Advanced Research on Information Systems Security, an International Journal

Paranoid OS: Wearable Trackers

Afonso Almeida [a*], Nuno Mateus-Coelho [b], Nuno Lopes [c]

[ab]*Polytechnic Institute of Cavado and Ave, 4750-810 Barcelos, Portugal*

[c]*2Ai – School of Technology, IPCA, Barcelos, Portugal*

[a]*Email: a13258@alunos.ipca.pt*

[b]*Email: ncoelho@ipca.pt*

[c]*Email: nlopes@ipca.pt*

Abstract

Throughout human evolution, communication has always played a central role in favor of the development and approximation of the species.

Within this project, the main objective is to analyze different wearable devices (more specifically fitness tracking devices) with the intention of presenting the strengths and weaknesses related to the security and privacy frameworks that these devices make use of.

To reach these objectives some devices will be acquired for testing, starting from the earliest point of the communication (Bluetooth connection) until the latter states (communications through the Internet).

"Paranoid" operating systems and methodologies have been developed and studied over the years, both for mobile and desktop systems in order to maintain the security and anonymity of their users, and although related studies have been in existence for some time, this proposal aims to develop an answer to a theme not very distinct, but more specific and modern "Paranoid OS: Wearable Trackers".

It is with this purpose in mind that the path taken by this technology will be presented in this document, considering what are the communication protocols, what data goes through these communication channels and finally where is the user's data.

Keywords: Communication; Wearables; Security; Operating Systems

1. Introduction

Within the context of a Master of Sciences in Computer Sciences Engineering, this research intends to extend the original POSMASWEB research, onto a new and more volatile field of action, the wearables. These devices have become popular in recent years, becoming in recent years a massive source of data and information, that is collected, stored and relayed to an unknown to the users, or without the user's knowledge [4].

This chapter is related to the theoretical positioning of the project, starting from the beginning of human communication, until the Internet emerges and consequently the wearables equipment that appeared along with the concept of "Internet of Things" ("IoT").

1.1. Context

Human beings made their appearance on planet Earth approximately two million years ago, without any means of communicating between themselves through language [1].

Throughout the years Human beings developed technics to solve this situation like body language, cave painting, using fire and stones, and finally through sounds [1].

Writing is the main technology of the Human race to collect, manipulate, retrieve and store communications and disseminate information, so it is possible to find traces of cuneiform writing as old as eight millennia before Christ [2].

In the current era, we have achieved the peak of the communication technologies through Internet, which has been considered one of the biggest social and technological achievement after the invention of the wheel and the control of fire [3], [28], offering to the world we know, one of the best forms of communications between technological devices.

Currently, and being more specific to the theme of this document, wearable technological devices are on high demand in the society [4].

These kinds of devices make use of "BLE" (Bluetooth Low Energy) technology in connections and communications [5], having become omnipresent and relatively cheap in the last years.

In this way, they have become excellent (and also cheap) tools in the research field (to conduct study cases) since they have the capability to collect activity data the whole day without limiting user freedom [6].

The main objective of these devices is related to personal use, and the whole process of data collecting starts from the earliest point in which the user connects the wearable device to their personal smartphone [7] (otherwise, most of the main functions of the wearable equipment will not be functional).

One of the biggest problems about these devices, corresponds to the misinformation that the users have (or merely the lack of important information) or because users don't really care, and also have no idea what information they will be providing, where and how it will be stored and what are the possible risks and conflicts that they might encounter [8], [32].

It is also important to have in consideration the quick appearance of the "sensor mania" concept in eco systems "IoT" [9], because users are progressively more and more exposed to 24/7 monitoring of their usual activities, performances and preferences in compliance with the large diffusion of the "IoT" systems that possess them [10].

1.2. Objectives

With this idea it is intended to evaluate and develop answers to questions related to security and risk perception of the wearable devices, regarding how them manipulate and store data.

Considering the increasing use of mobile/wearable equipment, and also considering that these contain operating systems in some cases free, and in others they possess a cost associated with the type of equipment, it is pertinent to know if the fact that they are free implies that sensitive personal information is shared as a mean of payment for the operating system, leading to the formulation of the following questions:

- Do health orientated applications, that collect biological data through mobile devices, guarantee the privacy and safety of the user?
- Are "mHealth" (mobile healthcare) applications truly agnostic in the various mobile platforms [31]?

In this project the following questions related to these devices will also be addressed:

- How is the data collected?
- How and where are those data used?
- Who owns the data?
- With whom is shared the data?
- How and for how long will the data be stored?
- What is the security of the involved technologies?
- How can users be safe?

2. Background

In this chapter it will be presented the project background related to the equipment that will be researched (wearable fitness tracking device), beginning by the definition and capabilities of these devices, the main communication protocols that encompass them and also some of the biggest concerns about the security and privacy that they provide.

2.1. Wearable Fitness tracking

A smartwatch, or in this specific case, a fitness tracker, is a wearable computer in the shape of a watch equipped

with multiple sensors, such that, these kinds of electronic equipment get embedded in our personal lives, and can be worn, carried, or even connected to the body [11].

A fitness tracking device is generally commercialized based on the premise that the manual and/or automatic data collection that it provides, stimulates users into adopting healthier habits [12] and also find "meaningful correlations between diet, exercise, sleep, and mental, physical, and cognitive well-being" [13]. Some examples of data collected by these devices sensor's:

- Height changes
- Hearth rate information
- Geolocation
- Time and sleeping periods
- Sleep quality
- Activity quality
- Type of activity

These kind of collected data can be controlled and/or owned by the individual or company that provides the tracking device and their associated systems as well [13].

In a market with such great amount of saturation as the mobile devices, this "IT" devices have been gradually gaining popularity and currently are a viable device that extends smartphones functionalities to a more intimate level, having advantages relative to others, like the place that they are worn and consequently the continuous connection with the body [14].

This extension is literal since these wearable devices are a mere complement to the mobile devices. Although wearable equipment functions independently of being connected to a smartphone, most of the functionalities required said connection [14].

The study of the communication protocol between the mobile device and the upload server could be supported by a software defined network environment [32] for assessing the information that is transmitted along with the privacy concerns of said data.

An example architecture of these devices is the following figure, related to Xiaomi's "MiBand", that shows the different connections required for every functionality to work as expected:

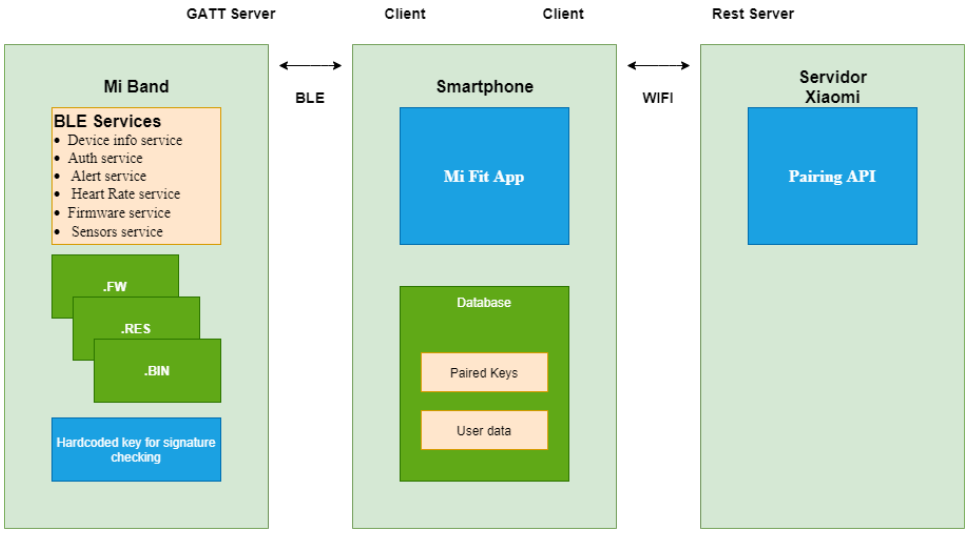

Figure 1: "MiBand" architecture. Source: [15]

2.2. Privacy in wearable devices

In the mobile computing area, wearables still fall short relating to their privacy and security issues [16].

Discreetly these equipment sense, process and collect sensitive user information in a continuous manner [17], [28].

Collected data by wearable devices can also be used to deduce more private information, especially when combined with other data from different devices, which results in huge risks to the security and privacy of the user [10].

The most controversial sensor is the "GPS" (Global Positioning System), since users feel watched and surveilled knowing that their location is currently being monitored, and can be for example shared on social media by a simple mistake [18].

"Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and Online Social Networks" gives a good idea about the problems that arise from the use of "wearables" paired with applications on "smartphones", stating that it introduces several new attack vectors during the communication all of the involved parties, referring to areas such as authentication and encryption mechanisms that are poorly implemented [10].

Some of the insecurity factors related to wearable devices are as following:

- Social unconsciousness: Activity trackers synchronize data that may be network-related of the user's friends and acquaintances, so it can collaterally impact the lives of other people.
- Right to forget: Because tracking is continuous, it can both include data that the user wants to be remember of later, as well as events that the user is not comfortable saving.
- Implications about location disclosure: Users analyzed in "Users' privacy concerns about wearables: Impact

of form factor, sensors and type of data collected" revealed that they felt fear that their location was being traced and may be disclosed to criminals or malicious third parties [18].

- Displaying confidential information: Wrist "Wearables" often show in their screen notifications to the user that may be confidential information, and anyone around can easily gain access to this data.
- Low access control: People uninformed about storage on systems "cloud" feel that organizations will use your personal data without your consent.
- Surveillance: Finally, users fear the constant vigilance that comes from the use of devices with sensors, as in the future there may be implications about the sensitive data by them captured.

Some attacks have been developed and documented as is the case of "Assessment of Fitness Tracker Security: A Case of Study", in which the following vulnerabilities have been analyzed [19]:

- Communication between wearable and mobile devices:
    - Public data bases
    - Unsecure "BLE" connections
    - Connections accept "unbounded" devices
- Communication between the mobile device and the server:
    - Authentication credentials sent in clear text
    - Poor use of "OAuth"
    - Non authorized data sharing
- "API" vulnerabilities:
    - Allow the use of "WebViews" (that don't offer the same level of protection as standard browsers, and can also be faked)
    - APIs with access tokens support, although they don't support refresh tokens
    - Some callbacks don't force the use of secure "HTTPS" connections, allowing man-in-the-middle attacks

2.3. Paranoid Methodology

The Paranoid Methodology it is not a new thematic, but it has become quite recently an area of study [29] with the appearance of the doctoral research The POSMASWEB – Paranoid Operating Systems Methodology for Anonymous and Secure Web Browsing [3], that implements a set of rules and operations to reinforce any operative system, may it be desktop, server or mobile [30]. This methodology was developed from 2013 to 2020, seeing its latest update when it became awarded research in the INNCYBER Research Awards for Best PhD Research in cybersecurity.

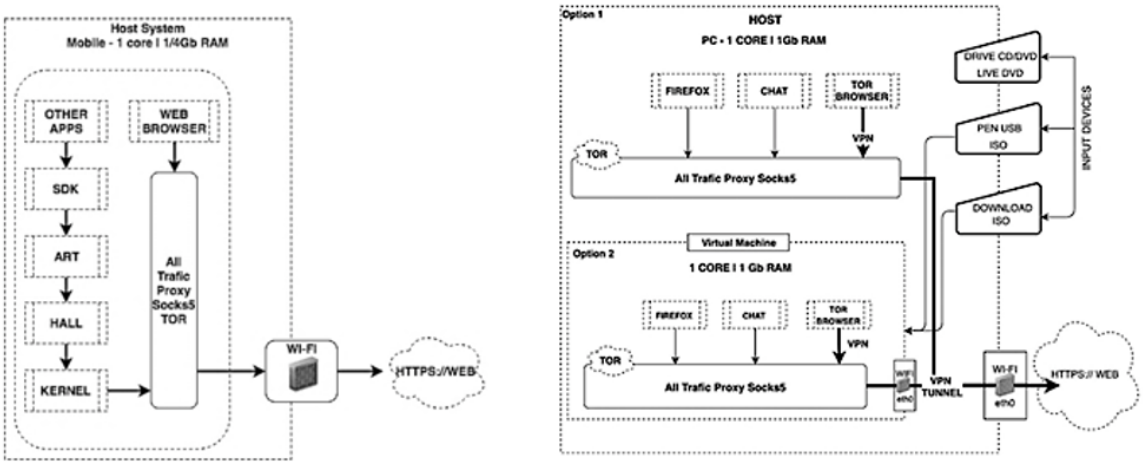

Figure 2: "POSMASWEB" architecture. Source: [3]

The methodology divides in layers the available applications, blocking common and unnecessary communications or data between them at kernel level, and forcing all TCP/IP through an internal proxy onto a secure internet communications relay or network, therefore, obfuscating from any ISP or traffic capture system the messages content [3], [30].

With a Proxy Socks5 and IPTABLES configuration, all traffic is redirect from the layered communications environment, through the internal firewall onto TOR, I2P or proprietary private internet relay system, maintaining secret the physical MAC Address of the network card, the IP, DNS details and other information that might lead to the discovery of the virtual or physical location of a given user [28]. Furthermore, this methodology uses a triple TOR circuit to promote an untraceable location of the user, bypassing modern constrains from IDS/IPS and Firewall systems every 60 seconds [30].

2.4. BLE Protocol architecture

Bluetooth low energy is one of the most popular and innovative technologies developed by "Bluetooth Special Interest Group" ("SIG"), with the intent of becoming the best choice among all other standard wireless technologies [20].

The good synergy between performance and energy consumption makes "BLE" a good choice for devices with smaller battery capacity and for applications that only require a smaller signal range [21].

"BLE" protocol architecture is defined by three primary blocks of components, each having their own layers and models.

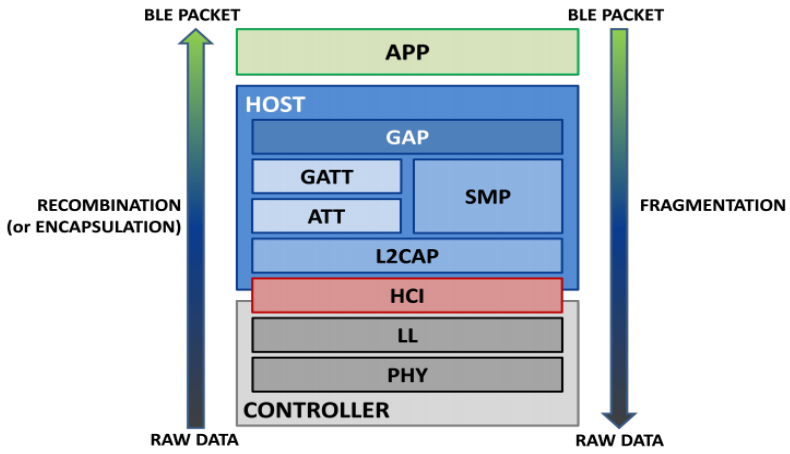

Figure 3: BLE protocol architecture. Source: Tosi et al. [20]

The application block is at the top of the architecture and represents the direct user interface. It also defines some profiles using "SIG" with the purpose of encouraging interoperability between devices and different manufacturers [20].

Next, the host layer utilizes some protocols and profiles that are basically functionalities provided by subjacent protocols. The "BLE" pillar is known as "Generic Access Profile" ("GAP"), and its purpose is to define how "BLE" devices communicate between them. It is also the responsible for the secure communications making use of rules and security algorithms implemented by the "Security Manager Protocol" ("SMP"), being responsible of the encryption/decryption of data packets [20]. After two devices establish a connection, they can only start communications after a secure pairing (usual key change practices, for example "Diffie-Hellman" elliptic curve) [19].

Still in this layer, the "Generic Attribute Profile" ("GATT") determines the way data is organized and sent within a "BLE" connection. It utilizes the protocol "Attribute Protocol" ("ATT") to divide data into attributes (to facilitate the transmission) as well as a transportation mechanism [19].

This layer also uses the "Logical Link Control and Adaptation Protocol" ("L2CAP") to send packets to the "Host Controller Interface" ("HCI"), or in case of "hostless" systems directly to the "Link Layer" ("LL") [19].

Lastly, the final layer is the "Controller", structured by the sublayers "Physical Layer", "Link Layer" and "Host Controller Interface". The first one oversees modulating analog signals and transform them into digital symbols ("BLE" devices can communicate by using "unicast" or "broadcast" connections).

"Link Layer" is constituted by a combination of hardware and software, being the layer that defines the type of communications that can be made between "BLE" devices, and it also generates and defines the different functions that each device is granted [20].

Finally, and still in this layer, the "Host Controller Interface" manages the communications between the

"Controller" and the host, being the base of the "BLE" protocol, and it manages the communications between hardware and the user application [20].

2.4.1. BLE: Connection

A connection is a permanent periodic packet exchange between two devices [22] that can be protected (or not) with security measures that make it private.

There are two roles in respect to the "BLE" connections:

- Master (central): searches for packets announcing connectivity and consequently initiates the connection. When there is an existing active connection, this is the device that manages all the settings and starts the periodic packet exchanges.
- Slave (peripheric): periodically sends packets announcing its intention of connecting, being the device that accepts connections started by the master. When the connection is established, it follows the settings defined by the master and exchanges packets with it.

Before the connection begins, the peripheric device is in advertising mode, sending packets with the intention of establishing a connection, while the master device is in discovery mode, meaning it awaits packets from the peripheric device to establish connection [20].

When the master device finds the peripheric packet to connect, it sends the latter one a connection request with intent to establish connection.

At this point, the devices can communicate between themselves using data packets.

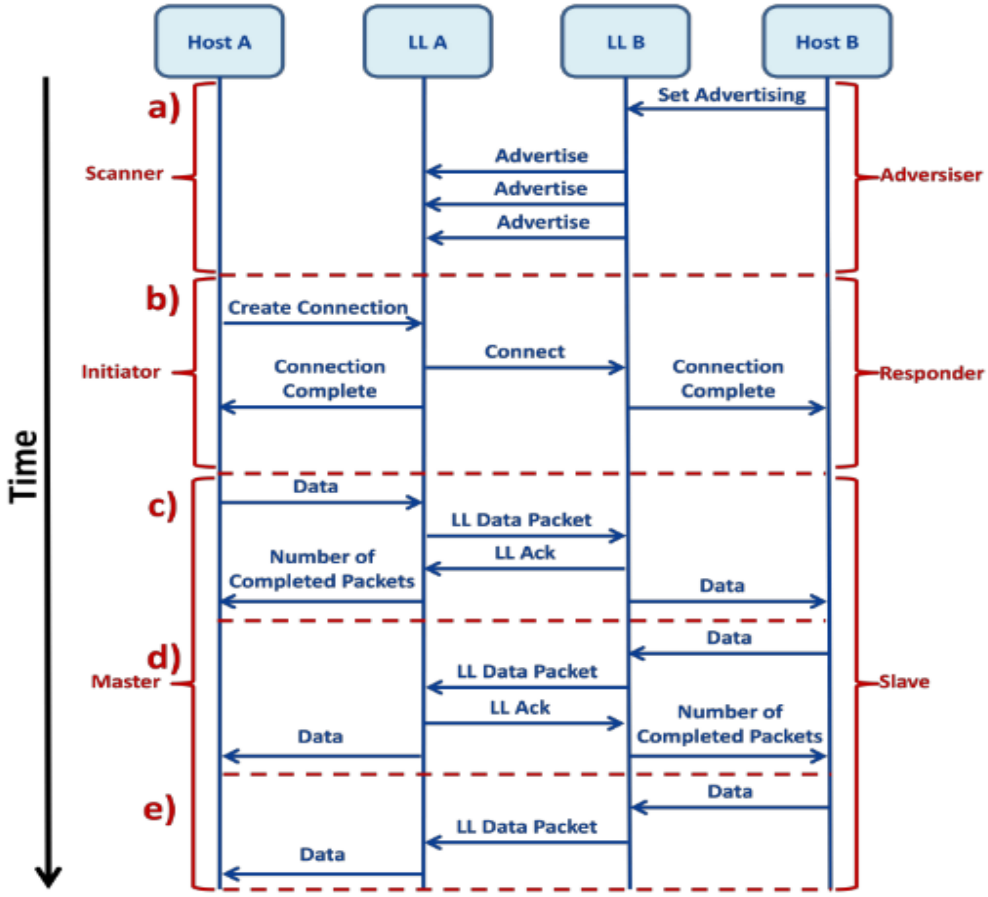

Figure 4: BLE connection between two devices. Source: [20]

The previous figure shows the connection process:

- a) Advertising mechanism
- b) Establishing connection
- c) Connection has been established and a packet is being transferred to the peripheric device
- d) Opposite of c)
- e) One way communication

2.4.2. BLE: Packet structure

The BLE packet structure is the same for all the communication types (broadcast and unicast) being divided into four sections [20]:

- Preamble ("PRE"): size depends on the data flow rate, one or two bytes. This is the sequence of bits that the receiver uses to define and control the frequency correspondent to the data flow rate
- Access Address ("AA"): group that includes the next four bytes that identify the physical connection of the communications, and it is also used to exclude packets with different destinations
- Protocol Data Unit ("PDU"): depends on the type of communications being used (for example, there are a lot

of different broadcasting packets);

- Cyclic Redundancy Check ("CRC"): verifies the presence of errors while analyzing "PDU".

Figure 5: BLE packet structure. Source: [20]

2.4.3. BLE: Related possible attacks

Specifically talking about Bluetooth related attacks, it's important to notice that the protocol is public information (as well as the way the protocol should be implemented), so it is important to follow the security procedures of the protocol, so attacks like "Denial-of-Service" ("DoS") or even attacks that grant full control of the devices are not simple to execute [23].

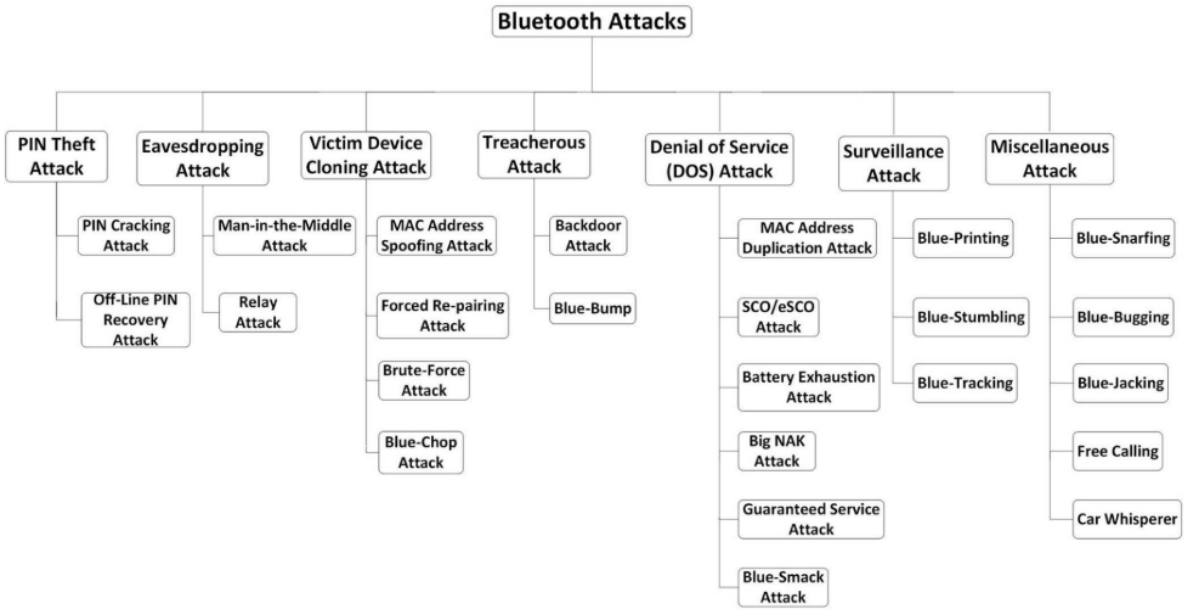

Figure 5: Bluetooth attacks categories. Source: [23]

3. Methods

The principle that will be followed as the research method is "Action-research", also known by other names including "Participatory research", "Collaborative research", "Emancipatory research", "Action learning" and also "Contextual action-research" [24].

There is no certainty as to who formalized this method, as it is a hard methodology to define, since it is a very natural process and it can appear in many different ways and can be developed differently for different use cases

[25]. It is a study method that allows the learning component to come naturally while the project keeps moving forward over time, in which the identification of the problem comes first, the researcher does whatever needs to be done to solve it, and at the end the success of the efforts gets qualified, and if they were not enough it is tried again [24].

According to "An Assessment of the Scientific Merits of Action Research", Gerald Susman divides this methodology into five different phases that are implemented in each research cycle [26]. Initially in the diagnosis phase, the problem is defined and, since in this phase it is important to have a global vision of the whole problem, to obtain a more detailed diagnosis, data is collected.

This is proceeded by the planning phase of the action, by a group of possible suppositions of the solutions, from which an action plan emerges and is implemented by choosing the most adequate alternative. Consequently, begins the execution phase in which starts the execution of the previous planned actions in the initial phases.

In the fourth phase (evaluation), the data is collected, analyzed, and interpreted relatively to the action success rate. Lastly, the problem is reevaluated, and a new cycle starts in the process.

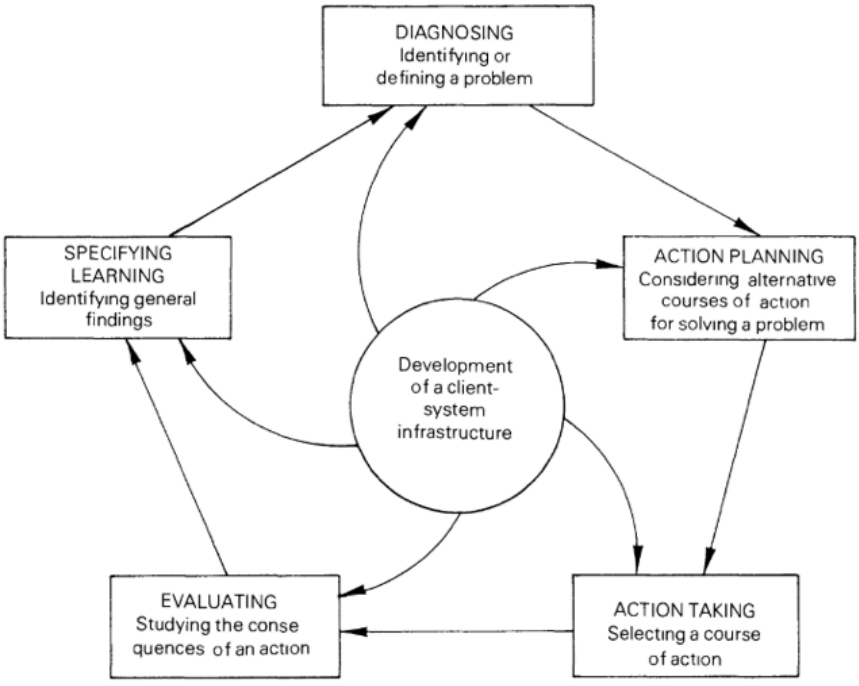

Figure 6: Action-Research model. Source: [26]

This methodology can be characterized by seven key principles [27]:

- Reflective criticism
- Dialectical criticism
- Collaborative resource
- Risk

- Plural structure
- Theory, practice, transformation

In this project the following topics are planned to be executed in each of the different phases of the chosen method ("Action-Research"):

- Diagnosis:
    - Verify how the applications work
    - Verify how they communicate
    - Verify how they store data
    - Verify how they share data
- Action planning:
    - Decision of the arguments to be included in the solution (possibly building a prototype)
    - Mitigation measures to be included in the solution
    - Included tools
    - Decide if the solution is deliverable of not, and if it can be in the prototype model
- Action execution:
    - Building the prototype
- Evaluation:
    - Prototype results
    - Prototype validation (privacy and security objectives)

4. Expected findings

The main purpose of this project, is to capture and register the behavior of the chosen wearable fitness tracking equipment "MiBand", developed by the Chinese company "Xiaomi".

The most important part of this project is to find out how the communications are being made throughout the whole process, starting from the setup of the wearable and its consequent communications with the mobile device that it is paired to, until the final communications between the mobile device and the external servers that maintain, and store user data captured by the wearable device itself.

To achieve the objectives defined in **1.2**, it is imperative that the "Bluetooth Low Energy" protocol is studied (for local communications), as well as all the protocols that are included in the network side of the communication, to limit and define the problem universe.

Starting by the "BLE" protocol, Android devices after 4.4 version have the functionality to capture and register Bluetooth traffic by simply navigating to the developer options and activating "Enable Bluetooth HCI snoop log".

The log file generated is stored in a zone of the device memory that require administrator permissions, or as it is generally called "root" access.

It is also possible to find and catalog BLE services and characteristics of specific BLE devices, by using a BLE scanner application for Android.

With the log file generated it is possible to analyze BLE traffic (using for example Wireshark) in conjunction with the BLE scanner app report.

WI-FI traffic in Android devices applications is usually encrypted as the apps make use of signed trusted certificates. Most of the big applications use a technic called "Certificate Pinning" meaning that the communication can only be established if the connection host certificate is expected by the application itself. Basically, apps hard code their certificates within their code (with security measures so they cannot be swapped manually, for example checksums), but in this case "MiFit" app doesn't make use of this security measure, which means that with a couple changes to the ".apk" file itself (Android application package), the traffic can be sniffed in plain text using a "man-in-the-middle" attack.

It is possible to decompile the application ".apk" file, manually change the manifest file to allow custom user installed certificates, recompile and self-sign the app again without any repercussions to the functionality of the application.

With these changes on the ".apk" file it is possible to decrypt the whole communication between the mobile device and the external servers, since the certificate used in the communication is in our possession making it easier to follow the trail of the user data being exchanged.

5. Acknowledgements

This work was partially supported by the Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF), within project "Cybers SeC IP" (NORTE-01-0145-FEDER-000044).

6. References

[1] P. B. Sharma, "REACHING OUT : A HISTORICAL OVERVIEW OF THE EVOLUTION OF NON VERBAL COMMUNICATION Dr . PREETI BALA SHARMA REACHING OUT : A HISTORICAL OVERVIEW OF THE EVOLUTION OF NON VERBAL Article Info :," no. August 2013, 2016.

[2] D. Schmandt-Besserat, "1 . Tokens as Precursor of Writing," *Briscoe Cent. Am. Hist.*, no. Marcus 1992, pp. 1–15, 2014.

[3] N. Coelho, "Universidade de Trás-os-Montes e Alto Douro Paranoid Operating System Methodology for Anonymous & Secure Web Browsing," 2020.

[4] M. E. Cecchinato, A. L. Cox, and J. Bird, "Smartwatches: The good, the bad and the Ugly?," *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 18, pp. 2133–2138, 2015, doi: 10.1145/2702613.2732837.

[5] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," *Sensors (Switzerland)*, vol. 12, no. 9, pp. 11734–11753, 2012, doi: 10.3390/s120911734.

[6] J. Pereira, "Technologies for Participatory Medicine and Health Promotion in the Elderly Population (GERIATIC).," *Technologies for Participatory Medicine and Health Promotion in the Elderly Population (GERIATIC). Available online: https://clinicaltrials.gov/ct2/show/study/NCT03504813?cntry=ES (accessed on 1 February 2021).*, 2018.

[7] R. Martín-Prieto, "Automation of the Data Acquisition System for Self-Quantification Devices," *Proceedings*, vol. 2, no. 18, p. 1184, 2018, doi: 10.3390/proceedings2181184.

[8] S. Gabriele, "User Awareness of Privacy Risks Related to the Collection of Fitness Tracker Data," 2020.

[9] M. Swan, "Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0," *J. Sens. Actuator Networks*, vol. 1, no. 3, pp. 217–253, 2012, doi: 10.3390/jsan1030217.

[10] A. Aktypi, J. R. C. Nurse, and M. Goldsmith, "Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and Online Social Networks," *MPS 2017 - Proc. 2017 Work. Multimed. Priv. Secur. co-located with CCS 2017*, vol. 2017-Janua, no. Ccs, pp. 1–11, 2017, doi: 10.1145/3137616.3137617.

[11] C. Buenaflor, H. Kim, and S. Korea, "Six Human Factors to Acceptability of Wearable Computers," 2013.

[12] A. Hilts, C. Parsons, and J. Knockel, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," 2016.

[13] H. Patterson, "Contextual Expectations of Privacy in Self-Generated Health Information Flows," *SSRN Electron. J.*, pp. 1–48, 2013, doi: 10.2139/ssrn.2242144.

[14] R. Rawassizadeh, B. A. Price, and M. Petre, "Wearables: Has The age of smartwatches finally arrived?," *Commun. ACM*, vol. 58, no. 1, pp. 45–47, 2015, doi: 10.1145/2629633.

[15] P. Mishra, A. Gupta, and S. Carvajal, "SECURITY ANALYSIS OF MI BAND 4."

[16] T. Starner, "The challenges of wearable computing: Part 1," *IEEE Micro*, vol. 21, no. 4, pp. 44–52, 2001, doi: 10.1109/40.946681.

[17] T. Starner, "The challenges of wearable computing: Part 2," *IEEE Micro*, vol. 21, no. 4, pp. 54–67, 2001, doi: 10.1109/40.946683.

[18] V. G. Motti and K. Caine, "Users' privacy concerns about wearables: Impact of form factor, sensors and type of data collected," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8976, no. January, pp. 231–244, 2015, doi: 10.1007/978-3-662-48051-9_17.

[19] F. Mendoza, L. Alonso, A. López, and D. and Patricia Arias Cabarcos, "Assessment of Fitness Tracker Security: A Case of Study," *Proceedings*, vol. 2, no. 19, p. 1235, 2018, doi: 10.3390/proceedings2191235.

[20] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance evaluation of bluetooth low energy: A systematic review," *Sensors (Switzerland)*, vol. 17, no. 12, pp. 1–34, 2017, doi: 10.3390/s17122898.

[21] A. K. Sultania, C. Delgado, and J. Famaey, "Enabling low-latency bluetooth low energy on energy harvesting batteryless devices using wake-up radios," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–19, 2020, doi: 10.3390/s20185196.

[22] K. Townsend, C. Cufí, A. Davidson, and R. Davidson, "Getting Started with Bluetooth Low Energy: Tools and Techniques for Low-Power Networking," *J. Mater. Process. Technol.*, p. 244, 2014.

[23] R. Witsenburg and K. Van Brakel, "Investigation of security on Chinese smartwatches," pp. 1–16, 2019.

[24] R. O'Brien, "An overview of the methodological approach of action Research. Faculty of Information Studies," *Univ. Toronto*, pp. 1–15, 1998.

[25] D. Tripp, "Action research: a methodological introduction," *Educ. Pesqui.*, vol. 31, no. 3, pp. 443–466, 2005, doi: dx.doi.org/10.1590/S1517-97022005000300009.

[26] G. Susman and R. Evered, "An Assessment of the Scientific Merits of Action Research," 1978, doi: 10.2118/169428-ms.

[27] R. Winter and S. Burroughs, *Learning from Experience: Principles and Practice in Action-research*. Falmer Press, 1989.

[28] N. M. Coelho, M. Peixoto and M. M. Cruz-Cunha, "Prototype of a paranoid mobile operating system distribution," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757551.

[29] N. Coelho, B. Fonseca, and A. Castro, "Paranoid operative system methodology for Anonymous & Secure Web Browsing, doctoral project," Atas da 17ª Conferência da Associação Portuguesa de Sistemas de Informação, 2017, doi: 10.18803/capsi.v17.127-143.

[30] N. R. Mateus-Coelho, B. R. Fonseca, and A. V. Castro, "POSMASWEB: Paranoid Operating System Methodology for Anonymous and Secure Web Browsing," Handbook of Research on Cyber Crime and Information Privacy, pp. 466–497, 2021, doi: 10.4018/978-1-7998-5728-0.ch023.

[31] N. Mateus-Coelho, M. M. Cruz-Cunha, and P. Silva-Ávila, "Application of the Industry 4.0 technologies to mobile learning and health education apps," FME Transactions, vol. 49, no. 4, pp. 876-885, 2021, doi: 10.5937/fme2104876M.

[32] S. Chagas, N. Lopes and I. Portela, "Performance Evaluation of Host Scalability in Software Defined Networks," 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), 2021, pp. 1-6, doi: 10.23919/CISTI52073.2021.9476545.