and Encryption: The device is paired from the application directly, so it uses *Just Works* method. There is no encryption of the packets, and it is easy to identify what kind of data is being sent. If paired from outside the application, the LTK is sent in clear text, so any sniffer can decrypt the exchanged packets (see Figure 19).



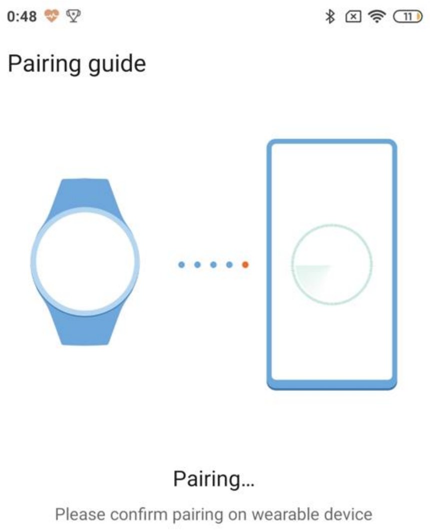
```
No.     Time     Source             PHY    Protocol   Length   Delta time (µs end to start)   Info
  2150  239.349  Master_0x8798b2ba  LE 1M  LE LL           0   149µs                          Empty PDU
  2151  239.477  Master_0x8798b2ba  LE 1M  LE LL           0   129421µs                       Empty PDU
  2152  239.478  Slave_0x8798b2ba   LE 1M  LE LL           1   150µs                          Control Opcode: LL_START_ENC_RSP
  2153  239.607  Master_0x8798b2ba  LE 1M  LE LL           0   129651µs                       Empty PDU
  2154  239.608  Slave_0x8798b2ba   LE 1M  SMP            21   150µs                          Rcvd Encryption Information

▶ Frame 2154: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface /var/tmp/wireshark_extcap_-dev-cu.usbmodem0006823098151WJQX50, id 0
▶ Nordic BLE Sniffer
▶ Bluetooth Low Energy Link Layer
▶ Bluetooth L2CAP Protocol
▼ Bluetooth Security Manager Protocol
    Opcode: Encryption Information (0x06)
    Long Term Key: c37b4a84c29d4b37649788595cc06ed8
```

Figure 19. LTK sent in cleartext by TOOBUR Smartwatch.

- MAC Address: the MAC address is static, does not change when the device is rebooted and is announced when it is not paired.
- Privacy: as it uses VeryFitPro, the same problems as those present in the BIGGERFIVE Fitness were identified.

1.2.1.2.6 Honor Band 5 and Honor Watch ES

- Authentication: It is necessary to use the Huawei Health application, which requires creating or logging in with a Huawei ID. The registration process requires a phone number and email account.
- Pairing and Encryption:
  - In a similar manner to how the Xiaomi Mi Fit app works, communications between the central device and the peripheral are unencrypted, and authentication is done on the Huawei server side to prevent other applications from being used.
- The pairing process requires the user to confirm the linking of the devices on the wearable's display (see Figure 20).


0:48

Pairing guide

Pairing...

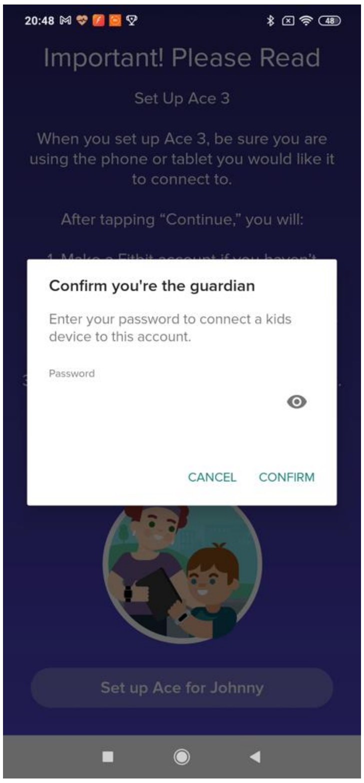
Please confirm pairing on wearable device

Figure 20. Pairing method and process implemented by Honor Band and Honor Watch series.

- MAC Address: The MAC address is static, does not change when the device is rebooted and is announced when it is not paired.
- Privacy: The application requests access to the following permissions:
  - Location
  - Contacts
  - Calls
  - Notifications
  - Photos, camera, and filesystem.
- The application uses Certificate Pinning to prevent the use of fraudulent certificates, so it is not possible to capture HTTP/HTTPS traffic by means of *mitmproxy.*

1.2.1.2.7 Fitbit Ace 3 and Fitbit Inspire 2

- Authentication: It is necessary to register in the Fitbit app and to create a family account. Once registered, the app allows the user to switch between different views for child/adult by validating with the password, as shown in Figure 21.



20:48

Important! Please Read

Set Up Ace 3

When you set up Ace 3, be sure you are using the phone or tablet you would like it to connect to.

After tapping "Continue," you will:

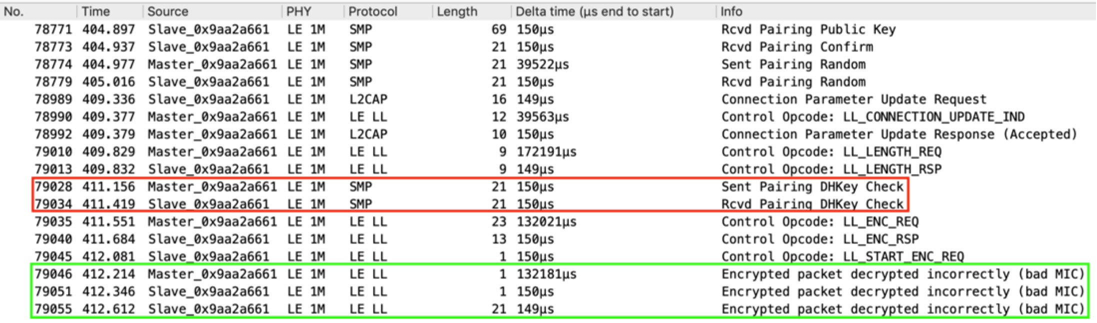
Confirm you're the guardian

Enter your password to connect a kids device to this account.

Password

Figure 21. Guardianship confirmation process over Fitbit Ace.

- Pairing and Encryption: The wristband features the most secure pairing method by implementing BLE Secure Connections. This method encrypts communications with public key cryptography and Elliptic Curve. By implementing an Elliptic Curve Diffie Hellman (ECDH) key exchange, it is not possible to decrypt the communication once the devices are paired (see Figure 22). The pairing method used is Passkey with a 4-digit key (instead of 6).



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)

Figure 22. Capture of the ECDH key exchange when pairing the FitbitAce 3.

- MAC Address: The MAC address is static, does not change when the device is rebooted and is announced when it is not paired.
- Privacy:
  - The Fitbit application must be used from an account that must be 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.
  - The application uses Certificate Pinning to prevent the use of fraudulent certificates, so it is not possible to capture HTTP/HTTPS traffic by means of *mitmproxy*.

1.2.1.2.8 Apple Watch Series 6

Apple smart watches are devices that only integrate with other Apple devices such as iPhone, iPad, or MacBook.

- Pairing and Encryption: The pairing process is robust and secure (leaving aside intrinsic Bluetooth problems such as BIAS or KNOB).
- MAC address. Apple Watch is the only device analysed that uses dynamic MAC addresses.
- Privacy:

Regarding privacy, this device is governed by Apple's base agreements and all sensitive information handled is processed securely.

1.2.1.3 Analysis of the results

The Table 5 shows a summary of the results of the tests performed throughout the project on the wearables selected.

Table 5. Comparative of all wearables analysed.

WEARABLES	Authentication	Secure pairing method	Encrypted communications	Encryption keys sent in clear text	Static MAC address	Sending information and firmware updates over HTTP
Mi Band 5	✓	✓	X	No enc.	✓	X
Garmin vívofit jr. 2	✓	✓	✓	✓	✓	X
Fitbit Ace 3	✓	✓	✓	X	✓	X
Honor Band 5	✓	X	X	No enc.	✓	X
Honor Watch ES	✓	X	X	No enc.	✓	X

WEARABLES	Authentication	Secure pairing method	Encrypted communications	Encryption keys sent in clear text	Static MAC address	Sending information and firmware updates over HTTP
Biggerfive Fitness	x	x	x	No enc.	✓	✓
TOOBUR Smartwatch	x	x	x	✓	✓	✓
Biggerfive Vigor	x	x	x	No enc.	✓	✓
Amazfit Band 5	✓	✓	x	No enc.	✓	x
Apple Watch 6	✓	✓	✓	x	x	x
Fitbit Inspire 2	✓	✓	✓	x	✓	x
TOOBUR Smart band	x	x	x	✓	✓	✓

It can be seen from it 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*. Even so, many of them do not encrypt BLE communications or implement pairing methods that do not ensure the privacy of user data. This is the case of devices such as 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.

On the other hand, the only wearables which can prevent MitM, and eavesdropping attacks are the Fitbit Ace 3 and Apple Watch 6 since they 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 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 versions 5 or less.

As for fitness apps and their privacy, all of them seem to state that they collect sensitive user information in their privacy policies. Moreover, VeryFitPro (used by BIGGERFIVE Fitness and TOOBUR Smartwatch) sends private date 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 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 the minor's information.

By not encrypting either the BLE connection or requests sent over HTTP, VeryFitPro is by far the most insecure and least private application among those analysed. As demonstrated in section 1.2.1.2.4, its operation is vulnerable to reverse engineering attacks, regardless of the connected device. Of particular concern is fact that, BIGGERFIVE and TOOBUR Smartwatch devices, which are designed specifically for minors, indicate in their boxes and manuals that the bands must be used with VeryFitPro app.

One last particularly relevant finding from the analysis is that all the devices analysed make use of static MAC addresses except the Apple Watch 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.

1.2.2 Smart Personal Assistants

1.2.2.1 Operation process

As with wearable devices, it is possible to systematize the evidence acquisition process during the execution of each test defined for each device. In this way, it is possible to obtain a uniform set of results and avoid excluding relevant data and evidence.

- Switching on the SPA and the mobile device.
- Connecting the SPA to the Internet via Wi-Fi.
- Registration/login to the application that manages the SPA. Personal account required (Google, Amazon, iCloud, Facebook, etc.).
- SPA recognition, synchronisation, and configuration process from the mobile application.
- Tests of interaction with the SPA:
  - Basic tests: voice authentication, recognition of non-human voices, exchange of personal data, storage of conversation histories, control of responses with personal content, etc.
  - Tests with devices connected to the SPA.
  - Testing with the SPA and third-party skills/competences, if any.
- Testing of voice payments and transactions.

1.2.2.2 Test results

The test described in detail on section 1.1.3.2 were performed in all SPA analysed. The results for every device are shown below. Additionally, this section provides the analysis of a Bluetooth speaker, JBL Charge 4, as an example of wireless speaker used by children and young adults.

1.2.2.2.1 JBL Charge 4

This type of device does not need installation or preparation of any kind. The only action expected or necessary by the user is the pairing process with the communication hub (smartphone). In this sense, it was found that the MAC of the device is transmitted clearly and is easily accessible by a possible attacker.

Leaving aside more sophisticated attacks like KNOB or BIAS, both feasible due to the Bluetooth version implemented by the device (v4.2.), a DoS has been proven. For this, a test scenario like the one described in Figure 23 has been created. The process followed in the test is detailed in Figure 24.

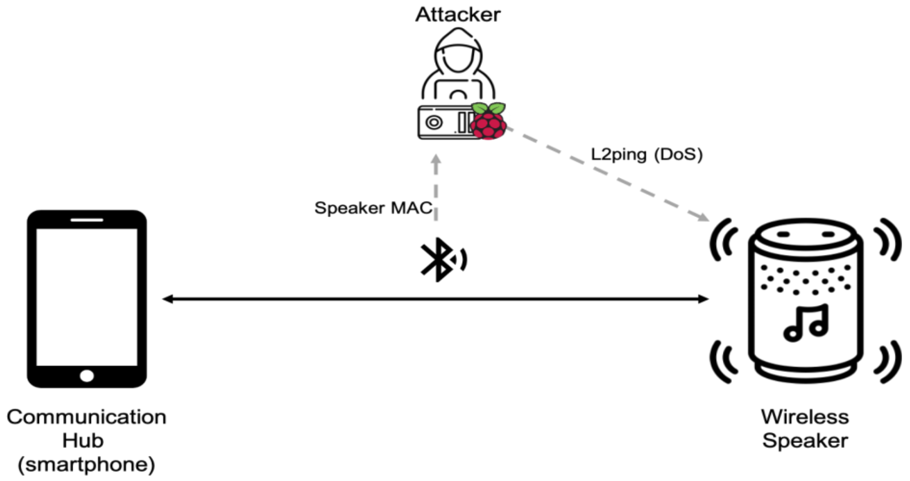


Figure 23. Overview of the DoS attack test performed to a JBL Charge 4 device.

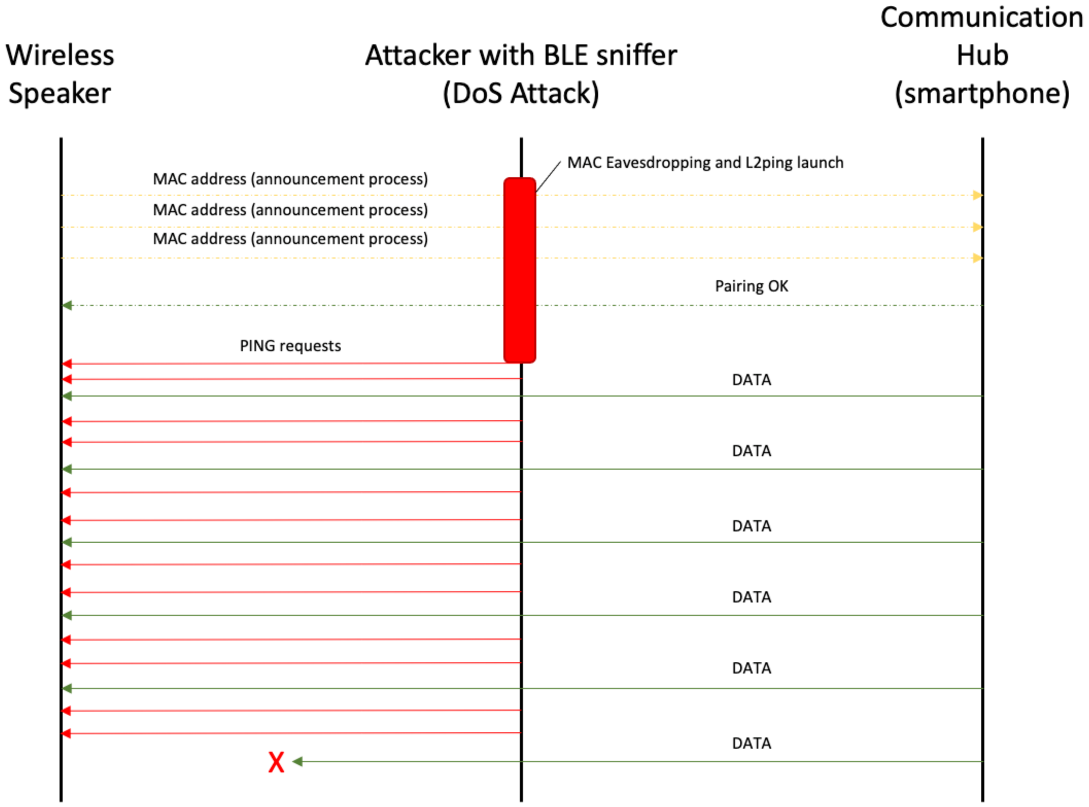

Wireless Speaker
Attacker with BLE sniffer (DoS Attack)
Communication Hub (smartphone)
MAC Eavesdropping and L2ping launch
MAC address (announcement process)
MAC address (announcement process)
MAC address (announcement process)
Pairing OK
PING requests
DATA
DATA
DATA
DATA
DATA
DATA
X

Figure 24. Sequence diagram of the DoS attack tested.

1.2.2.2.2 Apple HomePod Mini

- Installation
  - SPA installation. An iCloud account and an Apple device are required. Wi-Fi details, Siri and other preferences are shared from the iPhone.
  - Connected accessories installation. It is possible to configure whether a user has permission to add or edit devices.
  - Third-party skills installation. Third-party skills cannot be configured.
- Interaction
  - Interaction with SPA and connected devices. Voice and touch control can be deactivated. The use of multimedia devices can be disabled, and the control of connected accessories can be specified per user.
  - Interaction with third- party skills. There is no possibility to interact with third-party skills.
- Functionality
  - Payments and transactions. Payments or purchases from the HomePod Mini are not supported.
  - Possibility of creating “safe” profiles for minors. There is no possibility to create a user profile for minors, it is necessary to manually access every control and activate them.
- Privacy and security
  - Control of answers containing personal information. It is necessary to activate voice recognition to provide answers containing personal information. Additionally, a two-steps verification can be enabled using the authentication method available in the iPhone to provide personal answers.
  - Authentication methods. Authentication through voice profile recognition.
  - Non-human voice filtering. A pre-recorded activation message or a wake-up message read by a Text To Speech system can invoke the assistant.
  - Interaction with conversation history. It is possible to send a request to delete the conversation history from the servers. Nevertheless, the history is not visible.

1.2.2.2.3 Google Home Mini and Google Nest Audio

- Installation
  - SPA installation. A Google account is required. Wi-Fi details, Google account preferences and additional settings are shared from the mobile device.
  - Connected accessories installation. Permissions cannot be configured for home users. Anyone can add or edit accessories.

- Third-party skills installation. There is no third-party actions (skills) installation process. Knowing the activation phrase, any action can be used.

- Interaction
  - Interaction with SPA and connected devices. Media playback can be disabled for the device. It is not possible to define permissions from Google Home, being necessary to create a family in the external application Family Link and configure filters by device in the application Google Home.
  - Interaction with third-party skills. There are no third-party action controls per user, it is necessary to create a content filter for the entire group of users in the house.
- Functionality
  - Payments and transactions. Payments can be set up from the assistant. They support an additional authentication method based on the hardware of the device where the Google Home application is installed.
  - Possibility of creating "safe" profiles for minors. This option is only available on Android devices. For other devices it is required to manually create content filters that affect all the users equally, although options such as payments are still active after applying these filters.
- Privacy and security
  - Control of answers containing personal information. Personal responses can be disabled in the settings of the Google Home Mini.
  - Authentication methods. The device supports voice authentication. However, using a recording of a user invoking the assistant, it is possible to impersonate him, being able to perform any request later, as depicted in Figure 25 and Figure 26.

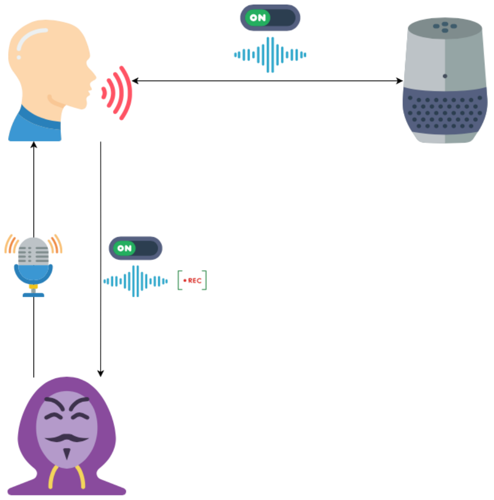


Figure 25. Recording of a legitimate activation message by a malicious actor

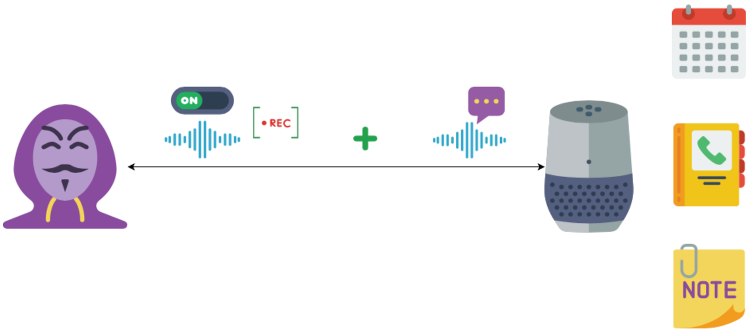


Figure 26. Impersonation attack with a legitimate activation message recorded

- Non-human voice filtering. Messages from recordings and synthetic voices are not filtered.
- Interaction with conversation history. Comprehensive options are included to view, pause, and automatically delete the conversation history. It also includes guest mode, which consists of anonymous use of the device without linking it to the user's account.

1.2.2.2.4 Amazon Echo Show 5 and Echo Dot 4

- Installation
  - SPA installation. An Amazon account is required to use the Echos. The Wi-Fi data is entered into the device and the Alexa settings are synchronized from the mobile device.
  - Connected accessories installation. The house administrator can enable the use of skills from the Amazon Alexa app before using them, but a regular user can

activate any skill from the Echos without confirmation, and even re-activate a skill previously disabled by the administrator.

  - Third-party skills installation. The house administrator can enable the use of skills from the Amazon Alexa app before using them, but a regular user can activate any skill from the Echos without confirmation, and even re-activate a skill previously disabled by the administrator.

- Interaction
  - Interaction with SPA and connected devices. The Echo Show 5 provides controls to turn off the camera and microphone. The Echo Dot does not have a camera but offers controls to turn off the microphone. There is no possibility to differentiate between users or to define permissions for specific interactions.
  - Interaction with third-party skills. The house administrator can permit the use of skills from the Amazon Alexa app before they are used in the Echos, but any user can trigger a skill from the Echos without confirmation.
- Functionality
  - Payments and transactions. Payments can be made with the assistant via Amazon 1 Click. Additional confirmation methods can be configured via a voice profile or a four-digit code.
  - Possibility of creating “safe” profiles for minors. There is no dedicated option to set a safe profile for minors. It is necessary to disable and restrict settings in each of the categories (media playback, web browser, payments, skills, etc.) It is not possible to restrict the use of connected accessories.
- Privacy and security
  - Control of answers containing personal information. There is no possibility to disable responses containing personal information. It is necessary to deactivate the functionalities completely since any user can invoke them.
  - Authentication methods. The Echo Show 5 and Echo Dot 4 have voice recognition, but it is only used for personalization functions, for example in skills. It is not used for security purposes. As in the Google Home Mini, a malicious actor can impersonate a legitimate user by playing a recording of the activation message (see Figure 25 and Figure 26).
  - Non-human voice filtering. Recorded messages and those originated by synthetic voices are not filtered before processing.
  - Interaction with conversation history. The Amazon Alexa application offers complete options for viewing, deleting, and pausing the conversation history, including automatic deletion options.

1.2.2.2.5 Facebook Portal

- Installation

  - SPA installation. A Facebook account is required to use the Portal. The 10'' touchscreen allows to users to interact with the Facebook Portal and perform some installation tasks such as entering the Wi-Fi connection data, language selection, and so on. As a Facebook product, it is necessary to associate the Portal with the user account in facebook.com/device by using a paring code.
  - Connected accessories installation. Anyone can enable the use of skills and plugins from the Facebook Portal software portal without confirmation, and even re-activate add-ons previously disabled by the main user.
  - Third-party skills installation. It is allowed by restricted to the Facebook Portal software portal.
- Interaction
  - Interaction with SPA and connected devices. The Facebook Portal provides controls to turn off the camera and microphone. There is no possibility to differentiate between users or to define permissions for specific interactions.
  - Interaction with third-party skills. The administrator can permit the use of skills from the Facebook Portal software portal before they are used in the Portal, but any user can trigger an add-on without confirmation.
- Privacy and security
  - Facebook Portal uses Amazon Alexa as voice agent, so, the analysis of privacy and security previously done to Amazon Echo Show 5/Echo Dot 4 is applicable to this device. In addition, Facebook Portal, records voice clips when the users activate the Smart Assistant by saying “Hey portal” and it sends back to Facebook these clips. Also, these voice clips are recorded and sent back to Amazon.
  - Finally, data about the Facebook Portal usage is used to target you with advertisements across Facebook. The company may also share specific demographic and audience engagement data with advertisers and analytics partners.

1.2.2.3 Analysis of the results

The analysis has shown that protection of minor users through simple and quick settings is practically non-existent in the tested conditions (device versions, app versions and mobile device to which they have been paired). In all cases it is necessary to go through the full set of device settings, even needing to switch between different configuration menus, to disable all features that may be unsafe for an unsupervised minor user. It was found that in many cases, restricted device settings affect all users equally, leaving features unusable for all members of the household, which is impractical and does not encourage users to establish these restrictions. A brief comparison of all SPA analysed is presented in Table 11 and Table 12, available in the Appendix section.

With respect to SPA authentication systems, it has been found that they can be compromised by the lack of protection measures against commands originated by an artificial source, that make the devices vulnerable to impersonation attacks as shown in Figure 25 and Figure 26.

Finally, the wireless speaker, JBL Charge 4, has been tested by means of a DoS attack supported by a portable device (Raspberry Pi 4 model B). This test shows that, in addition to being susceptible to more complex attacks such as KNOB or BIAS, it is possible to disconnect said device from its master. In this way, by creating false device identities, it would be possible to connect the master to a fake device, which will be used as an access vector for the attacker.

1.2.3 Smart Home IoT

1.2.3.1 Operation process

The security and privacy tests performed to the home IoT devices have been carried out within a virtual environment (see section 0). For its part, the operation process performed during the analysis of smart home IoT devices is the following:

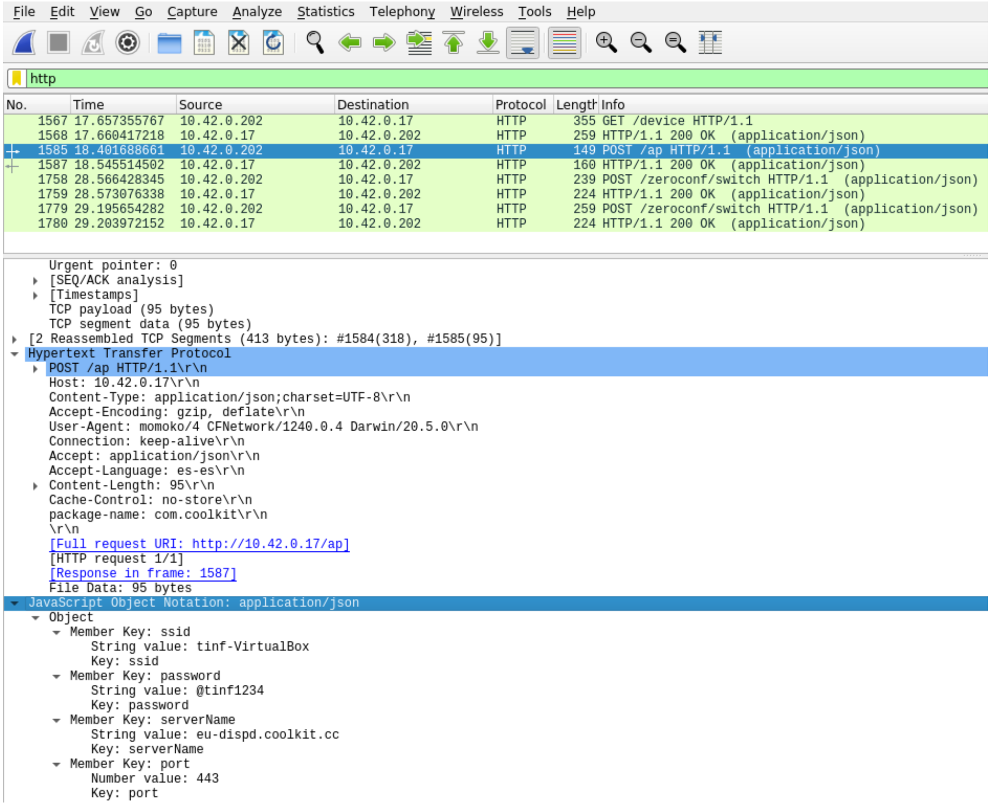
- Installing the recommended mobile application for managing the device.
- Plugging the device.
- Switching on the device, if necessary, and the mobile application.
- HTTP data collection activities:
  - Pairing of smart home IoT device and the smartphone.
  - Turning on and use the device.
  - Device shutdown.
- Disconnection.

1.2.3.2 Test results

1.2.3.2.1 Sonoff devices family

All Sonoff devices had a similar behaviour and the results obtained were the same. So, the results are presented together along this section.

- Authentication: the application associated with the smart home IoT device requires a user account which is verified by a code sent to an email account.
- Insecure pairing method: the mobile app does the pairing process. To perform this process, the mobile app asks to user about the Wi-Fi hotspot and its credentials. As it can be seen in Figure 27, these credentials are sent in clear through HTTP messages.



http

```
No.    Time          Source         Destination    Protocol Length Info
  1567 17.657355767  10.42.0.202    10.42.0.17     HTTP      355 GET /device HTTP/1.1
  1568 17.660417218  10.42.0.17     10.42.0.202    HTTP      259 HTTP/1.1 200 OK  (application/json)
  1585 18.401688661  10.42.0.202    10.42.0.17     HTTP      149 POST /ap HTTP/1.1  (application/json)
  1587 18.545514502  10.42.0.17     10.42.0.202    HTTP      160 HTTP/1.1 200 OK  (application/json)
  1758 28.566428345  10.42.0.202    10.42.0.17     HTTP      239 POST /zeroconf/switch HTTP/1.1  (application/json)
  1759 28.573076338  10.42.0.17     10.42.0.202    HTTP      224 HTTP/1.1 200 OK  (application/json)
  1779 29.195654282  10.42.0.202    10.42.0.17     HTTP      259 POST /zeroconf/switch HTTP/1.1  (application/json)
  1780 29.203972152  10.42.0.17     10.42.0.202    HTTP      224 HTTP/1.1 200 OK  (application/json)
```

```
     Urgent pointer: 0
   ▸ [SEQ/ACK analysis]
   ▸ [Timestamps]
     TCP payload (95 bytes)
     TCP segment data (95 bytes)
 ▸ [2 Reassembled TCP Segments (413 bytes): #1584(318), #1585(95)]
 ▾ Hypertext Transfer Protocol
   ▸ POST /ap HTTP/1.1\r\n
     Host: 10.42.0.17\r\n
     Content-Type: application/json;charset=UTF-8\r\n
     Accept-Encoding: gzip, deflate\r\n
     User-Agent: momoko/4 CFNetwork/1240.0.4 Darwin/20.5.0\r\n
     Connection: keep-alive\r\n
     Accept: application/json\r\n
     Accept-Language: es-es\r\n
   ▸ Content-Length: 95\r\n
     Cache-Control: no-store\r\n
     package-name: com.coolkit\r\n
     \r\n
     [Full request URI: http://10.42.0.17/ap]
     [HTTP request 1/1]
     [Response in frame: 1587]
     File Data: 95 bytes
 ▾ JavaScript Object Notation: application/json
   ▾ Object
     ▾ Member Key: ssid
         String value: tinf-VirtualBox
         Key: ssid
     ▾ Member Key: password
         String value: @tinf1234
         Key: password
     ▾ Member Key: serverName
         String value: eu-dispd.coolkit.cc
         Key: serverName
     ▾ Member Key: port
         Number value: 443
         Key: port
```

Figure 27. Information sent by Sonoff devices during pairing process.

- Unencrypted Communications: the communications between the Sonoff devices and external servers are supported by TLS v1.3.
- Static MAC address: the MAC address does not change, and it is sent in clear.
- Transmission of sensitive information to third-party servers: the privacy issues are managed by the mobile app and all information sent to external servers is informed and correctly protected.
- Sending of information and firmware updates via HTTP: see “Insecure pairing method” and “Unencrypted communications” points.

1.2.3.2.2 NiteBird smart led light strip

- Authentication: this smart home IoT device uses the GoSund application (GoSund Group Co. Ltd, Shenzhen, RPC) to manage its behaviour and functionality.
- Insecure pairing method: the pairing method is based on ZeroConf and all information exchange is encrypted.
- Unencrypted Communications: the communications between the NiteBird device and external servers are encrypted using TLS v1.3.
- Static MAC address: the MAC address is anonymized or not shown.

- Transmission of sensitive information to third-party servers: the privacy issues are managed by the mobile app and all information sent to external servers is informed and correctly protected.
- Sending of information and firmware updates via HTTP: see "Insecure pairing method" and "Unencrypted communications" points.

1.2.3.3 Analysis of the results

The results of security and privacy tests show that those low-cost devices based on Sonoff technology have certain shortcomings in terms of encryption of pairing information. Specifically, these devices send the SSID and WPA password without any encryption during the initial pairing and confirmation process. This unprotected information exchange can lead to a takeover situation of the home Wi-Fi network.

On the other hand, high-end commercial devices, such as the smart led light strip from NiteBird, use robust and secure pairing methods such as ZeroConf, which ensures a secure communication from the initial moment of use of this type of device.

1.3 Recommendations

Considering the results obtained and their analysis, we can conclude that, in general, most low-cost devices present a greater amount of 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 shared through insecure connections with third-party servers. In this way, it is possible to offer a series of recommendations whose objective is to mitigate the detected vulnerabilities. Furthermore, these recommendations are defined with a general application purpose, without discerning the device's type, price, manufacture, or origin.

First, users must be aware of the information (data) that each device captures during its use. For this, it is necessary, in some cases, to read and understand the privacy policy set by the device or the underlying management application. In addition, it is important to limit the information shared with the applications, giving access only to those data necessary for their operation.

Second, it is important to use well-configured users to interact with the devices and their management applications. For example, it is interesting to use a different username and password than the usual ones for each application, using key rings to safeguard more complex keys.

From the point of view of configuring the devices, it is important to give them an identifying name and hide their MAC address if possible. A representative name facilitates unequivocal identification by the user for pairing with other devices or the local Internet network. Furthermore, the MAC address hiding prevents some attacks made through this identifier.

Finally, it is essential to ensure that devices that use voice as a method of interaction can recognise the user. In general, this type of device has the necessary tools to perform this recognition. This operation, together with the possibility of establishing different or non-default activation words, allows for reducing the likelihood that agents, external to the user's environment, can carry out action orders for this type of device.

1.4 Honeypot

A honeypot is a computer security mechanism set to deceive attackers giving an appearance of a legitimate site with what looks like valuable information or resources for the attackers. However, honeypots are used to analyse the behaviour of the attackers and to identify the types of tools they use to penetrate the network, which vulnerabilities they exploit, and how they implement lateral movement.

The objective of this section is to design and deploy an IoT honeypot to carry out research about how IoT attackers behave, how their attacks work, and what tools are more popular among this type of attacks.

To classify honeypots, there are different factors to be considered that help choosing the appropriate honeypot technology depending on the target application. These factors are: the purpose of the project, the role of the system, level of interaction, scalability, resource level, availability of source code and application. Making use of this information, the taxonomy of honeypots shown in Figure 28 can be defined [5]:

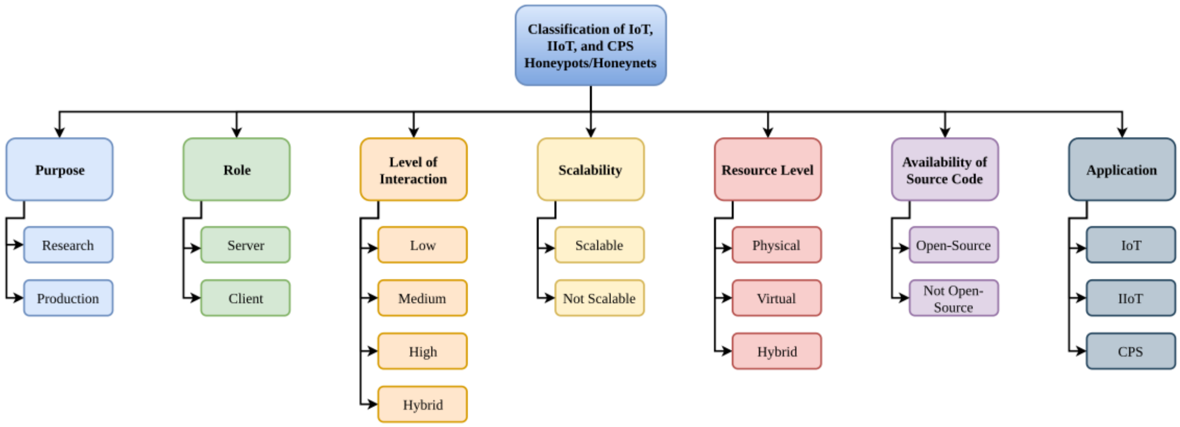


Figure 28. Taxonomy of honeypots.

Depending on the level of interaction that the honeypot provides to the attacker, they can be classified into three groups:

- **Low-interaction**: only limited interaction for an attacker or malware is permitted. All services offered by a low-interaction honeypot are emulated. Thus, low-interaction honeypots are not themselves vulnerable and will not become infected by the exploit attempted against the emulated vulnerability. But will only be able to catch an attacker’s attention and deceive them into attacking. These are easy to implement but not as useful because the attackers will rapidly know they are not in a real environment.

- **Mid-interaction**: this type of honeypots is mid-way between low and high-interaction. They provide a compromise between implementation complexity and level of realism to deceive attackers.
- **High-interaction**: is a honeypot designed to give an attacker full reign of an environment in the sense that they are lured into compromising it. This system will be configured to utilize extensive system and file system logging and will also be subject to a very exhaustive set of IDS rules and monitoring. High interaction honeypots are often implemented using virtual machines, so that they can be reverted back to a known clean snapshot with relative ease. This type of honeypot is difficult to implement because of its complexity, but it is the most realistic one.

In order to select the best scenario for the aim of the project, we study different honeypots [6]. Even though there are many more honeypots, the honeypots analysed in Table 6 are the most popular. Since they are widely used, their implementation will probably be easier because better documentation is available. All honeypots studied are open source, so that they could be implemented in our project.

Table 6. Analysis and comparison of most popular open-source honeypots.

HONEYPOT	SERVICE	CODE	DESCRIPTION	ADVANTAGES	DISADVANTAGES
KIPPO	SSH	Open Mid-interaction	Records brute force attacks and information associated with attacker's interaction	Useful GUI that shows the success/failure of command execution, visited URLs…	Cannot simulate complete files
COWRIE	SSH y Telnet	Open Mid-interaction	Records brute force attacks and captures the interaction made by an attacker	- Using SCP and SFTP commands to download files beyond using "wget" or "curl" - Kippo new version - Emulation that logs an attacker's sessionà better understanding of attackers' TTPs	It still is a mid-interaction honeypot
DIONAEA	SIP, FTP, TFTP, SMB, BBDD	Open Low-interaction	Emulates Intel x86 services and instruction execution and detects shellcodes.	It obtains a copy of the malware It has support for IPv6 and TLS protocol.	Easy detection by attackers, if used isolated
HONEYD	Creates virtual hosts in a network	Open Low-interaction	Allows you to configure several virtual hosts in a computer network with distraction and honeypot uses	In the logs you can see if there is traffic going to the configured virtual hosts	Low interaction

HONEYPOT	SERVICE	CODE	DESCRIPTION	ADVANTAGES	DISADVANTAGES
GLASTOPF	Web applications honeypot	Open Low-interaction	It emulates web application vulnerabilities	It allows collecting information related to attacks as RFI, LFI, SQLi, …	Low interaction Focus on web applications

Having studied these honeypots, it was decided that a mid-interaction honeypot would be interesting for the project. Cowrie was considered the best option in this case because of all the features and possibilities it provides. In addition, a low-interaction honeypot will also be implemented, selecting Dionaea as the most suitable solution.

In order to see how attacks are developed against IoT devices, the SPA shown in Table 7 are considered for the study:

Table 7 - SPA considered for the honeypot

DEVICE	TYPE	FEATURES	ADVANTAGES	DISADVANTAGES
Apple HomePod Mini	SPA	SPA: Siri It can be configured if a user has permission to add or edit devices Cannot interact with third party skills Does not support payments	3º SPA in the market	Limited ecosystem
Google Home Mini	SPA	SPA: Okay Google Permissions cannot be set per user, but anyone can add or edit accessories Knowing the activation process, any action can be used Payments can be made with an additional method of authentication	Market share: 31.4% (2019)	Somehow limited ecosystem
Amazon Echo Show 5	SPA	SPA: Alexa WiFi data is entered, and Alexa settings are synchronized from the mobile device Administrator can enable use of Amazon Alexa apps, but any user can activate any skill without confirmation	Most used SPA on the market Allows more actions than other SPAs	N/A

In the case of wearables, in contrast with most IoT devices, that implement WiFi communications to connect directly to the Internet, wearable devices typically implement Bluetooth communications. A wearable device connects to a smartphone through BLE. This smartphone normally runs an application that connects to cloud servers of the wearable's company or sometimes a third-party company. Figure 29 illustrates this configuration [7] and Table 8 analyse the wearables considered for the honeypot.

Table 8 - Wearables considered for the honeypot

DEVICE	TYPE	APP	DESCRIPTION
Mi Band 5 [8]	Wearable	Mi Fit	High-end device It requires authentication through the app, using an account (My Account or third-party account such as Google) App pairs the phone with Huami's servers and hides the *Auth Key* in the phone's file system, so that it cannot connect with other apps The device's MAC is static and is being announced non-stop when it is not paired
Garmin vívofit jr.2	Wearable	Garmin Jr.	High-end device It requires authentication through the app, using an account (can be a third-party account such as Google) Lack information about app-server communication The device's MAC is static and is being announced non-stop when it is not paired
Fitbit Ace 3	Wearable	Fitbit	High-end device The app uses Certificate Pinning to avoid the use of fraudulent certificates, so it is not possible to capture HTTP/HTTPS traffic with a MITM
Honor Band 5	Wearable	Huawei Health	High-end device The app uses Certificate Pinning to avoid the use of fraudulent certificates, so it is not possible to capture HTTP/HTTPS traffic with a MITM
Honor Watch ES	Wearable	Huawei Health	Same as Honor Band 5
BIGGERFIVE Fitness	Wearable	VeryFitPro	Low-end device Does not require any kind of authentication or register
TOOBUR Smartwatch	Wearable	VeryFitPro	Same as BIGGERFIVE Fitness

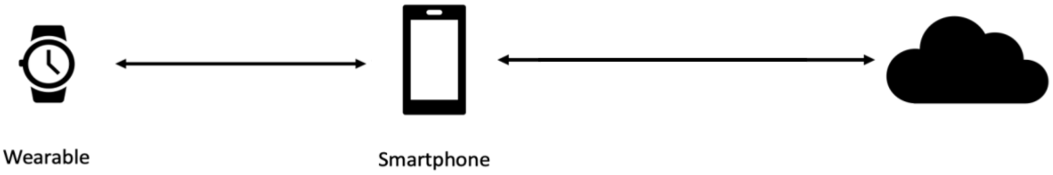


Figure 29 - Communication scenario for wearables

Other available IoT devices considered for the honeypot are shown and analysed in Table 9.

Table 9 – Other IoT devices considered for the honeypot

DEVICE	TYPE	DESCRIPTION
Sonoff	Smart switch	IoT device that allows control by commuting the on/off status of any electrical or electronic device or appliance from any smart device such as a tablet or cell phone as long as the mobile phone has a network (2G/3G/4G/WiFi)
Dahua Vandal Proof Wi-Fi Dome Camera	Webcam	Configuration through an application called "Easy4ip" that scans a QR code and allows viewing the video from the mobile

Once all the devices have been selected, the architecture of the honeypot can be set. Figure 30 shows the overall architecture designed for such a honeypot. As it has already been said, to collect a useful amount of information for the study, two honeypots will be implemented: Cowrie and Dionaea. These two honeypots will be implemented in a Raspberry Pi, that will be connected to the Internet through a router.

As it is also shown in Figure 30, the considered SPAs will be deployed to collect information about different attacks depending on the SPA, and which one of the three receives more attacks. The SPAs will be connected to the network through a Wi-Fi access point configured in the Raspberry Pi. The main idea is that the Sonoff and the webcam will also be connected to the network through this access point.

Wearable devices need to connect to an app, as mentioned above, so to connect them to this network, we will use an Android phone to which the wearables will be connected though BLE. This phone will have all the different apps configured. It will then be connected through Wi-Fi to the Raspberry Pi, where the honeypots will be working to deceive the attacker. Multiple wearables will be connected, some high-end and some low-end to see how differently they are attacked.

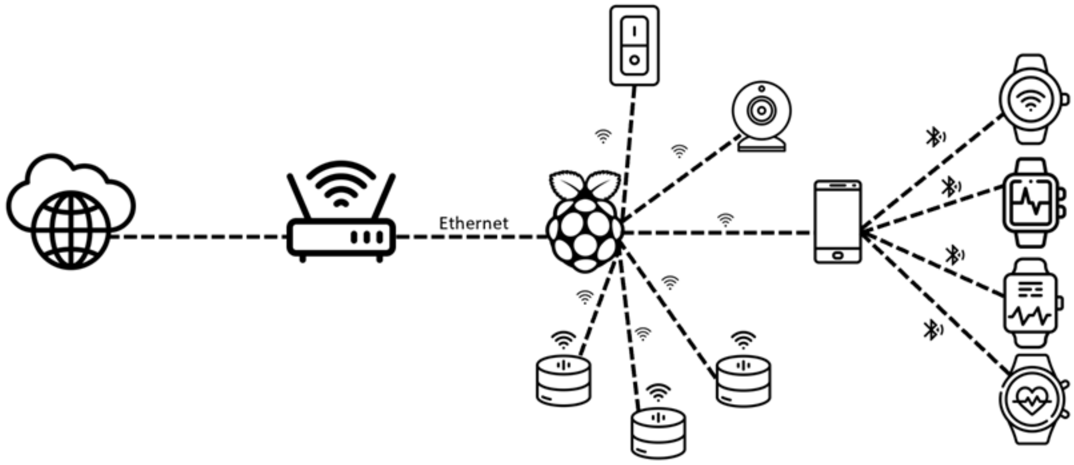


Figure 30. Overall architecture of the designed honeypot.

This honeypot will be deployed during 2 to 3 months. The data gathered through the honeypot will be analysed to learn more about how these devices are attacked, complementing the study carried out in the rest of the deliverable.

1.5 Open Access Platform

To bring together all the above, an open access platform available to the public has been developed. It includes:

- The methodology described for the realization of tests for evaluating the security and privacy level assessment testing of IoT devices.
- The hardware and software tools used for the automation of the tests and obtain the results.
- The tests themselves and the steps followed to perform them.
- The tool developed for automatic testing of any connected device.
- The results obtained together with a set of recommendations for the user.

The open access platform is available in https://rayuelaproject.github.io/RAYUELA/

It provides an overview of the project together with background information that facilitates the related pre-tasks and the contribution of these tests to the context of the RAYUELA project, see Figure 31.

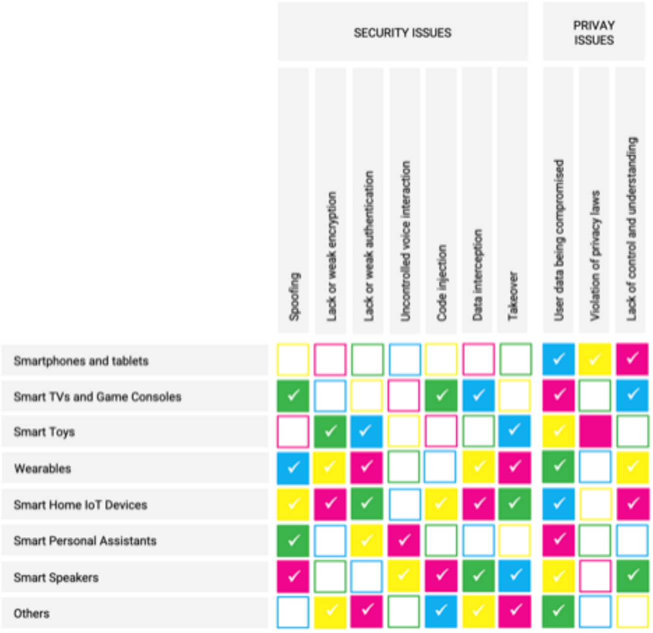
ABOUT THE TASK

This repository includes information in relation to technology assessment and the IT threat landscape. For this purpose, we carried out a set of vulnerability tests and risk assessment of security issues linked to connected devices. These tests were approached from the point of view of the most common online threats for young people. In addition, Cybercrime-as-a-Service (Caas) models that exploit these Internet of Things (IoT) vulnerabilities were evaluated.

The main objective of this repository is therefore to describe and explain a methodology for the security and privacy rsisk assessment in IoT devices, as well as a catalogue of vulnerabilities in IoT devices frequently used by children and young people and sobre recommendations for risk mitigation. In addition, to support the methodology, this repository exposes a set of interesting tools for testing security and privacy vulnerabilities in the conext of the IoT. In addition, alongside the purely technological aspects, this methodology will consider the human factors affecting such vulnerabilities and their expoitation in new CaaS models. As a starting point, previous research has studied young people's use of connected devices and which devices they use most in their daily lives. This study resulted imn a categorisation of 7 types of connected devices that are widely uesd by young people:

1. Smartphones and tablets
2. Smart TVs and Game consoles
3. Smart toys
4. Wearables
5. Smart home IoT devices
6. Smart Personal Assistants
7. Smart speakers
8. Others, such as drones, cameras, or intimate devices

In addition, the security and privacy problems of these connected devices were analysed, which led to the definition of 7 security issues and 3 privacy issues, as described below:



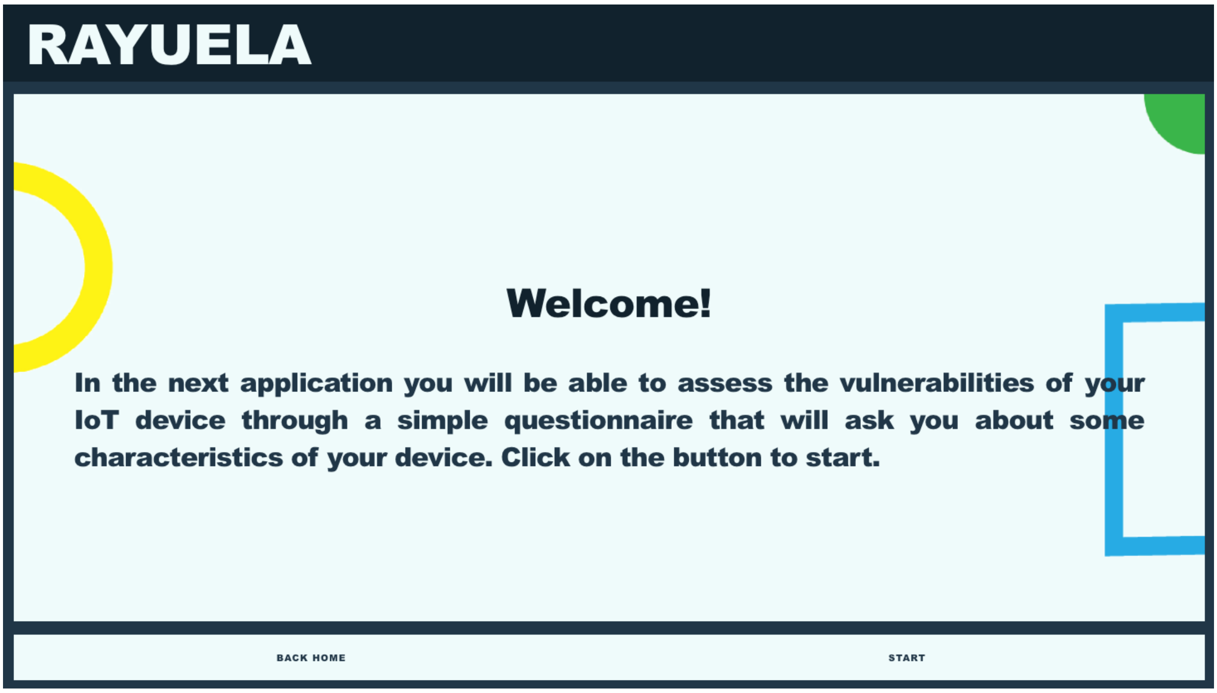
	SECURITY ISSUES							PRIVAY ISSUES		
	Spoofing	Lack or weak encryption	Lack or weak authentication	Uncontrolled voice interaction	Code injection	Data interception	Takeover	User data being compromised	Violation of privacy laws	Lack of control and understanding
Smartphones and tablets	□	□	□	□	□	□	□	✓	✓	✓
Smart TVs and Game Consoles	✓	□	□	□	✓	✓	□	✓	□	✓
Smart Toys	□	✓	✓	□	□	□	✓	✓	■	□
Wearables	✓	✓	✓	□	□	✓	✓	✓	□	✓
Smart Home IoT Devices	✓	✓	✓	□	✓	✓	✓	✓	□	✓
Smart Personal Assistants	✓	□	✓	✓	□	□	□	✓	□	□
Smart Speakers	✓	□	□	✓	✓	✓	✓	✓	□	✓
Others	□	✓	✓	□	✓	✓	✓	✓	□	□

All these problems have been analysed from technological, psychocological and socio-economic points of view, so that not only technological or engineering factors, but also human and socio-economic factors influencing the implementation, development and establishment of these problems and the urderlying threats have been assessed.

Figure 31. Overview of the project.

These tests have focused on the user-connected device interaction, and on the communication between the connected device and the communication hub. However, no tests as such have been performed on the part of external server or third-party applications and the hub system, focusing here on a theoretical study of the scenario.

However, we are aware that despite the steps taken to enable the replication of the tests, not all users have the necessary knowledge and tools. Therefore, we have developed an automatic testing tool that allows the less expert user to assess the security and privacy vulnerabilities of their connected device without the need to install any tools. See Figure 32.



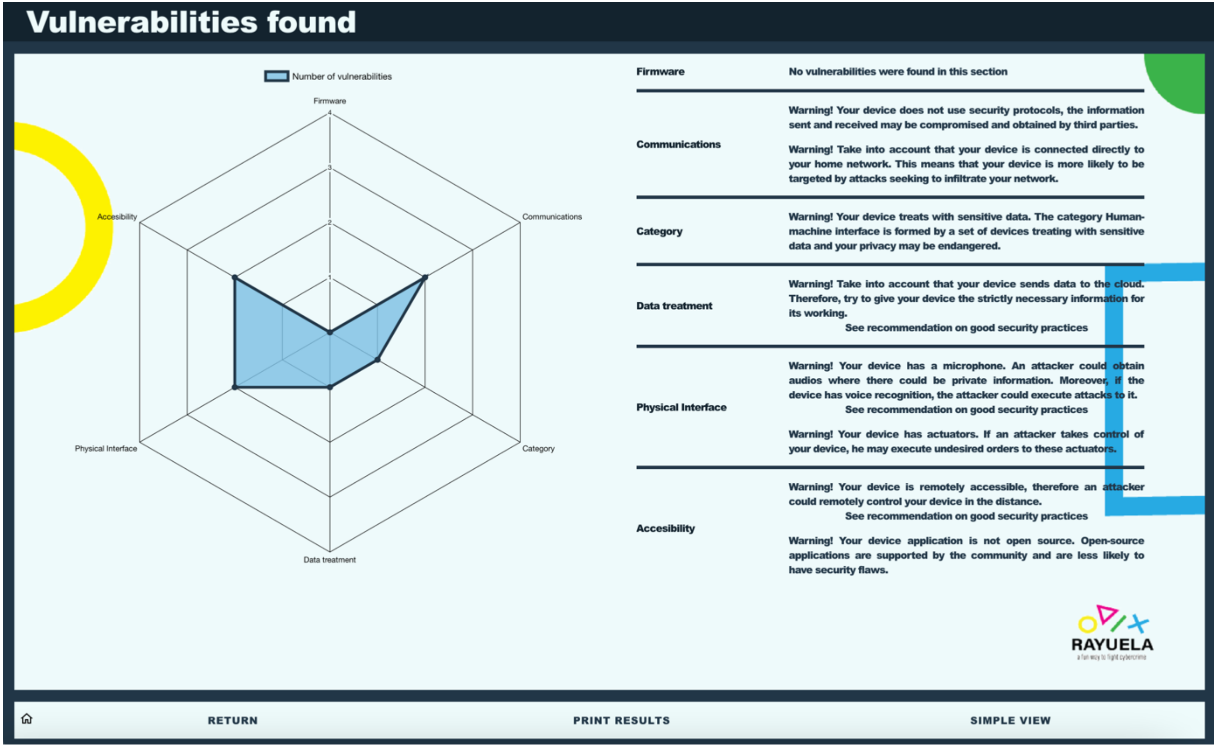
RAYUELA

Welcome!

In the next application you will be able to assess the vulnerabilities of your IoT device through a simple questionnaire that will ask you about some characteristics of your device. Click on the button to start.

Figure 32. Automatic testing tool.

To do so, the user has to answer several questions related to device characteristics such as communication protocols, category, or physical interface, etc. These questions vary depending on the answers given. Since the user may not know the concepts related to some of the questions, the application includes pop-up windows with explanations of some terms that may be complex to understand. At the end of the process, the application displays a graphical comparison of all vulnerabilities related to the connected device, along with relevant recommendations, as you can see in Figure 33. This can be accessed in "Automatic testing" section.

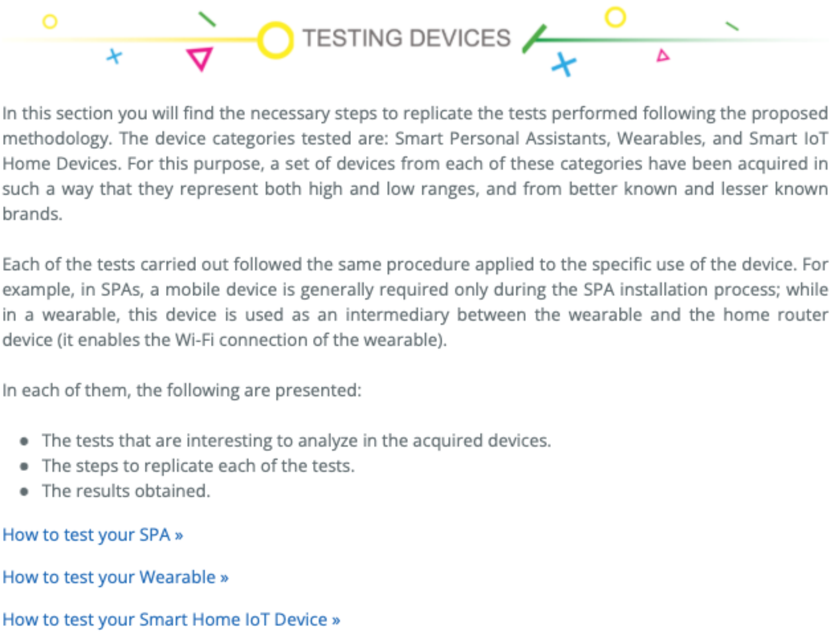


Vulnerabilities found

Firmware	No vulnerabilities were found in this section
Communications	Warning! Your device does not use security protocols, the information sent and received may be compromised and obtained by third parties. Warning! Take into account that your device is connected directly to your home network. This means that your device is more likely to be targeted by attacks seeking to infiltrate your network.
Category	Warning! Your device treats with sensitive data. The category Human-machine interface is formed by a set of devices treating with sensitive data and your privacy may be endangered.
Data treatment	Warning! Take into account that your device sends data to the cloud. Therefore, try to give your device the strictly necessary information for its working. See recommendation on good security practices
Physical Interface	Warning! Your device has a microphone. An attacker could obtain audios where there could be private information. Moreover, if the device has voice recognition, the attacker could execute attacks to it. See recommendation on good security practices Warning! Your device has actuators. If an attacker takes control of your device, he may execute undesired orders to these actuators.
Accesibility	Warning! Your device is remotely accessible, therefore an attacker could remotely control your device in the distance. See recommendation on good security practices Warning! Your device application is not open source. Open-source applications are supported by the community and are less likely to have security flaws.

Figure 33. Example of Amazon Echo Dot 4 results and recommendations.

While it is true that this tool is less precise than the tests themselves, the steps to follow to perform the tests have been included in the “Manual testing” section, see Figure 34. The categories included in the platform are SPAs, smart home IoT devices, and wearables.



TESTING DEVICES

In this section you will find the necessary steps to replicate the tests performed following the proposed methodology. The device categories tested are: Smart Personal Assistants, Wearables, and Smart IoT Home Devices. For this purpose, a set of devices from each of these categories have been acquired in such a way that they represent both high and low ranges, and from better known and lesser known brands.

Each of the tests carried out followed the same procedure applied to the specific use of the device. For example, in SPAs, a mobile device is generally required only during the SPA installation process; while in a wearable, this device is used as an intermediary between the wearable and the home router device (it enables the Wi-Fi connection of the wearable).

In each of them, the following are presented:

- The tests that are interesting to analyze in the acquired devices.
- The steps to replicate each of the tests.
- The results obtained.

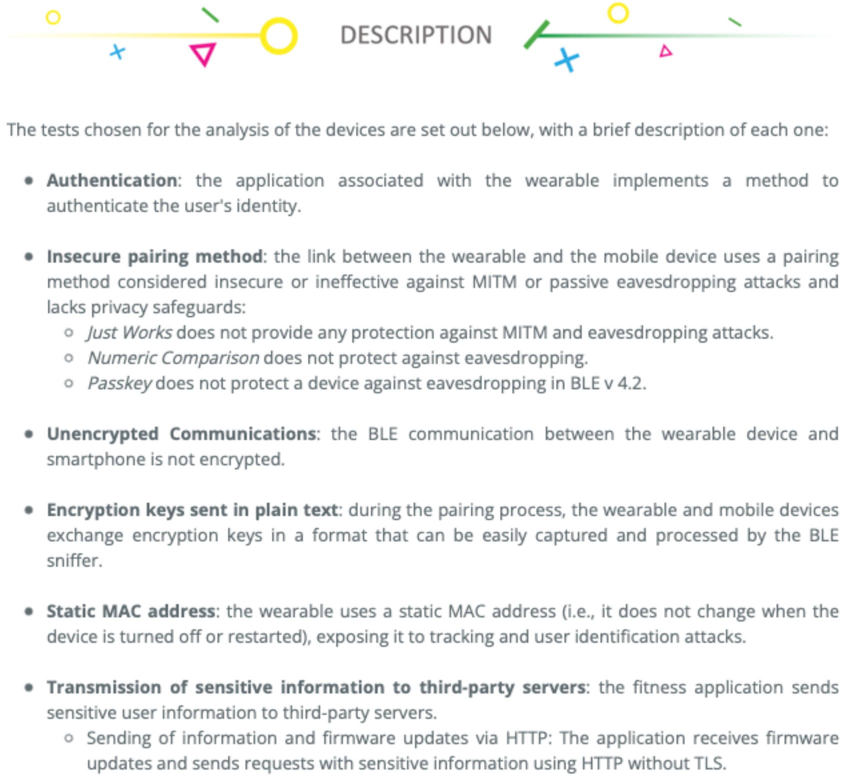
How to test your SPA »

How to test your Wearable »

How to test your Smart Home IoT Device »

Figure 34. Devices manual testing.

For each of them, the main security and privacy issues interesting to be studied have been described as shown in Figure 35 (an example of wearable devices). In each of the categories, common steps have been extracted for the security and privacy analysis tests to be performed on each brand and model of connected device. These steps, defined in the “Test with us!” section of the platform, allow the interested user to replicate the tests performed, see Figure 36.

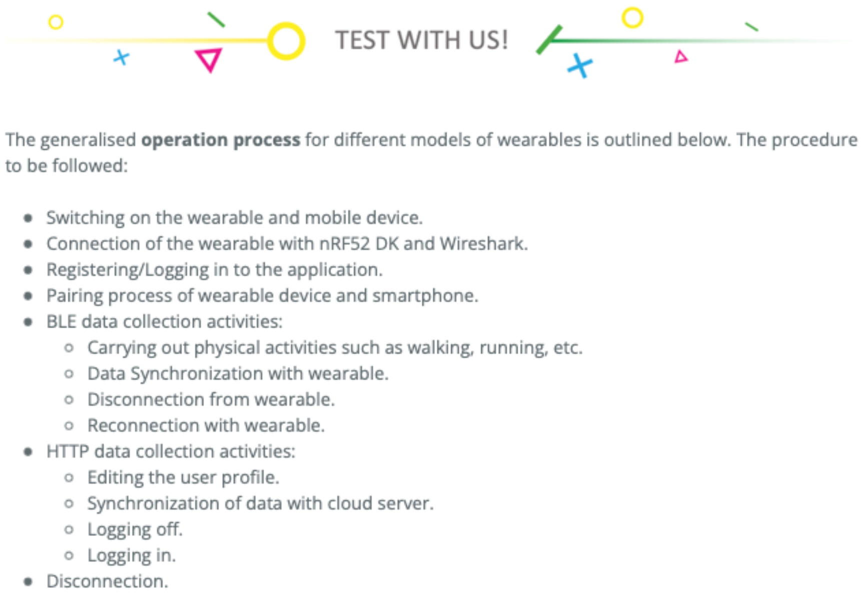


DESCRIPTION

The tests chosen for the analysis of the devices are set out below, with a brief description of each one:

- **Authentication**: the application associated with the wearable implements a method to authenticate the user's identity.
- **Insecure pairing method**: the link between the wearable and the mobile device uses a pairing method considered insecure or ineffective against MITM or passive eavesdropping attacks and lacks privacy safeguards:
  - *Just Works* does not provide any protection against MITM and eavesdropping attacks.
  - *Numeric Comparison* does not protect against eavesdropping.
  - *Passkey* does not protect a device against eavesdropping in BLE v 4.2.
- **Unencrypted Communications**: the BLE communication between the wearable device and smartphone is not encrypted.
- **Encryption keys sent in plain text**: during the pairing process, the wearable and mobile devices exchange encryption keys in a format that can be easily captured and processed by the BLE sniffer.
- **Static MAC address**: the wearable uses a static MAC address (i.e., it does not change when the device is turned off or restarted), exposing it to tracking and user identification attacks.
- **Transmission of sensitive information to third-party servers**: the fitness application sends sensitive user information to third-party servers.
  - Sending of information and firmware updates via HTTP: The application receives firmware updates and sends requests with sensitive information using HTTP without TLS.

Figure 35. Security and privacy issues to be tested.



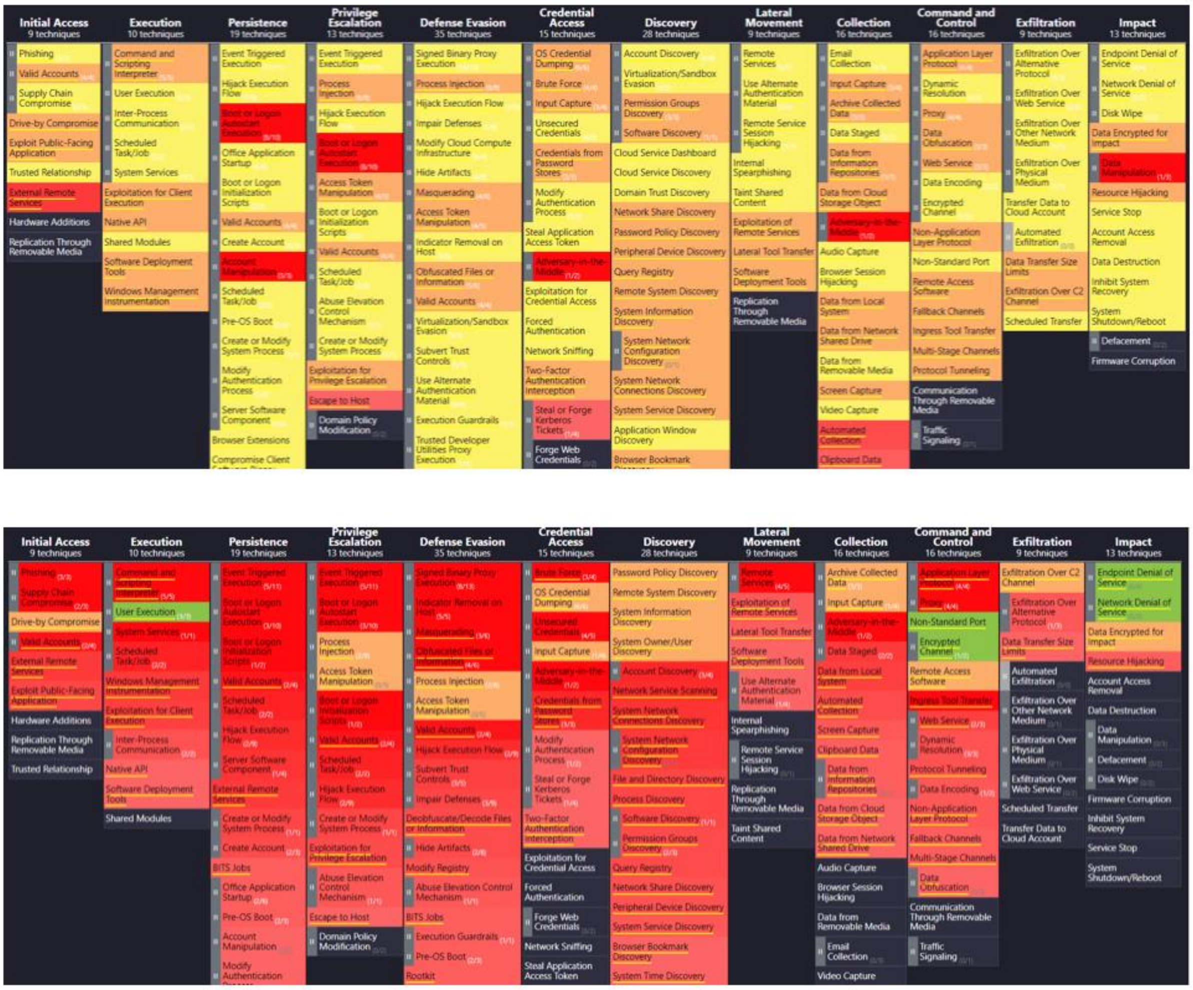
TEST WITH US!

The generalised **operation process** for different models of wearables is outlined below. The procedure to be followed:

- Switching on the wearable and mobile device.
- Connection of the wearable with nRF52 DK and Wireshark.
- Registering/Logging in to the application.
- Pairing process of wearable device and smartphone.
- BLE data collection activities:
  - Carrying out physical activities such as walking, running, etc.
  - Data Synchronization with wearable.
  - Disconnection from wearable.
  - Reconnection with wearable.
- HTTP data collection activities:
  - Editing the user profile.
  - Synchronization of data with cloud server.
  - Logging off.
  - Logging in.
- Disconnection.

Figure 36. Steps to be followed for the test replication.

The results obtained from the tests developed for each category are presented as a conclusion of the information extracted. In addition, it is interesting to contrast these results with those obtained from other sources of information. This is the case of MITRE ATT&CK, which is an open database with tactics and techniques used by cyber attackers in the context of user security and privacy. Therefore, a visibility and detection analysis were performed to compare the carried out tests with real-world observations. By selection specific groups focused on technological devices such as those tested, it is analysed which technique are most likely on these devices. For each of the device categories, several techniques ranked in the MITRE matrices are selected based on the tests performed. Seven of these techniques are remarked due to the poor visibility and detection results obtained. See Figure 37.



Initial Access 9 techniques	Execution 10 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 35 techniques	Credential Access 15 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Phishing	Command and Scripting Interpreter	Event Triggered Execution	Event Triggered Execution	Signed Binary Proxy Execution	OS Credential Dumping	Account Discovery	Remote Services	Email Collection	Application Layer Protocol	Exfiltration Over Alternative Protocol	Endpoint Denial of Service
Valid Accounts	User Execution	Hijack Execution Flow	Process Injection	Process Injection	Brute Force	Virtualization/Sandbox Evasion	Use Alternate Authentication Material	Input Capture	Dynamic Resolution	Exfiltration Over Web Service	Network Denial of Service
Supply Chain Compromise	Inter-Process Communication	Boot or Logon Autostart Execution	Hijack Execution Flow	Hijack Execution Flow	Input Capture	Permission Groups Discovery	Remote Service Session Hijacking	Archive Collected Data	Proxy	Exfiltration Over Other Network Medium	Disk Wipe
Drive-by Compromise	Scheduled Task/Job	Office Application Startup	Boot or Logon Autostart Execution	Impair Defenses	Unsecured Credentials	Software Discovery	Internal Spearphishing	Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Data Encrypted for Impact
Exploit Public-Facing Application	System Services	Boot or Logon Initialization Scripts	Access Token Manipulation	Modify Cloud Compute Infrastructure	Credentials from Password Stores	Cloud Service Dashboard	Taint Shared Content	Data from Information Repositories	Web Service	Transfer Data to Cloud Account	Data Manipulation
Trusted Relationship	Exploitation for Client Execution	Valid Accounts	Boot or Logon Initialization Scripts	Hide Artifacts	Modify Authentication Process	Cloud Service Discovery	Exploitation of Remote Services	Data from Cloud Storage Object	Data Encoding	Automated Exfiltration	Resource Hijacking
External Remote Services	Native API	Create Account	Valid Accounts	Masquerading	Steal Application Access Token	Domain Trust Discovery	Lateral Tool Transfer	Adversary-in-the-Middle	Encrypted Channel	Data Transfer Size Limits	Service Stop
Hardware Additions	Shared Modules	Account Manipulation	Scheduled Task/Job	Access Token Manipulation	Adversary-in-the-Middle	Network Share Discovery	Software Deployment Tools	Audio Capture	Non-Application Layer Protocol	Exfiltration Over C2 Channel	Account Access Removal
Replication Through Removable Media	Software Deployment Tools	Scheduled Task/Job	Abuse Elevation Control Mechanism	Indicator Removal on Host	Exploitation for Credential Access	Password Policy Discovery	Replication Through Removable Media	Browser Session Hijacking	Non-Standard Port	Scheduled Transfer	Data Destruction
	Windows Management Instrumentation	Pre-OS Boot	Create or Modify System Process	Obfuscated Files or Information	Forced Authentication	Peripheral Device Discovery		Data from Local System	Remote Access Software		Inhibit System Recovery
		Create or Modify System Process	Exploitation for Privilege Escalation	Valid Accounts	Network Sniffing	Query Registry		Data from Network Shared Drive	Fallback Channels		System Shutdown/Reboot
		Modify Authentication Process	Escape to Host	Virtualization/Sandbox Evasion	Two-Factor Authentication Interception	Remote System Discovery		Data from Removable Media	Ingress Tool Transfer		Defacement
		Server Software Component	Domain Policy Modification	Subvert Trust Controls	Steal or Forge Kerberos Tickets	System Information Discovery		Screen Capture	Multi-Stage Channels		Firmware Corruption
		Browser Extensions		Use Alternate Authentication Material	Forge Web Credentials	System Network Configuration Discovery		Video Capture	Protocol Tunneling		
		Compromise Client		Execution Guardrails		System Network Connections Discovery		Automated Collection	Communication Through Removable Media		
				Trusted Developer Utilities Proxy Execution		System Service Discovery		Clipboard Data	Traffic Signaling		
						Application Window Discovery					
						Browser Bookmark					

Initial Access 9 techniques	Execution 10 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 35 techniques	Credential Access 15 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Phishing	Command and Scripting Interpreter	Event Triggered Execution	Event Triggered Execution	Signed Binary Proxy Execution	Brute Force	Password Policy Discovery	Remote Services	Archive Collected Data	Application Layer Protocol	Exfiltration Over C2 Channel	Endpoint Denial of Service
Supply Chain Compromise	User Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Indicator Removal on Host	OS Credential Dumping	Remote System Discovery	Exploitation of Remote Services	Input Capture	Proxy	Exfiltration Over Alternative Protocol	Network Denial of Service
Drive-by Compromise	System Services	Boot or Logon Initialization Scripts	Process Injection	Masquerading	Unsecured Credentials	System Information Discovery	Lateral Tool Transfer	Adversary-in-the-Middle	Non-Standard Port	Data Transfer Size Limits	Data Encrypted for Impact
Valid Accounts	Scheduled Task/Job	Valid Accounts	Access Token Manipulation	Obfuscated Files or Information	Input Capture	System Owner/User Discovery	Software Deployment Tools	Data Staged	Encrypted Channel	Automated Exfiltration	Resource Hijacking
External Remote Services	Windows Management Instrumentation	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection	Adversary-in-the-Middle	Account Discovery	Use Alternate Authentication Material	Data from Local System	Remote Access Software	Exfiltration Over Other Network Medium	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Hijack Execution Flow	Valid Accounts	Access Token Manipulation	Credentials from Password Stores	Network Service Scanning	Internal Spearphishing	Automated Collection	Ingress Tool Transfer	Exfiltration Over Physical Medium	Data Destruction
Hardware Additions	Inter-Process Communication	Server Software Component	Scheduled Task/Job	Valid Accounts	Modify Authentication Process	System Network Connections Discovery	Remote Service Session Hijacking	Screen Capture	Web Service	Exfiltration Over Web Service	Data Manipulation
Replication Through Removable Media	Native API	External Remote Services	Hijack Execution Flow	Hijack Execution Flow	Steal or Forge Kerberos Tickets	System Network Configuration Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Scheduled Transfer	Defacement
Trusted Relationship	Software Deployment Tools	Create or Modify System Process	Create or Modify System Process	Subvert Trust Controls	Two-Factor Authentication Interception	File and Directory Discovery	Taint Shared Content	Data from Information Repositories	Protocol Tunneling	Transfer Data to Cloud Account	Disk Wipe
	Shared Modules	Create Account	Exploitation for Privilege Escalation	Impair Defenses	Exploitation for Credential Access	Process Discovery		Data from Cloud Storage Object	Data Encoding		Firmware Corruption
		BITS Jobs	Abuse Elevation Control Mechanism	Deobfuscate/Decode Files or Information	Forced Authentication	Software Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Inhibit System Recovery
		Office Application Startup	Escape to Host	Hide Artifacts	Forge Web Credentials	Permission Groups Discovery		Audio Capture	Fallback Channels		Service Stop
		Pre-OS Boot	Domain Policy Modification	Modify Registry	Network Sniffing	Query Registry		Browser Session Hijacking	Multi-Stage Channels		System Shutdown/Reboot
		Account Manipulation		Abuse Elevation Control Mechanism	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Data Obfuscation		
		Modify Authentication Process		BITS Jobs		Peripheral Device Discovery		Email Collection	Communication Through Removable Media		
				Execution Guardrails		System Service Discovery		Video Capture	Traffic Signaling		
				Pre-OS Boot		Browser Bookmark Discovery					
				Rootkit		System Time Discovery					

Figure 37. Visibility and detection analysis matrices with MITRE ATT&CK.

All the extracted information has been contrasted with our own results and displayed on the Open Access Platform. In this way, a set of recommendations are offered with the sole objective of avoiding or mitigating the exposed problems. Analysis of the results shows that, in general, most low-cost devices present a greater amount of 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 shared through insecure connections with third-party servers.

Thus, the recommendations offered are as follows:

- First, users must be aware of the information (data) that each device captures during its use. For this, it is necessary, in some cases, to read and understand the privacy policy set by the device or the underlying management application. In addition, it is important to limit the information shared with the applications, giving access only to the data necessary for their operation.

- Second, it is important to use well-configured users to interact with the devices and their management applications. For example, it is interesting to use a different username and password than the usual ones for each application, using key rings to safeguard more complex keys. From the point of view of configuring the devices, it is important to give them an identifying name and hide their MAC address if possible. A representative name facilitates unequivocal identification by the user for pairing with other devices or the local Internet network. Furthermore, the MAC address hiding prevents some attacks made through this identifier.
- Finally, it is essential to ensure that devices that use voice as a method of interaction can recognise the user. In general, this type of device has the necessary tools to perform this recognition. This operation, together with the possibility of establishing different or non-default activation words, allows for reducing the likelihood that agents, external to the user's environment, can carry out action orders for this type of device.

2 Human factors affecting the vulnerability and risks associated to connected devices

2.1 Human Factors Affecting Cybersecurity

In this section, we have analysed the human factors that could play a role in cybersecurity. In the X-Force Threat Intelligence Index 2018 report by IBM security researchers, it was revealed that 95% of cybersecurity incidents are due to human error [9]. To reach this conclusion, they analysed the causes of various security incidents publicly disclosed throughout 2015, 2016, 2017, and 2018.

2.1.1 Demographic Factors

2.1.1.1 Age

Some studies indicate adolescents seem to become more aware of risks with age and experience. Early adolescents tend to be more trusting, naive, and attention-seeking, hence being easier targets [10]. However, it is noteworthy that late adolescents are also more likely to engage in risky online behaviours [11] due to puberty, biopsychosocial changes, and their tendency to experiment with self-identity and to discover the environment [12], [13]. Besides, late adolescents tend to receive more unwanted sexual solicitations, practice more the exchange of sexual messages (sexting), interact more with unknown people, and talk less with their parents about their online activities [14].

2.1.1.2 Gender

Some studies show that girls tend to practice protective behaviour more than boys. Girls tend to talk more with their parents about their online activity, and boys tend to interact more with unknown people. Perhaps this is caused by gender socialization (i.e., in general, boys tend to have a different perception of risk due to the implicit ideal of bravery in masculinity) and facts such as that girls receive more unwanted sexual solicitations than boys (i.e., girls have more experience dealing with negative online situations) [14].

2.1.1.3 Internet Usage

Frequent Internet users are at greater risk for encountering online risks such as meeting with strangers, sexting, and cyberbullying [13]. Besides, Internet addiction and dependency behaviours seem to be a predictor of risky online behaviours [15].

2.1.2 Psychological Factors

2.1.2.1 The Perception of Risk

A variety of factors led to perceive risk as:

1) Voluntary/involuntary;
2) Familiar/unfamiliar;
3) Controllable/uncontrollable;

4) Fair or unfair;
5) Whether the risk causes ‘dread’.

When judging online risks, it would depend on the ability to control or avoid the risk, the dread of consequences, the unfamiliarity, and the immediacy of consequences [16].

Blythe and Camp explain that the motivation to apply security mechanisms depends on the perception of susceptibility to exogenous security threats, their potential severity, and the cost and efficacy of preventive/mitigating behaviours [17]. The trust in the place/organization is also relevant.

The perception of risk is related to both safe behaviours and self-efficacy. This suggests that people who have higher risk perception and are familiar with previous attacks may practice safer behaviour and develop a higher confidence in their ability to mitigate risks. Higher risk perception also correlates with a higher privacy attitude [18].

Teenagers tend to show more confidence about perceived risks than those they face. They tend to be over-confident, for example, when labelling genuine emails [19]. Minors with a higher perception of risks have exhibited more protection skills. This study also found a relation between that perception and parent intervention and healthier practice [20]. In the case of teenagers, unlike adults, personal norms might be a more decisive factor for security behaviours. A feeling of embarrassment or guilt would be stronger than the fear of being hacked.

2.1.2.2 Self-Efficacy

Each person’s beliefs in his or her capabilities and the possibilities of being in control have a significant influence when making decisions or accepting online risks [17]. In some studies, it has been observed that men feel more confident in their ability; however, no differences have been found in behaviour. There were differences across countries, the USA having more significant differences than India and United Arab Emirates, and USA men perceiving higher levels of self-efficacy than other men. In general, “risks tend to be judged lower by men than women and by white people than by people of colour” [18].

There is no further processing when the perceived threat is low, like analysing efficacy (Parallel Process Model). If the threat grows and self-efficacy is perceived as low, the person can deny the risk or even perform riskier behaviours to avoid fear and anxiety:

> *“Individuals who judge themselves to be effective in managing potential threats may feel neither fear nor avoid threats. On the contrary, if people judge themselves as ineffective in exercising control over potential threats, they react with stress and do not want to have any contact with them, therefore avoiding them.”* [17]

2.1.2.3 Personality Traits (Big Five Personality Traits [21])

- <u>Conscientiousness (efficient/organized vs. extravagant/careless)</u>:

Conscientiousness is a tendency to show self-discipline, act diligently, and strive for achievement against external measures or expectations. It is related to the way people control, regulate, and direct their impulses. Impulsivity and spontaneity (low level of conscientiousness) are highly correlated with online risk behaviours [15]. Hard-working, organized, and detailed-oriented people tend to be more secure online.

- Extraversion (outgoing/energetic vs. solitary/reserved):

Extraversion is characterized by breadth of activities, urgency of external activities/situations, and energy creation from external means. This trait is characterized by a pronounced engagement with the outside world. Extraverts enjoy interacting with people and are often perceived as energetic people. Lonely people with low levels of extroversion seem to become victims more often than others.

- Agreeableness (friendly/compassionate vs. critical/rational):

The trait of agreeableness reflects individual distinctions in the general concern for social harmony. Agreeable individuals value getting along with others, even if they are strangers. They tend to be considerate, kind, generous, trusting, and trustworthy, helpful, and willing to compromise their interests with others. Agreeable people also have an optimistic view of human nature. Disagreeableness people tend to be more sceptical about the motives of others' actions/petitions. Agreeable people who are inclined to be kind to strangers and compassionate to others tend to fall more for deception or manipulation.

- Neuroticism (sensitive/nervous vs. resilient/confident):

Neuroticism is the tendency to experience negative emotions, such as anger, anxiety, or depression. It is sometimes referred to as emotional instability and is inversely correlated to self-efficacy [18]. On the one hand, people with high levels of neuroticism are less trusting of others and have a greater sense of danger in everyday situations, which in theory, makes them more cautious online. On the other hand, emotional instability is correlated with social exclusion and loneliness, which influences their communication with family and friends about their online activities.

- Openness to experience (inventive/curious vs. consistent/cautious):

Openness to experience is a general appreciation of art, excitement, adventure, unusual ideas, imagination, curiosity, and a variety of experiences. People open to experience are intellectually curious, open to emotions, sensitive to beauty, and willing to try new things. High openness can be perceived as unpredictability or lack of focus, and more likely to engage in risky behaviours or drug-taking [22].

2.1.2.4 Locus of Control

People with the perception that their online security is in the hands of companies or governments (responsibility external to the individual) will take fewer steps to protect themselves and be less cautious [17].

2.1.2.5 Other Psychological Effects

- The Online Disinhibition Effect:

The online disinhibition effect is the lack of self-containment one feels when communicating online compared to communicating in person. People generally feel safer saying things online that they would not say in real life because they can remain completely anonymous and invisible behind the computer screen. In addition to anonymity, other factors such as asynchronous communication, empathy deficit or individual personality, and cultural factors also contribute to online disinhibition.

- Learned Helplessness:

Learned helplessness is the behaviour shown by a subject after enduring repeated aversive stimuli beyond his control. Lack of knowledge (about attacks or avoiding them) could lead to accepting being a victim. If the user thinks that he/she will become a victim eventually, he/she may not take any measures to prevent it [17]. Over the past few decades, neuroscience has provided insight into learned helplessness: the brain's default state assumes that control is not present, and the presence of "help" is what is learned first. However, it is unlearned when a subject is faced with prolonged aversive stimulation.

2.1.3 Sociological Factors

2.1.3.1 Social and Family Relationships

Lack of communication usually leads to a failure to transmit knowledge or education in the correct use of the Internet and other technologies, and therefore typical risk situations are not avoided. The quality of interpersonal relationships and their sense of loneliness also influence the amount of time children spend online.

This human factor has important cultural and geographical components. Within European Union countries, the estimated percentage of teenagers who do not talk about their bad experiences online varies between 4% (France) and 30% (Estonia). Children who communicate openly about their online activity and negative situations during this time are less likely to act in risky ways on the Internet. Criminals often seek out socially or familiarly vulnerable victims because they (empirically) know that they are more likely to succeed in their attack.

Regarding parental supervision:

- Parental overprotection decreases the child's independence. Therefore, it can be counterproductive and lead children to excessive Internet use and rebellious behaviour [23].

- Parental monitoring/supervision from parents (using filters, checking the online history, sitting with the child while on the Internet) does not significantly affect online children's behaviour. It is much more critical that parents understand the child and know how to communicate with him/her [24].

- Parental care and general family support are related to open communication. Communication is a more decisive factor than any restriction or parental monitoring since a child that communicates about their activity and negative situations on the Internet is less likely to act risky while online.

2.1.3.2 Privacy Attitude:

Attitude to privacy may be culturally influenced: In Halevi et al.'s research [18], U.S. participants shared more information online than participants from India, United Arab Emirates, and Ghana. However, the level of education of each person also plays an essential role.

2.1.3.3 Socioeconomic Status:

Families with lower incomes are related to lower levels of education (especially technological education). According to Mitchell et al. [25], [26], the educational level of the parents is more relevant than the income itself as a risk factor for suffering online grooming. However, the socioeconomic status has also an impact on the quality of the IoT devices purchased. Cheaper IoT devices are highly related with lower-quality security layers, as discussed in section 2.

2.1.3.4 Peer Influence/Pressure:

Children tend to be more influenced by social pressure than adults, causing them to attempt to imitate some behaviours to become a part of the community, impress, or fit within a specific group. This behaviour can assiduously lead the child into risky situations [9].

2.2 Relationship between human factors and technological threats

Having analysed the human factors that could play a role in cybersecurity, in this section we will relate them to the security and privacy issues analysed in this deliverable (Table 10). To do so, we will use the concept of attack vectors ("entry gates") in which the user intervenes.

- The vectors of "weak passwords" and "bad/no privacy and security settings" are related to the configuration performed by the user, typically the first few times the device is used.
- "Low-end devices" refers to low-quality devices, which are usually low-priced as well.
- The "Phishing, Vishing, and Smishing" attack vectors are social engineering methods based on an impersonation of a legitimate entity (e.g., bank, social network, public entity) with which we feel confident. These messages are usually of an urgent and attractive nature to prevent victims from having second thoughts. These attacks take advantage of a lack of critical attitude and lack of attention to details (e.g., the fraudulent link is usually like the one of the impersonated entities but never the same).
- The "Baiting and Spam" attack vectors are social engineering methods based on using a price, a discount, or some material/economic advantage to gain access to our devices or to obtain sensitive personal information. Spam is more focused on advertising messages, while baiting tries to catch us through the excitement of "having won a prize" or "an incredible discount". Baiting can also be performed in person by making the user plug an infected device (e.g., USB) into his or her personal devices.

- The “Shoulder surfing” vector is another social engineering method based on in-person interaction where the offender watches our device while using it in public spaces. For example, entering a social network or bank account password on public transport without realizing that a person nearby is spying on us.

The security and privacy issues are defined as follows according to previous analysis:

- Spoofing: Impersonation of the identity of the user or the device.
- Lack or weak encryption: Exposure of data during the transfer of information between peers because these are exchanged in plain text or protected by unreliable or obsolete encryption methods.
- Lack or weak authentication: Obsolete or null authentication mechanisms that allow access to the device with a specific role.
- Uncontrolled voice interaction: Possibility of execution of voice commands by strangers or unauthorized users, as well as side-channel attacks. This security issue considers problems related with VMA, VSA and hidden voice commands attacks.
- Code injection: Execution of malicious commands prepared to modify the common operation of the system or facilitate unauthorized access to protected parts or data. A specific attack included in this category is the SQL injection.
- Data interception: Active or passive (sniffing) listening of communications between interconnected devices that goes unnoticed by common users. A common attack related with this issue is the MitM.
- Takeover: Taking full control of the device to access data or carry out attacks that require cooperation between connected devices, such as the DDoS attack.
- User data being compromised: Operation of the connected device, the underlying server, or third-party applications involving the loss, misuse, or unauthorized access of user data.
- Violation of privacy laws: Improper use of sensitive and / or personal data that implies a total or partial violation of specific privacy laws such as the GDPR, COPPA, etc.
- Lack of control and understanding: Loss of control over the management of user data and/or ignorance of the use made by the underlying devices and applications or services. This issue considers the user perception over what happen with the personal data managed by the device or underlaying application.

Table 10. Relationship between human factors and security and privacy issues.

			Human-Intervened Cyber-Attack Vectors					
			Weak Passwords	Bad/None Privacy and Security Settings	Low-end Devices	Phishing, Vishing, and Smishing	Baiting and Spam	Shoulder Surfing
Human Factors	Demographic	Age (Being Older)	-	-	-	-	-	-
		Gender (Being a Boy)	x	x	x	+	+	+
		Excessive Internet Use/Addiction	x	x	x	+	+	+
	Psychological	Low Perception of Risk	++	++	+	++	++	++
		Low Self-Efficacy	+	+	x	+	+	+
		Low levels of Conscientiousness (Impulsivity)	+	+	x	++	++	+
		Low levels of Extraversion (Loneliness)	x	x	x	+	+	-
		High levels of Agreeableness (friendly/confident)	+	+	x	++	++	++
		High levels of Neuroticism (emotional instability)	-	-	x	-	-	-
		High levels of Openness to Experience (curious/risk-taker)	+	+	x	+	++	+
		External locus of control	++	++	+	+	+	+
		Learned Helplessness	++	++	x	+	+	+
	Sociological	Lack of Communication	x	x	x	+	+	x
		Parental Overprotection	x	x	x	x	+	x
		Careless Privacy Attitude	++	++	+	++	+	+
		Low Socioeconomic Status	x	+	++	+	+	x

			Human-Intervened Cyber-Attack Vectors					
			Weak Passwords	Bad/None Privacy and Security Settings	Low-end Devices	Phishing, Vishing, and Smishing	Baiting and Spam	Shoulder Surfing
		Compliance of Peer Pressure	x	x	x	+	+	x
Security and Privacy Issues	Security	Spoofing	✓			✓	✓	✓
		Lack or Weak Encryption		✓	✓			
		Lack or Weak authentication	✓	✓	✓			
		Uncontrolled voice interaction		✓				
		Code injection			✓	✓	✓	
		Data interception		✓	✓	✓	✓	✓
		Takeover	✓	✓		✓	✓	
	Privacy	User data being compromised	✓	✓	✓	✓	✓	✓
		Lack of control and understanding		✓		✓	✓	
		Violation of privacy laws			✓			

* ++ → high correlation

+ → medium correlation

x → no correlation

- → medium negative correlation

-- → high negative correlation

3 Cybercrime-as-a-Service exploiting IoT vulnerabilities

3.1 Introduction

IoT devices are increasingly becoming part of our daily life, facilitating our current lifestyle by bringing together a wide array of technologies that ultimately make possible what once was impossible. CaaS has seen in this emerging technology as an opportunity to increase their illegal services in other fields. EUROPOL, through the Internet Organised Crime Threat Assessment (IOCTA), which is published on a yearly basis, provides key recommendations to law enforcement, policy makers and regulators to allow them to respond to cybercrime in an effective and concerted manner. The 2020 IOCTA considers CaaS a key cybercrime issue. In fact, one of the three current priorities established in its introduction is “disrupting criminal activities related to attacks against information systems, particularly those following CaaS business models and working as enablers for online crime.”

To have a general picture of CaaS on IoT devices, several reports besides IOCTA have been analysed, with a particular emphasis on this issue. Next sections point out the most important outcomes extracted from them.

3.1.1 Standard&Poors report

In [27], Standard and Poor’s (S&P) highlights the cyber insurance premiums, which now total about $5 billion annually, will increase 20% to 30% per year on average soon. Also, they point out the small and medium-sized enterprises, “which have a considerable untapped demand for cyber insurance,” will be a key growth avenue.

3.1.2 Trend Micro report

The analysis performed by Trend Micro in [28] indicates that, at present, cybercriminals from different underground communities are in the process of refining attacks against IoT devices. Although monetization schemes for IoT-related attacks are not yet in place for many of the cybercriminal underground communities, the interest we found is headed in that direction.

Strong security measures should begin at the design phase and continue during the device deployment phase. Vulnerability management for different IoT devices plays a crucial role in minimizing attack openings.

In addition, this report analyses the most active communities on CaaS. It states that the Russian underground holds the most dynamic discussions on IoT-related attacks. In this community, cybercriminals often post ads for services or information that they are willing to pay for — and one example of these are vulnerabilities.

Monetization is the focus in this community and posts about fewer common devices show an exploration of new opportunities. For example, smart meters and gas pumps were also talked about, but only modified physical versions were being offered.

The second most active underground community that was mentioned is the Portuguese. The highlight of the findings in this community included a discussion on a criminal service that takes advantage of router infections, which they call “KL DNS.” It’s a redirection service that allows phishers to capture banking information, among others. What is of interest about this service is that it could be monetizing a previous mass infection of routers in Brazil in 2018 [29], which exploited a vulnerability in MikroTik routers. Cybercriminals could be on the lookout for opportunities to launch attacks of the same magnitude.

The English underground also displayed particular interest in exploiting connected printers, likely because of their ubiquity in industrial and office environments, which makes them potential entry points.

Finally, of interest in the Spanish underground community were methods for finding unprotected or unauthenticated devices that could be entry points for new attacks. An example of this is a discussion on how to use Google dork to find unprotected industrial refrigerators. The Spanish underground community even produced a software that allegedly could find specific devices using canned Shodan searches. The tool is called “Simple Active Bot,” and the seller claims it can allow remote access to the devices it finds.

3.1.3 Nokia Threat Intelligence report

According to the analysis carried out by Nokia in [30], IoT devices are now responsible for 32.72% of all infections observed in mobile networks, up from 16.17% in 2019. This trend lines up with the growing number of IoT devices that are now connected to mobile networks.

Comparing with 2019, the share occupied by infected Android devices has decreased, reflecting the shifting interest of the malicious actors toward IoT devices. Android-based devices still represent a major target in mobile networks.

Future networks will suffer due to a continuous increase of IoT botnets like Mirai or toolkits for mobile devices like DroidJack, which has recently been used to attack web services and network infrastructure.

3.1.4 IOCTA report

The IOCTA 2020 report [31] pointed out that IoT connected devices are an additional avenue for DDoS attacks. According to private sector respondents, connected devices which run on legacy operating systems, or which have weak or non-existent password protection could be compromised for implementing DDoS attacks or for criminals wanting to provide DDoS services for other criminals, particularly as connected devices could be used for lateral movement to infiltrate networks. Private sector respondents also observed IoT botnets emerging, and while these have been mostly experimental, not yet witnessed in use for specific scenarios, criminals may advertise these for DDoS attacks.

3.2 CaaS on IoT devices: an LEA perspective

CaaS on IoT devices poses many challenges to LEAs, who must cope with emerging threats that usually evolve at a higher pace than highly regulated and bureaucratized public organizations such as them.

Bearing this in mind, LEA partners from RAYUELA project have put in common how their organizations are coping with this phenomenon. One of the key tools employed for this purpose has been the SWOT analysis, which has already been previously used in different European and other international police forces with successful results. The SWOT analysis is described in the following sections.

3.2.1 Investigation based on SWOT analysis method

A SWOT analysis is a tool designed to understand the situation of an organization by making a complete list of its strengths, weaknesses, opportunities, and threats. It is essential for current and future decision making, as it provides a guideline for knowing what is being done well and everything that represents a current or potential challenge.

The analysis provides a broader picture of the organization, from its competitive advantages to the difficulties that may affect it. SWOT creates an accurate and useful diagnosis to detect internal and external problems, determine the course the organization should follow and provide greater knowledge about the value characteristics.

3.2.1.1 Strengths

In this part, LEAs' strengths coming from the internal factors are brought forward. These are elements on which LEA organizations have full control and are well performed. Things like resources, skilled labour, previous experience, assets, specialization, equipment, and so on, that might be beneficial for a proper development of their duties.

- What are your assets, and which one of those assets is the strongest?
- What actions do you perform best?
- What makes you better than others in fighting CaaS on IoT devices?
- Do you have prior experience in this issue?

3.2.1.2 Weaknesses

Like the strengths of a project, the weaknesses are also part of the internal environment. Weaknesses are negative elements or low points of the company that can affect the achievement of objectives and hinder the achievement of the expected results. Outdated office equipment, low wages or low incentives would fit in this category.

- What could you improve to fight CaaS?
- In what ways are you not efficient?
- What knowledge, skills and background are you missing?
- What areas do hackers have an advantage on?

3.2.1.3 Opportunities

Moving away from the internal environment, opportunities fall into the external factors. In short, these are situations in which the project can take advantage of, or are feasible for, the upcoming future as having a positive impact. Opportunities may come in the form of new regulations, positive market tendencies, economic factors, or high demand.

- What external changes will bring you opportunities?
- Will ongoing trends affect you in a positive manner?
- What could be done today that is not being done?
- Who can support you and how?
- Is the industry failing to satisfy the customer needs in any way?

3.2.1.4 Threats

This refers to external factors that may hinder the success of your objectives. For example, threats to your project may be legislative changes to which you must adapt. External factors, similarly, to the opportunities, are beyond the organization´s control. In other words, they are situations foreseen for the upcoming future that need to be avoided or at least try to mitigate their effects. However, as most external factors are in fact challenges, some can be perceived as both opportunities and threats, often providing a valuable indicator.

- What are the negative aspects/ tendencies in the current market?
- What obstacles are you currently facing in this mission?
- Who might cause you problems in the future and how?
- Are there potential competitors who can give you a competition in the future?
- What is the competition doing that might pose risks to your work?
- Are there any potential new regulations going to affect you?

3.2.2 SWOT Analysis results

An overall synopsis of the answers from the partners is presented. The answers will be presented in a form of a summary, to respect the confidential nature of the partners' responses.

3.2.2.1 Strengths

There is consensus among LEAs regarding proper cooperation and coordination channels to combat cybercrime. More specifically, LEAs in cybercrime specialised units, and cooperation at a national and international level are very adequate, being considered one of our biggest strengths against cybercrime on IoT devices. Cooperation between LEAS and industry is also good according to some LEAs.

Another strength mentioned by several LEAs is the use of OSINT technologies for investigative purposes. These have proven to be useful not only by themselves, but also as a complement to other digital forensic tools owned by private companies.

3.2.2.2 Weaknesses

RAYUELA LEAs have unanimously pointed out some intrinsic difficulties of CaaS that may hinder the investigations: CaaS usually involve multiple actors (from different countries), as well as heterogeneous infrastructures and legislation. On the one hand, this implies a lot of bureaucracy, creating difficulties to international cooperation through 'red tape' when investigating. On the other, the required number of resources to cope with it is considerably high.

Anonymisation techniques. For the average user, surfing the web does not, in general, offer much invisibility. If it is not an advertising agency trying to target you, it could be a criminal looking to steal your passwords. And although it is more difficult than it used to be, it is still possible to maintain anonymity online.

3.2.2.3 Opportunities

Although cooperation between LEAS and industry is good and it has been considered strength, several LEAs have considered public-private partnerships as an opportunity to better tackle cybercrime by strengthening ties and working together to combat threats and educate citizens.

Cybersecurity among its priority actions by the European Commission. The cybersecurity strategy is called "Open, Secure and Safe Cyberspace" and is responsible for providing an overview of how the EU should better prevent and deal with network disruptions and cyber-attacks. The main objective is, in line with EU policy, to promote and foster European values of freedom and democracy and to ensure the secure growth of the digital economy. To implement the EU's priorities, several measures are envisaged to strengthen the cyber resilience of IT systems. The aim is to reduce online crime and strengthen the EU's international cyber-security and cyber-defence policy and to develop the necessary industrial and technological resources.

Regulation on European data governance (Data Governance Act) will strengthen international cooperation. This proposal aims to promote a single market for data that favours agility in data management and, at the same time, is based on EU principles and values. The objective is to establish the foundations of a regulatory model based on the protection of the rights and interests affected, thus facilitating the optimal legal conditions to promote the re-use of public sector information with the appropriate guarantees.

3.2.2.4 Threats

Absence of borders in cyberspace. While technology has advanced at great speed and developed various unsuspected technical capabilities, legal frameworks, legal tools, and forums for public discussion of these issues have not. A difficult issue to resolve that should force states to take the initiative to find ways of regulatory conciliation; and to address the cases that have been raised.

Coordination between countries could be better. Law enforcement must combat highly complex cyber threats (such as malware, DDoS attacks and ransomware) and deal with new challenges, including the handling of large volumes of data, cross-border investigations, and new areas of expertise. As the cybercrime landscape continues to evolve, LEAs need to exchange information and knowledge with their counterparts around the world to provide a timely law enforcement intelligence-led response.

Lack of data encryption on IoT devices. More security is needed on these gateways to improve overall system security, determining that more efforts are needed to protect IoT-related data to ensure the privacy of consumers and brands. Due to the constant evolution of these technologies, it is very difficult to know how far IoT will advance in the services of the future. However, what is clear today is that there are many cybersecurity and user data privacy issues that may affect users.

Lack of authentication for accessing personally identifiable information on IoT devices. As people and devices become more connected, issues related to data protection and cybersecurity threat management become increasingly important. IoT devices can collect significant amounts of information about their users and their environment, including identifiable, confidential, and sensitive data. Unfortunately, early IoT devices have several vulnerabilities that can be easily exploited, making them easy targets for cybersecurity attacks.

3.3 Definition of action strategies

The most straightforward approach to developing strategies with the SWOT analysis can be resumed in the following four key points:

- build on your strengths
- minimize your weaknesses
- seize opportunities
- counteract threats

In this sense, following sections detail the main outcomes that have been extracted from the LEAs SWOT analysis.

3.3.1 Build on your strengths

3.3.1.1 Boosting legislative harmonisation

The Budapest Convention is an international treaty on crimes committed over the Internet and other computer networks, which deals with copyright infringement, computer fraud, child pornography and network security violations. Its main objective is to implement a common criminal policy aimed at protecting society against cybercrime, notably through the adoption of appropriate legislation and the promotion of international cooperation.

In practice, it is the only binding international instrument on this subject. It is intended as a guide for countries to develop comprehensive and aligned national legislation against cybercrime.

It also facilitates the adoption of measures to detect and prosecute cybercriminals, both nationally and internationally. The Budapest Convention has reinforced a process of legislative reform worldwide, thus facilitating a minimum of harmonization of legislation around the world. Although many efforts have been done, legislative harmonisation should be improved at a European level.

3.3.1.2 Boosting police and judicial cooperation

The EUROPOL is a central element of the Union's overall internal security architecture. Police cooperation and policies in terms of cybersecurity are still being developed, with a particular focus on the fight against terrorism, cybercrime, and other forms of crime. The main objective is to achieve a safer Europe for the benefit of all citizens of the Union, while respecting fundamental rights and data protection rules.

3.3.2 Minimize your weaknesses

3.3.2.1 Improving coordination

The Cybercrime Strategy outlines INTERPOL's plan to support member countries' efforts in their fight against cybercrime by good coordinating and facilitating specialized police capabilities.

It must be periodically reviewed to ensure that it maintains its relevance, continues to respond to new threats in the dynamic environment in which it operates, and responds to member countries' expectations.

3.3.2.2 Coping with anonymisation techniques

Cybercrime as a service takes advantage of the fact that technology is often ahead of the law and ahead of the knowledge of many professionals. Thanks to the existence of the Internet, where knowledge flows quite freely, it is not complicated to learn how to do certain things and contact other people through the different platforms and tools that this technology facilitates.

With regards to anonymity and impersonation, it is not too difficult to “disappear” in the virtual world, which makes it difficult to track down cybercriminals. Therefore, better tools and legislation to tackle these anonymisation techniques used with malicious purposes can help LEAs in the fight against cybercrime.

3.3.3 Seize opportunities

3.3.3.1 Boosting public-private collaboration on investigating crimes in ICT networks

Of all the types of crime, cybercrime continues to increase at the fastest rate. According to INTERPOL’s recent assessment of the global cyberthreat landscape, cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social, economic and health situation around the world.

The private sector plays a fundamental role in the ability to understand and act against cybercriminals. Only by ensuring that leading companies work side by side with law enforcement can we effectively respond to these cybercrime threats.

3.3.3.2 Boosting international cooperation

Collaboration between different international bodies is essential to respond effectively to ICT global threats.

In this sense, the European Data Governance Act, which is currently at a proposal phase, will provide a legislative framework for the governance of common European data spaces and for ensuring that the actions taken by Member States are coordinated with a view to create a single data market.

The Data Governance Act helps to address one of the main obstacles to its development: regulatory fragmentation. Besides. the proposal for a Data Governance Regulation seeks to make data more widely available for use by establishing a framework that increases trust in data intermediaries and strengthens data exchange mechanisms across the EU.

3.3.4 Counteract threats by improving data encryption and data standardization on IoT devices

With the rapid increase in the number of IoT devices in everyday life, both personal and professional, new cybersecurity challenges are emerging. While they are a step forward in our daily lives, these connected devices often lack security. This partly explains why vulnerabilities are being discovered and exploited every day.

Not everything remains the responsibility of IoT manufacturers. Aspects such as poor security practices (default or simple identification codes), unencrypted traffic and lack of network segmentation remain common failures attributable to human management. Therefore, encryption and standardizations must be improved to enhance the security of IoT devices.

4 Conclusions

This deliverable delves into the security and privacy vulnerabilities involved in the use of connected devices by minors. To do this, we start from the results of the previous task T2.1, where an exhaustive review of the principal vulnerabilities reported in the literature was carried out, and a selection of devices frequently used by young people, such as wearables, smart personal assistants, and smart home IoT devices, was done.

Based on this, a general methodology is defined to assess connected devices' privacy and security risks. This methodology involves using hardware equipment and software tools to monitor the exchange of packets between the devices and the Internet.

The application of the methodology to a specific set of selected devices makes it possible to verify that indeed, in many cases, there are security and privacy vulnerabilities, especially in low-cost devices. Among the principal vulnerabilities are those associated with weak authentication and encryption mechanisms (sometimes even lacking them), compromising user privacy and the possibility of being a victim of different types of cyberattacks.

In parallel to this development, the attacker’s perspective in this area is analysed. For this purpose, an IoT honeypot is designed and deployed to understand in a practical way how attackers act and what are the steps followed to breach the connected device. The honeypot has been already deployed, but results have not been obtained yet. As an additional source this information is also obtained from real databases such as the MITRE ATT&CK framework that provides information regarding the tactics and techniques preferred by attackers when carrying out an attack.

All this information is available for public consultation on an open access platform available at https://rayuelaproject.github.io/RAYUELA/ where the user can find the tests performed step by step, and even replicate them. In addition, for non-expert users, a connected device testing software tool has been developed that analyses the device based on answers given by the user to a set of questions. The tool concludes with a report of vulnerabilities found and recommendations for use.

Based on this, these recommendations are proposed to mitigate these vulnerabilities and their collateral effects: reading and understanding the privacy policies, limiting the information that the user shares to what is strictly necessary, using strong credentials, and not reusing them in different devices/applications.

After analysing cybersecurity problems from a technological point of view, we focus on studying the human factors that can influence minors' greater or lesser vulnerability to cyber threats. The analysis covers demographical (age, gender), psychological (perception of risk, self-efficacy, personality traits, locus of control), and sociological (social and family relationships, privacy attitude, socioeconomic status, peer influence/pressure) factors. The analysis establishes the relationship between these factors and the main threats to security and privacy previously identified. As a result, a table indicating the greater or lesser impact each aspect has on the different types of threats has been elaborated. These results are helpful when developing policies or measures to protect the vulnerability of specific user profiles or improve their experience with technology. They can also be beneficial for designing the serious game in RAYUELA. However, this is something to be addressed in WP3, considering other WP1 and WP2 inputs.

Finally, and given the growing importance of the CaaS phenomenon, it has specifically addressed how cybercriminals increasingly draw on exploiting vulnerabilities in IoT devices, taking advantage also of human factors. This becomes clear when analysing some relevant reports in this regard, such as those elaborated by various institutions and companies (EUROPOL, Trend Micro, Nokia Standard & Poor). Therefore, to prevent and combat the CaaS phenomenon, the role to be played by LEAs is considered vital. In this sense, the LEAs participating in RAYUELA have carried out a SWOT analysis, elaborating a complete list of strengths, weaknesses, opportunities, and threats that need to be considered. Based on this analysis, a series of strategic actions are proposed as the basis for current and future decision making.

References

[1] W. K. Zegeye, ‘Exploiting Bluetooth low energy pairing vulnerability in telemedicine’, 2015.

[2] T. Rosa, ‘Bypassing Passkey Authentication in Bluetooth Low Energy.’, IACR Cryptol EPrint Arch, vol. 2013, p. 309, 2013.

[3] Y. Ojha, ‘I hacked MiBand 3, and here is how I did it.’, Medium.org. https://medium.com/@yogeshojha/i-hacked-xiaomi-miband-3-and-here-is-how-i-did-it-43d68c272391

[4] A. Pratik, ‘How To Use Mi Band 5 Without The Mi Fit App’, TECHWISER. https://techwiser.com/use-mi-band-without-the-mi-fit-app/

[5] J. Franco et al., ‘A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, an Cyber-Physical Systems’, 2021,

[6] J. Gorriz, ‘Seguridad en Internet de las Cosas Honeypot to capture IoT-attack methods’, 2018

[7] Fuente, ‘Análisis de dispositivos wearable para menores desde un punto de vista de privacidad y seguridad’, 2021

[8] Shapes, "Integrating Xiaomi Mi Band 4 devices with smart mirror" [Online]. Available: https://arcogroup.bitbucket.io/shapes/integrating_miband_with_smart_mirror/

[9] C. Singleton, ‘IBM X-Force Threat Intelligence Index’, IBM, 2018. Accessed: Jul. 30, 2021. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence

[10] S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao, and S. J. Upadhyaya, ‘Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens’, IEEE Trans. Prof. Commun., vol. 52, no. 2, pp. 167–182, Jun. 2009, doi: 10.1109/TPC.2009.2017985.

[11] S. L. Escobar-Chaves and C. A. Anderson, ‘Media and risky behaviors’, Future Child., pp. 147–180, 2008.

[12] E. B. Dowell, A. W. Burgess, and D. J. Cavanaugh, ‘Clustering of Internet Risk Behaviors in a Middle School Student Population’, J. Sch. Health, vol. 79, no. 11, pp. 547–553, 2009, doi: 10.1111/j.1746-1561.2009.00447.x.

[13] M. Gámez-Guadix, E. Borrajo, and C. Almendros, ‘Risky online behaviors among adolescents: Longitudinal relations among problematic Internet use, cyberbullying perpetration, and meeting strangers online’, J. Behav. Addict., vol. 5, no. 1, pp. 100–107, Mar. 2016, doi: 10.1556/2006.5.2016.013.

[14] D. Smahel et al., ‘EU Kids Online 2020: Survey results from 19 countries. EU Kids Online’, 2020. doi: 10.21953/lse.47fdeqj01ofo.

[15] L. Hadlington, ‘Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours’, Heliyon, vol. 3, no. 7, p. e00346, Jul. 2017, doi:

10.1016/j.heliyon.2017.e00346.

[16] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, 'Guidelines for usable cybersecurity: Past and present', in 2011 Third International Workshop on Cyberspace Safety and Security (CSS), Sep. 2011, pp. 21–26. doi: 10.1109/CSS.2011.6058566.

[17] M. Bada and J. R. C. Nurse, 'Chapter 4 - The social and psychological impact of cyberattacks', in Emerging Cyber Threats and Cognitive Vulnerabilities, V. Benson and J. Mcalaney, Eds. Academic Press, 2020, pp. 73–92. doi: 10.1016/B978-0-12-816203-3.00004-6.

[18] T. Halevi et al., 'Cultural and psychological factors in cyber-security', in Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services, New York, NY, USA, Nov. 2016, pp. 318–324. doi: 10.1145/3011141.3011165.

[19] J. Nicholson, Y. Javed, M. Dixon, L. Coventry, O. D. Ajayi, and P. Anderson, 'Investigating Teenagers' Ability to Detect Phishing Messages', in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), Sep. 2020, pp. 140–149. doi: 10.1109/EuroSPW51379.2020.00027.

[20] I. Ramos Soler, C. López-Sánchez, and T. Torrecillas Lacave, 'Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital = Online risk perception in young people and its effects on digital behaviour', Comun. Rev. Científica Iberoam. Comun. Educ. Sci. J. Media Educ. 56 3 2018, pp. 71–79, 2018, doi: 10.3916/C56-2018-07.

[21] J. M. Digman, 'Personality Structure: Emergence of the Five-Factor Model', Annu. Rev. Psychol., vol. 41, no. 1, pp. 417–440, 1990, doi: 10.1146/annurev.ps.41.020190.002221.

[22] B. Ambridge, Psy-Q: You know your IQ-now test your psychological intelligence. Profile Books, 2014.

[23] A. Faltýnková, L. Blinka, A. Ševčíková, and D. Husarova, 'The Associations between Family-Related Factors and Excessive Internet Use in Adolescents', Int. J. Environ. Res. Public. Health, vol. 17, no. 5, Art. no. 5, Jan. 2020, doi: 10.3390/ijerph17051754.

[24] A. K. Liau, A. Khoo, and P. Hwaang, 'Factors Influencing Adolescents Engagement in Risky Internet Behavior', Cyberpsychol. Behav., vol. 8, no. 6, pp. 513–520, Dec. 2005, doi: 10.1089/cpb.2005.8.513.

[25] K. J. Mitchell, D. Finkelhor, and J. Wolak, 'Online Requests for Sexual Pictures from Youth: Risk Factors and Incident Characteristics', J. Adolesc. Health, vol. 41, no. 2, pp. 196–203, Aug. 2007, doi: 10.1016/j.jadohealth.2007.03.013.

[26] K. J. Mitchell, D. Finkelhor, and J. Wolak, 'Youth Internet Users at Risk for the Most Serious Online Sexual Solicitations', Am. J. Prev. Med., vol. 32, no. 6, pp. 532–537, Jun. 2007, doi: 10.1016/j.amepre.2007.02.001.

[27] M. Adam, 'Cyber Risk In A New Era: Insurers Can Be Part Of The Solution', Sep.

2020. [Online]. Available: https://www.spglobal.com/ratings/en/research/articles/200902-cyber-risk-in-a-new-era-insurers-can-be-part-of-the-solution-11590046

[28] S. Hilt, V. Kropotov, F. Mercês, M. Rosario, and D. Sancho, ‘The internet of things in the cybercrime underground’, Trend Micro Res., 2019.

[29] N. TrendMicro, ‘Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign’, Aug. 2018. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign

[30] Nokia, ‘Nokia: Threat Intelligence Report 2020’, Comput. Fraud Secur., vol. 2020, no. 11, p. 4, Nov. 2020, doi: 10.1016/S1361-3723(20)30115-9.

[31] E. EUROPOL, ‘INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA)’, Oct. 2020. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Appendix. Tables

Table 11. Comparison of installation and interaction features of SPA.

SPA	Apple HomePod Mini	Google Home Mini / Google Nest Audio	Amazon Echo Show 5 / Echo Dot 4	Facebook Portal
Installation				
SPA installation	An *iCloud* account and an *Apple* device are required. Wi-Fi details, *Siri* and other preferences are shared from the *iPhone*.	A *Google* account is required. Wi-Fi details, *Google* account preferences and additional settings are shared from the mobile device.	An *Amazon* account is required to use the *Echos*. The Wi-Fi data is entered into the device and the *Alexa* settings are synchronized from the mobile device.	A *Facebook* account is required to use the *Facebook Portal*. The Wi-Fi data is entered into the device ant then the device is associated with the user account by using a parity code.
Connected accessories installation	It is possible to configure whether a user has permission to add or edit devices.	Permissions cannot be configured for home users. Anyone can add or edit accessories.	Only the house administrator can add devices and edit them with the *Alexa* application.	Anyone can enable the use or skills and plugins from the device software portal without confirmation, an even re-activate add-ons previously disabled by the main user.
Third-party skills installation	Third-party skills cannot be configured.	There is no third-party actions (skills) installation process. Knowing the activation	The house administrator can enable the use of skills from the *Amazon Alexa* app before using them, but a regular user can activate any skill	It is allowed by restricted to the device software portal.

		phrase, any action can be used.	from the *Echos* without confirmation, and even re-activate a skill previously disabled by the administrator.	
Interaction				
Interaction with SPA and connected devices	Voice and touch control can be deactivated. The use of multimedia devices can be disabled, and the control of connected accessories can be specified per user.	Media playback can be disabled for the device. It is not possible to define permissions from *Google Home*, being necessary to create a family in the external application *Family Link* and configure filters by device in the application *Google Home*.	The *Echo Show 5* provides controls to turn off camera and microphone. In case of Echo Dot 4, there is not camera, but it is possible to turn off the microphone. In both cases, there is no possibility to differentiate between users or to define permissions for specific interactions.	The device provides controls to turn off the camera and microphone. There is no possibility to differentiate between users or to define permissions for specific interactions.
Interaction with third-party skills	There is no possibility to interact with third-party skills.	There are no third-party action controls per user, it is necessary to create a content filter for the entire group of users in the house.	The house administrator can permit the use of skills from the *Amazon Alexa* app before they are used in the *Echo Show 5* or *Echo Dot 4*, but any user can trigger a skill from the *Echos* without confirmation.	The administrator can permit the user of skills from the device software portal app before they are used in the *Facebook Portal*, but any user can trigger and add-on without confirmation.

Table 12. Comparison of functionality, privacy, and security features of SPA.

SPA	Apple HomePod Mini	Google Home Mini / Google Nest Audio	Amazon Echo Show 5/Echo Dot 4/Facebook Portal
Functionality			
Payments and transactions	Payments or purchases from the *Apple HomePod Mini* are not supported.	Payments can be set up from the SPA. They support an additional authentication method based on the hardware of the device where the *Google Home* application is installed.	Payments can be made with the SPA via *Amazon 1 Click*. Additional confirmation methods can be configured via a voice profile or a four-digit code.
Possibility of creating “safe” profiles for minors	There is no possibility to create a user profile for minors, it is necessary to manually access every control and activate it.	This option is only available on *Android* devices. For other devices it is required to manually create content filters that affect all the users equally, although options such as payments are still active after applying these filters.	There is no dedicated option to set a safe use profile for minors. It is necessary to disable and restrict settings in each of the categories (media playback, web browser, payments, skills, etc.). It is no possible to restrict the use of connected accessories.
Privacy and security			
Control of answers containing personal information	It is necessary to activate voice recognition to provide answers containing personal information. Personal responses that may contain sensitive information require an additional authentication step with the smartphone. This feature can be disabled in the *Home* application	Personal responses are linked to the voice profile of the user. They can be disabled in the settings of the *Google Home Mini.*	There is no possibility to disable responses containing personal information. It is necessary to deactivate the functionalities completely since any user can invoke them.

SPA	Apple HomePod Mini	Google Home Mini / Google Nest Audio	Amazon Echo Show 5/Echo Dot 4/Facebook Portal
Authentication methods	Authentication through voice recognition. Activating the additional authentication step with the smartphone can prevent impersonation attacks with a voice recording of a legitimate user.	The device supports voice authentication, however, using a recording of a user invoking the SPA, it is possible to impersonate him, being able to perform any request later.	The device has voice recognition. But it is only used for personalization functions, for example in skills. It is not used for security purposes. A malicious actor can impersonate a legitimate user using a recording of the activation message, being able to make any request.
Non-human voice filtering	A pre-recorded activation message or a wake-up message read by a TTS system can invoke the assistant.	Messages from recordings and synthetic voices are not filtered.	Recorded messages and those originated by synthetic voices are not filtered.
Interaction with conversation history	It is possible to send a request to delete the conversation history from the servers, however, the history is not visible.	Comprehensive options are included to view, pause, and automatically delete the conversation history.	The device application offers complete options for viewing, deleting, and pausing the conversation history, including automatic deletion options.