Rede Nacional de Pesquisa (RNP) and National Science Foundation (NSF)

US-Brazil Joint Program in Cybersecurity

The State-of-the-Art of Attack Vectors in Wearable Medical Devices and Existing Countermeasures

HealthSense Project
– Deliverable D1.2 –

Collaborators of this deliverable:
Aldri Santos[1], Eduardo Cerqueira[2], Denis Rosário[2], Michele Nogueira[1], Bruno Cremonezi[1], Andressa Vergutz[1]

[1]Universidade Federal do Paraná – Curitiba – PR – Brazil

[2]Universidade Federal do Pará – Belém – PA – Brazil

Contents

1 Introduction **3**

2 Wearable devices **4**

2.1 Architecture 4

2.2 Sensors for human activity monitoring 4

2.2.1 Mechanical sensors 5

2.2.2 Electrical sensors 7

2.2.3 Optical sensors 8

2.2.4 Electrochemical sensors 8

2.3 Wireless communications for wearable devices 9

3 Attacks vectors and countermeasures on wearable devices **9**

3.1 Security and Privacy Requirements 10

3.2 Adversary Classes 11

3.3 Passive Attacks 11

3.3.1 Eavesdropping 11

3.3.2 Traffic Analysis 12

3.4 Active Attacks 12

3.4.1 Denial of Service 12

3.4.2 Man-in-the-middle 15

3.4.3 Impersonation 15

4 Final considerations **16**

1. Introduction

With the rapid development of nanotechnology and wireless communication, small, low power, implantable and wearable devices have gained increasing popularity. These devices are commonly used for diagnosing and monitoring various medical conditions, providing timely data [1, 2, 3]. In general, they collect vital or non-vital physiological data such as heart rate, body temperature, blood pressure and respiratory rate [4]. Then, these devices transfer the gathered data to a final destination, such as a hospital repository [5, 6]. The use of wired communication in the data transmission, despite effective, limits the application of medical devices because it can cause discomfort to users and constraint user's mobility [6]. Differently, wireless communication allows wearable devices to monitor patients while they continue their daily activities, without the need of being physically in a hospital [7, 6]. Hence, today a large number of wireless wearable devices monitors users anytime and anywhere, such as smart watches, fitness tracker and smart glasses, improving users' quality-of-care without disturbing their comfort [8].

Due to the large number of applications and the great potential to offer a better life to users, wearable devices are a trend. Market estimates the use of over 3 billion wearable wireless sensors by 2025, being over 30 percent of them new types of sensors that are emerging [9]. Among big companies such as Nike, Jawbone, Fitbit and Garmin, it is common to find a fitness tracker well received by the market. The two big technology players on the market, Microsoft and Apple, also have their own wearable devices; they have introduced the Apple Watch and the Microsoft Band, respectively. These devices, besides also being a fitness tracker, provide phone calls and text messaging alerts, UV monitoring and digital assistants [10, 11]. The success of these devices are very well-known. Apple did not disclose specific sales numbers for its Apple watch in 2017, but the company said its sales have risen 50 percent compared to the previous year [12]. Following the trend, the pharmaceutical industry is also embracing the wearable technology. Some companies have been experimenting with ingestible pills that can capture all sorts of biometric data. Helius, for example, is a consumable pill developed by Proteus Digital Health used in healthcare scenarios. Once ingested, the pill is able to indicate if prescribed medicines are taken and how the organism is responding to them [13].

Wearable devices are vulnerable to a broad range of cyberthreats [14]. Once these devices collect and exchange users health data, that are sensible, securing them is very important. When an adversary with malicious intention detects a vulnerability, it opens an opportunity to perform an attack through a varied set of attack vectors. A recent study shows that 94 percent of healthcare institutions reported having been victims of cyberattacks [15]. Therefore, the lack of security may not only lead to loss users' privacy, but it may also allow adversaries to introduce bogus data or modify/suppressing legitimate data, inducing erroneous diagnosis [16]. Further, wearable devices operate in environments with open access by various people, such as hospital or medical organization, which are also prone to attackers [17]. The nature of wireless channel makes the data vulnerable to eavesdropping, modifications, and injection [18].

The main goal of this deliverable is to identify security vulnerabilities in wearable devices, the types of attack vectors, and the existing countermeasures for healthcare applications. Section 2 introduces the characteristics of wearable devices, since the architecture until the type of sensors, and the main wireless communication technologies

employed by these devices. Section 3 presents the concept of attack vector and shows generic examples for attacks on wearable devices and its countermeasures. Finally, Section 4 concludes this derivable presenting the final remarks.

2. Wearable devices

A wearable device is defined as an autonomous device, noninvasive, and that performs a specific function in general related to the body, such as monitoring a patient's health. This section provides an overview of wearable devices, presenting the state-of-art architecture, surveying the classes of sensors employed by them and presenting the most popular communication technologies for wearable devices.

2.1. Architecture

Figure 1 illustrates the generic architecture of a wearable device. In general, a wearable device comprises of sensors, low power computation (processor), communication (transceiver), low capacity storage, and display. The sensor collects physiological signals from the body and then, convert the collected signals in raw data. Depending on the monitoring task, different types of sensors may be used. We detail the different classes of sensors and the basic body-to-signal transduction method for each type of sensor in the next subsections. The collected data may be preprocessed and displayed in the own device, or the sensor can transmit the collected preprocessed data (alternatively, data can be compressed) to another device (e.g., a smartphone) through a close-range transceiver, assuming the sensor is equipped with a wireless communication transceiver that follows one of the body-area network technologies, such as bluetooth or Near Field Communication (NFC). In this deliverable, we focus on the later case, where the prevailing wireless technologies used in these transceivers are referenced in Subsection 2.3. The device that receives data through the close-range communication may be the final destination or the gateway to forward the data to final destination. When reaching the final destination, data is processed and displayed either in a graphical format or as a numerical value [19].

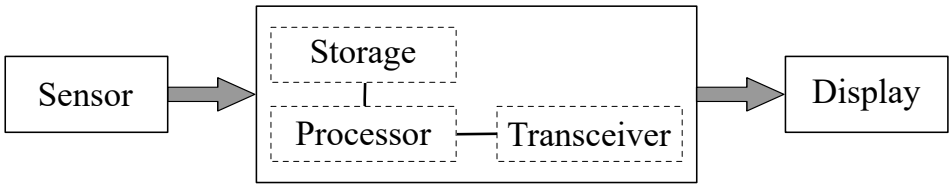

Figure 1. The Generic Architecture of a Wearable Wireless Device.

2.2. Sensors for human activity monitoring

In this subsection, we describe the main types of sensors for monitoring human activities. Being fundamental elements of the whole monitoring system, the sensors should accurately measure the physiological parameters over a long duration. Thanks to the rapid development of microelectronic, micromechanics, integrated optics and other related technologies, we are enabled to find various types of smart sensors to sense and measure data efficiently and faster, with low energy consumption and low processing resources [20]. In the next subsections, we highlight the main types of sensors and briefly describe the main characteristics related to each type.

2.2.1. Mechanical sensors

Mechanical sensors are involved in sensing of mechanical movements in an indirectly way. Based on physical principles such as conductive materials resistivity and capacitive change, they are used for medical applications like the monitoring of heart rate, lung volume, body movements and so many others. Due to the large amount of mechanical sensors, in this section we will review their main subcategories. The first reviewed subcategory is the **Piezoresistive sensors**. The piezoresistive effect is the basis for sensors on this category. This effect consists in an electromagnetic response when a conductive material (ex. nickel, chrominum) suffers a mechanical deformation. The poisson ratio measures the piezoresistive effect taking as basis the phenomenon in which a material tends to expand in a perpendicular direction to the direction of compression. When the material elongates, it contracts in the transverse direction of elongation, modifying the cross-sectional area of the conductive material (conductor). The resistance R of a conductive material is expressed as:

$$R = \rho L/A,$$

where ρ is the resistivity, L is the length of the conductive material, and A is the cross-sectional area of the conductive material. However, a deformation may change the resistance of the conductive material, due to changes in L and A [21].

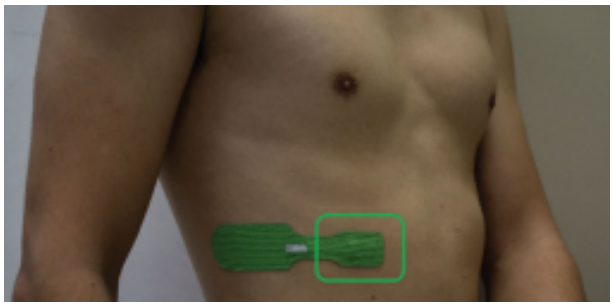

Figure 2. Piezoresistive sensors [21].

Due to simple design and high sensitivity, the sensors of this subcategory are widely used in wearable electronics to detect human physiological movement. Figure 2 shows an example of a typical piezoresistive sensor, which consists of a thin film conductor on a silicone elastomer. When stretched, the conductor changes the geometrical form, changing then the electrical resistivity. Once in the human body, these sensors are able to detect and quantify movements. Figure 3 shows an example of results from an piezoresistive sensor employed to estimate the chest movement from a respiratory process [20]. In the plots, the Y axis represents the variation of the resistance (left graph) and the approximate lung volume (right graph), while the X axis shows the time passage in both graphs. We see that both curves show almost the same behavior. Consequently, the piezoresistive sensors use this resistance change behavior to measure and predict the lung volume with relative precision.

The second subcategory of mechanical sensor covered in this deliverable is the **capacitive sensor**. Widely used in electronic touch screens, these sensors are based in parallel-plate capacitors that collect data based on the pressure [20]. While piezoresistive

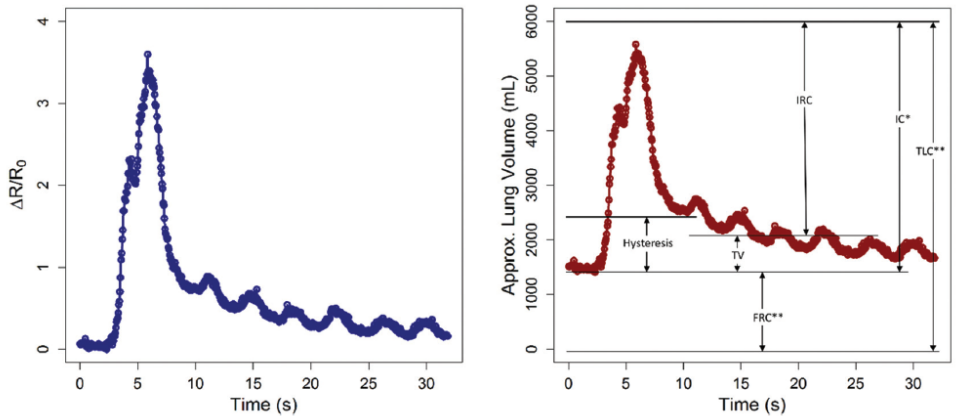

Figure 3. Variation of resistance in piezoresistive sensors and the variation of lung volume over time [21].

sensors are based on changes of the resistance of conductive materials, the capacitive sensors measure changes in the capacitance of a capacitor. The capacitance of a capacitor follows the equation:

$$C = \varepsilon A/d,$$

where ε is the permittivity of the cavity between two plates, A represents the overlap area of the plates, and d the distance between the two plates. Figure 4 shows an example where the distance between plates are altered by an external pressure (d and d'). The applied pressure leads to a change in the capacitance, enabling to measure the pressure applied over the capacitor. As mentioned, the parallel plate capacitive sensors dominate the commercial market. Consumer electronics and industrial applications already employ these sensors. Recent trends propose using them to mimic tactile sensation, detect joint bending and map the body pressure.

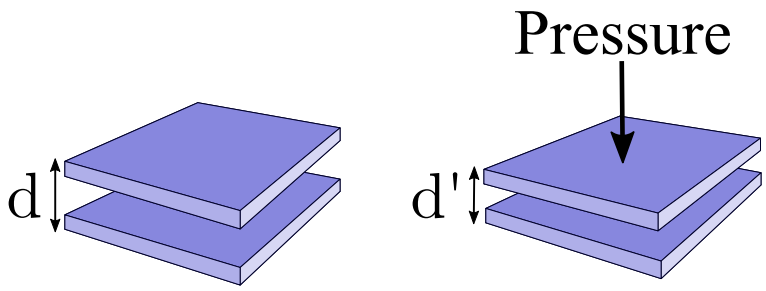

Figure 4. Schematic diagram of capacitive sensors.

The last subcategory of mechanical sensors presented in this deliverable is the **Piezoelectric sensor**. The Piezoelectric effect occurs in piezoelectric materials, such as tourmaline, quartz, topaz, and it is the basis for the sensing mechanism for these sensors. Figure 5 shows an certain material that, when subjected to mechanical stresses, produces a change in their electric polarization. This change in the polarization (V and V') is the piezoelectric effect and manifests as a measurable voltage across the material. Based on the change in electrical polarization inside the material, one can measure the pressure

applied over it. Applications of this technology include skin-mounted sensors for tactile sensation, finger bending motion detection and biomechanics characterization [20].

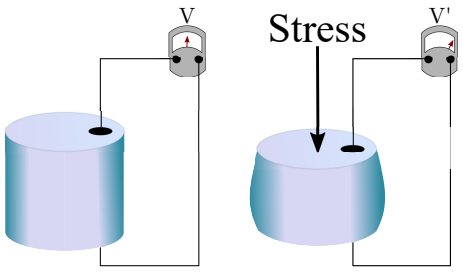

Figure 5. Schematic diagram of piezoelectric sensors.

2.2.2. Electrical sensors

Biopotential is a voltage produced by a tissue of the body, particularly muscle tissue during a contraction. For example, in each heartbeat, a special group of cells, that have the ability to generate electrical activity on their own, separates charged particles and then leaks this charged particles into the cells. This produces electrical impulses in the pacemaker cells, which spread over the heart, causing contractions on it. Due to the conductivity of the human body, these impulses manifest on the body's surface. This characteristic allows the creation of the electrocardiogram (ECG or ECK), allowing the measure of the electrical activity of the heart over a period using electrodes placed on the skin. A broad range of physiological relevant biopotentials also uses this concept, such as electromyogram (EMG) and electroencephalogram (EEG), both used in the diagnosis of neuromuscular and brain disorders, respectively.

Electrical sensors measure changes in electrical resistance of the skin or measure changes in capacitive or conductively coupled charge at the skin surface. The major challenge for this kind of sensors is to establish a good electrical contact with the skin when the skin is dry, oily or electrically resistive. The quality of the data gathered by the sensor depends on the electrical impedance (opposition that a circuit presents to a current when a voltage is applied) of the electrode-skin-body interface.

There are two major types of electrical contacts: wet electrodes and dry electrodes. The wet electrodes consist in a solid conductive electrode interfaced to the skin via an electrically conductive adhesive or a hydrogel. The prolonged use of these gels hydrate the skin, reducing the electrical impedance, resulting in a good electrical contact with the skin. Not all application allows the use of wet electrodes. Many of them require a repeated placement and removal of the wearable device. Dry electrodes eliminate the need of an electrolyte material and rely on a direct contact with the skin. Usually, they are made of gold and/or other biocompatible materials, such as cobalt and titanium to avoid any chemical reactions with the biofluids, such as sweet and saliva, and/or immune reactions by the skin. Besides that, they are usually ultrathin, low-modulus and stretchable [20].

2.2.3. Optical sensors

When a light source introduces light into the body through the skin, the transmission, absorption and scattering properties associated with the human skin can reveal information about the health of underlying organs through the light back reflected. Figure 6 illustrates optical sensors under a light source, where the wavelength can range from UV into deep infrared, depending on the needed penetration depth, and an optical detector which captures the light [20].

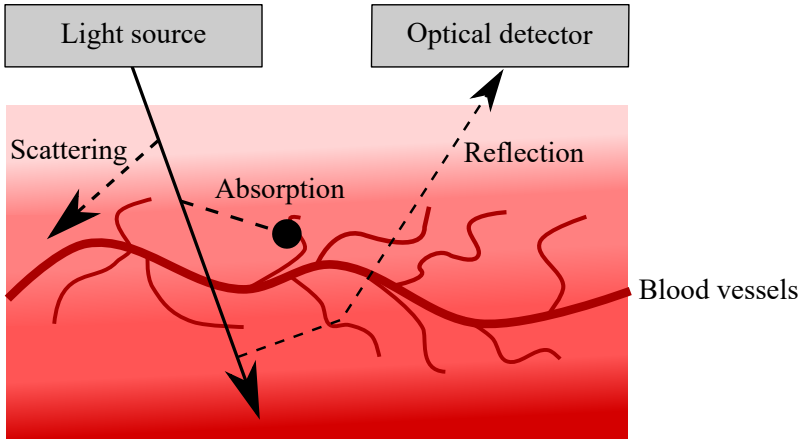

Figure 6. Schematic diagram of optical sensors.

The Apple watch, as example, uses an optical sensor to measure heartrate. It essentially tests how much red or green light it can see when looking at the skin on the wrist. Blood is red because it reflects red light and absorbs green light, so when your heart beats, there is more blood flow in the wrist, and more green light absorption. Between heartbeats, there is less absorption of green light. Due this changes in the optical properties of the skin, the watch can extract the heartrate and oxygenation of the user [12].

2.2.4. Electrochemical sensors

Chemical sensors are one of the most common sensors today and are extensively used in standard blood and urine tests. The vast majority of these sensors require a direct contact with the chemical solution to detect a particular chemical component. Once the skin is a nearly perfect barrier for the most chemicals, it is a great challenge to extract biomarkers from the body in a reliable and non-invasive manner. To accomplish this, a non-invasive wearable chemical sensor must take advantage of the biofluids secreted from the body, such as saliva, sweat and tears. In this way, the chemical sensors have access to chemical substances without any invasive procedure [20]. Electrochemical sensors are composed of two electrodes and a contacting sample solution, which constitute the electrochemical cell. There are two major classes of electrochemical sensors the potentiometric and the amperometric ones.

Potentiometric sensors rely on measuring a potential response associated with an chemical substance, where the signal measured is the potential difference between the two electrodes. The potentiometric sensor electrodes are coated with a membrane that

allows the passage of only one ionic species that will dominate the voltage between them. **Amperometric sensors** involve electron transfer processes across the electrode/solution interface and rely on measuring the current signal when a potential is applied between the two electrodes. The applied potential is used for driving an oxidation/reduction reaction of the target chemical substance while resulting current signal proportional to the chemical component concentration.

2.3. Wireless communications for wearable devices

Among their different applications, wearable devices may be the solution for ambulatory monitoring during normal daily activities for prolonged periods of time. This makes it possible to gather a high quantity and a variety of user's data. In order to overcome the inconvenience of a constant monitoring, the main features that a wearable device must present are: comfort; non-intrusiveness and non-obtrusiveness; do not require skillful preparation to wear; and do not require accurate positioning.

These devices may transmit the collected data through a close-range transceiver to another device, which will process and display the collected data. Assuming that conventional transmission in wearable sensors are traditionally handled by wires, user's mobility and comfortableness are severely hindered and there is a great risk of system failure [22]. A more favorable approach to transmit the data collected by sensors comes through the use of wireless communication technologies.

The most traditional wireless communication technologies for wearable devices are NFC [23], ZigBee [24] and Bluetooth [25]. All these communication technologies are used because they can offer a low-cost, low data-rate communication with long battery life, and present very low complexity. However it is possible to find devices that operate under cellular, 3G, and other radio frequencies communication technologies [5, 26]. In fact, more technologies wearable devices support, easier for them to be integrated with other applications [26].

In short, RF technology dominated the wireless communication in the wearable devices. The problem is that many factors can influence the transmission/reception of a radio signal. The most common issues are radio interferences, electromagnetic interferences and antenna issues. Interferences can come from a vast number of sources, since microwave ovens, and wireless equipment until police radar, electrical motors [27]. Besides that, if an malicious user supplied by a radio frequency device can work on promiscuous mode to intercept and read any packet that arrives from the radio frequency, this can lead to several attacks, which we discuss in Section 3 [28].

3. Attacks vectors and countermeasures on wearable devices

Establishing confidentiality and privacy between communicating peers is still an issue in different contexts where solutions based on asymmetric keys are not viable, such as wearable devices and wireless body area networks made up of heterogeneous and resource constrained devices. The approaches or paths followed to assault a computer system or network is called attack vector [29]. One adversary can achieve one attack by exploiting stereotypical thinking, processing ability, inexperience, truth bias and other attack vectors [29]. With great popularity of wearable devices using short-range low-power

communication technologies, the number of information available for a privacy attack increases. Once that these devices can gather and store various kind of data, they often are considered the prime targets for attackers.

Malicious attackers may eavesdrop on traffic between the nodes and the remote medical personnel and then inject messages, replay old messages, spoof, and ultimately compromise integrity of device operation. If successful, such behaviors can not only invade user's privacy but also suppress legitimate data or insert bogus data into the network leading to unwanted actions (e.g., drug delivery) or preventing legitimate actions (e.g., notifying doctor in case of and emergency). Some demonstrations, already have shown that if an adversary with malicious intent can bypass the security mechanism of these devices, causing damages ranging from invasion of privacy to the threating life of the user [28]. In an attack demonstrated by Jerome Radcliffe, utilizing the ID of the device, he was able to took control of an insulin pump and was capable to command the pump to inject insulin at every three minutes, leading to a hypoglycemia or even stop insulin delivery [30]. Since that wearable devices are prone to a variety of attack vectors, in what follows, we focus on the communication related to attack vectors.

3.1. Security and Privacy Requirements

The security and privacy of user-related data are two indispensable components for the security of wearable devices. Data security is the guarantee that the data is securely stored and transferred; and the data privacy is the guarantee that the data can be only accessed and used by an authorized user [31]. In the following, we show the security and privacy requirements.

Confidentiality: Data, device information, and device system configurations should be accessible only to authorized devices. User's data must always be kept confidential at the wearable device or at the display device. Besides that, the devices should be resilient to any compromise attacks; that is, compromising one device should not help the adversary to gain access from the data stored at that device or elsewhere. In fact, ideally the adversaries should not be able to determine that an user has a wearable device. However, it is not always possible to hide the existence of the device. In these cases, the adversaries should not be able to determine the device's ID or even what type of device and sensors that user is wearing. The ID information may allow an unauthorized access and could result in deeper invasions and the device type and sensors may allow an indirect type of eavesdropping, which could harm the patient's life.

Integrity: Data, device information, and device system configurations should not be modifiable by unauthorized devices. In wearable devices the user-related data may be vital, and modified data would lead to disastrous consequences. In short, the device must be able to detect modification of data at end users and check then during storage periods, in order to discover potential malicious modification [32].

Availability: Data, device information, and device system configurations should be accessible when requested by authorized devices [32]. In wearable devices, the user-related data may be vital, and making an authorized user unable to access the data would lead to disastrous consequences [7].

3.2. Adversary Classes

To discuss about the attack vectors that may occur in wearable devices, we must be define a model which establish all resources available for the adversary. The following attacks described in this section consider attacks by one or by the two following adversarial models:

- **Passive adversaries.** Such adversaries have the capability to eavesdrop communications on the wireless channel between transceiver and the display. We assume that the adversary possesses all the equipment to capture record and analyze the acquired signal from the transmissions, independent of the communication technology applied on the wearable device.
- **Active adversaries.** These adversaries are capable to do everything that a passive adversary can do and they can generate signals to send commands to the processor/transceiver and the display, modify messages in transit or even just block them, not letting them reach the destination.

3.3. Passive Attacks

A passive attack is characterized by the attacker listening communications, without any attempt to break into the device or change data. Thus, either a passive or an active adversary may do these attacks. Even though a passive attack sounds less harmful, the damage in the end can be just as severe if the right type of information is obtained.

3.3.1. Eavesdropping

Due to the broadcast nature of wireless medium, wireless communication is extremely vulnerable to eavesdropping attack [33]. Being the most common attack to privacy, the eavesdropping consists in an adversary snooping any unencrypted data transmitted through the medium. Doing that, the adversary could easily discover the communication contents, putting in risk the user's privacy. An example of this attack was presented in [34]. Using a software radio platform, the authors are able to eavesdrop on wireless communications of a popular insulin pump on the market and, since that the device does not employ any privacy mechanism, they are able to eavesdrop the data in a clear text form. After reverse-engineering the device's communication protocol and packet format, they are able to create a legitimate data packet, which is accepted by the insulin pump, containing misleading information, e.g., an incorrect reading of the glucose level, control command for stopping/resuming of insulin injection, and control command for immediately injecting a dose of insulin into the human body. Therefore, an adversary can force a wrong insulin therapy which may cause hyperglycemia (high blood glucose) or hypoglycemia (low blood glucose) and endanger the patient's life [35].

Countermeasures: The most commonly used security approaches to confront the eavesdropping attack rely on cryptographic encryption techniques. The technique's objective is to offer an end-to-end protection to the communication, even if transmitted through a wireless medium. By using an encryption method, the data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Although encryption is effective, it has an expressive computational cost and secret key distribution and management problem. The

traditional public key cryptography requires a great quantity of computational processing and communication capabilities. Thus, it is not well suited for the resource-constrained environment of wearable devices. In that case, the use symmetric ciphers are better option for such requirements [28]. However, the symmetric key distribution scheme suffer with the problem of trust between two devices that share a secret symmetric key.

3.3.2. Traffic Analysis

Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Identifiable traffic features, such as packet size, frequency of a packet and the packet inter arrival time, can potentially reveal enough information to enable an adversary to identify user's activities [36]. The traffic analysis when aggregated or combined with other sources of information, for example, the knowledge of the communication behavior from a sensor when a critical event is happening (e.g. A heart failure, high body temperature and others) may reveal information about user's health [37].

Countermeasures: A commonly used technique to defend against traffic analysis is packet padding, setting all packets to the same length. This strategy usually incurs significant communication overhead; hence, it is not an ideal solution [36]. Traffic morphing, is another strategy to avoid the traffic analysis. The concept of this countermeasure is to morph the network traffic from one class to another. For example, morph the traffic generate by a wearable device to looks like a VoIP or a web-browsing application. Despite effective, is expected a increment in the communication overhead due to increased payloads [38].

3.4. Active Attacks

In contrast with passive attacks, active attacks involves an adversary attempts to gain any information by the introduction of data into the network as well or even changing data within the network. To achieve that, the adversary can utilize any resource available and can actively participate in the communication. For example, the adversary may deprives another device's access to a network, it can also pretends to be a particular device of a system to gain access to another device or even alters packet header addresses to direct a message to a different destination. Due these characteristics, the active attack can only be done by and active adversary. However, it must be emphasized that passive attacks are often preparatory activities for active attacks [39].

3.4.1. Denial of Service

An effective way to cause wearable device access interruption is by physical destruction. Although effective, the attacker may not be able to have a physical access to the device, making it a useless attack vector. A most elegant way to deny a service consists in an active adversary disrupting the network in a way that stops legitimate users from accessing the device [40]. For example, Figure 7 shows an adversary disrupting the connection between the wearable device and the display device. On the other words, the adversary is executing a Denial of Service Attacks (DoS). The DoS main purpose is to interrupt specific resources or services on the network and with this, compromise the access by

legitimate users. One of the ways to make services inoperative, for example, is to overload the target (e.g. links or servers) with a significant volume of requests. In general, the volume of requests directed to a particular victim is much larger than your processing capacity, overloading it easily. The DoS attacks presented in this deliverable are classified according to the protocol network layer used to carry out the attack, following the Open System Interconnect (OSI) model.

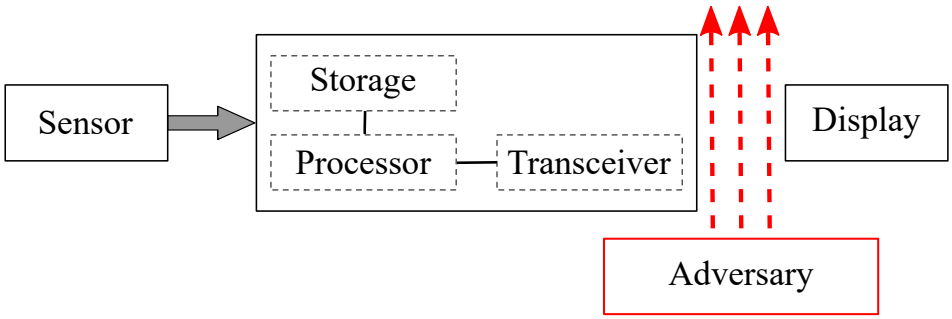

Figure 7. The Generic Architecture of a Wearable Wireless Device under an Denial of Service Attack.

At the physical layer, the proliferation of wireless communication technology makes the medium attractive target for saboteurs [41]. The exposed nature of wireless links, makes that any device connected at them can be easily attacked by jamming technology [42]. To achieve a jamming attack, the attacker will need a jamming device that continuously emits electromagnetic energy on the medium. This constant noise results in a great decrease of the SNR, resulting in a large number of packet collisions. Besides the increase the overall network latency, a study shown that the packet collision have a great impact on the battery usage [43].

Countermeasures: A logical countermeasure to jamming attack vector is to put the devices to sleep when identified that a jamming is occurring. To identify if the attack ends, the devices will wake periodically and test if the channel still jammed. This will not prevent the Denial of Service attack; however, it could significantly increase the life of device by reducing power consumption. Despite to offer a longer battery life, the latency still be compromised by the jammer [44]. Another strategy for defending against jamming is to have devices collaboratively identify the jammed region and then route traffic around it. Through this strategy, the devices can effectively identify multiple paths that provide high availability. [45]. Despite effective, in the medical context, this solution may not be applicable. Many works already show that multihop transmission has a higher delay and lower transmission power compared to the one-hop topology. The multihop configuration involves overheads along with its network operation; as increasing the number of hops could lead to a high complexity [7].

The link layer has a sublayer called MAC layer, which concern is in the sharing of the medium among the devices. To fulfill its duty, the MAC layer offers MAC protocols, which require a cooperation between nodes to arbitrate channel use. However, the cooperation required by these protocols making them particularly vulnerable to DoS attacks. An interrogation attack, also Known as the ”sleep deprivation torture”, may drain the batteries in only a few days. They exploit the RTS/CTS handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node’s resources by

repeatedly sending RTS messages to elicit CTS responses from a targeted [44].

Countermeasures: This attack is so lethal that, sometimes, the best solution is the retreat. Channel surfing, for example, involves devices changing the channel they are communicating on when a denial of service attack occurs. In this countermeasure, if an adversary has disrupted the medium, all devices change their channel assignment to a new channel in order to avoid adversary's interference. Though seemingly simple, implementing these basic strategies, however, may a very difficult task as reliably coordinating multiple devices switching to new channels faces the usual challenges of distributed computing: asynchrony, latency, and scalability [46].

Some routing protocols at network layer require that devices announce themselves to their neighbors through broadcast hello messages. Hello flooding is an attack that abuse of these protocols and does not require any encryption knowledge. In the routing protocols, a device that receives such a hello message may assume that it is within a radio range of the sender device. However if an adversary starts to broadcast, with large transmission power, a very high route quality to the display device it could tempt the device to use its route. If the adversary are sufficiently far away from the receiver device, all packets sent by the device are sending into oblivion. This scenario leaves the device in a state of confusion, once that the route isn't within that device's radio range, compromising the device's reliably [47].

Countermeasures: A countermeasure to hello flood attacks is using authentication protocols, which verifies the bi-directionality of a link. In these counter measures, two devices share the same secret key. This key is generated on fly during the communication, ensuring that only reachable devices can decrypt and verify the transmitted data [47].

The transport layer manages end-to-end connections. The protocols at this layer can be connection-oriented or connectionless-oriented. In connection-oriented protocols, after receive a connection request, the device insert an entry in the SYN queue and perform a handshaking to set up an end-to-end connection [44]. The SYN flood attack occurs when a adversary send connection requests in rapid succession, without ever completing the connection, filling the device's SYN Queue. This situation may overwhelm the resources of the device to the point where it becomes unresponsive, or even crashes [48].

Countermeasures: A connectionless protocols are immune to this type of attack, but they might not provide the necessary transport-layer functionality to applications [44]. In the connection-oriented protocol, SYN cookies is a countermeasure to these attacks. Instead of open connection on the beginning of the handshaking, through the SYN cookies, the connection is establish at the end of the handshaking. This technique is used to protect the device's SYN Queue from filling up under SYN floods [49].

At the application layer, an adversary might attempt to overwhelm network nodes with sensor stimuli, causing the wearable device to forward large volumes of data, consuming network bandwidth and draining device's energy. For example, in mechanical sensors an adversary can overstimulate it to create a data flow, which will drains the device's battery rapidly.

Countermeasures: A way to avoid this attack is set sensors with fixed readings intervals. In that way, a sensor will send their data only after a certain period, indepen-

dently of the stimulus applied to the sensor. However, it is not in all sensors that this countermeasure can be applied; some of them must send a data after a desired stimulus occurs. In those cases, a way to mitigate this attack is by carefully set a minimum stimulus to send data. If those counter measures still not reduce the problems, Rate-limiting and efficient data-aggregation algorithms can also reduce these attacks' effects [44].

3.4.2. Man-in-the-middle

A Man-in-the-middle attack may looks like a kind of eavesdropper attack. An adversary comes in between two devices, i.e. Figure 8 shows the wearable device and the display device, and all the communication between them goes only through the adversary. After put itself in-between the communication, the adversary secretly impersonates both the devices to one another and, if necessary, alters the communication between them. In the medical context, such attacks are even more dangerous. If done right, an adversary not only have access to data being sent and received, they can also input their own data, which threats the patient's life.

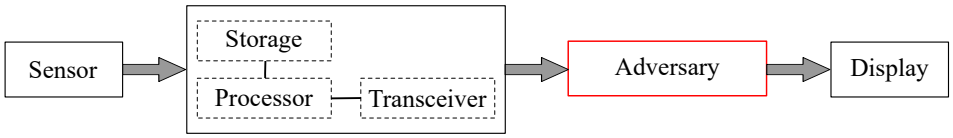

Figure 8. The Generic Architecture of a Wearable Wireless Device under an Man-in-the-middle attack.

Countermeasures: Since a man-in-the-middle attack can succeed only when the adversary can impersonate each device to the satisfaction of the other, crucial point in defending against man-in-the-middle is authentication. Authentication protocols in the wearable devices are substantially different from that classic protocols adopted in computer systems. First, device's constraints do not allow classic protocols to operate efficiently. Second, like discussed at Section 3.1, wearable devices require access polices of dynamic nature. Therefore, they must adopt access control policies to mitigate unauthorized access, however when a life threatening medical event takes place, they should offer a more permissive access control policies [32].

3.4.3. Impersonation

Impersonation attacks are also called spoofing attacks. In these attacks, the adversary assumes the identity of another device, thus receiving messages directed to the device that it fakes. For example, Figure 9 shows an adversary impersonating and display device. This attack is dangerous because, usually, they would be one of the first steps to a deepest intrusion, which may be used for carrying out further attacks. Depending on the access level of the impersonated device, the intruder may even be able to reconfigure the device so that other attackers can easily join or he could remove security measures to allow subsequent attempts of invasion. Besides that, a compromised device may also offer to the adversary access to encryption keys and authentication information [50]. In wearable devices, such attacks can be used to harvest further information regarding the

patient therapies or to feed falsified information to the display device which can delay the response to the needs of the patient and in some cases endanger her life [28].

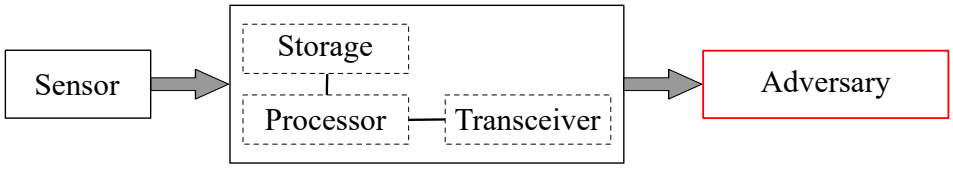

Figure 9. The Generic Architecture of a Wearable Wireless Device under an Impersonation attack.

Countermeasures: A countermeasure to impersonation is through the authentication. Once that the device is able to identify another legitimate device, it is able to prevent impersonation. Like discussed at the previous section, the constraints and requirements of authentication protocols at the wearable devices make authentication process much more difficult.

4. Final considerations

This deliverable provided a review of the wearable devices in terms of architecture, sensor's behavior and communication technologies. With that information, the goal of this deliverable was to investigate how an adversary can explore those characteristics to proceed an attack and how to protect from attacks. Therefore, this deliverable also presented a definition of attack vector, it showed the adversary classes and a list of possible attack vectors in wearable devices. This information may allow understanding the concept behind an attack, which could result in improvements in the countermeasures for them. In summary, the research registered in this deliverable has significant importance in providing a better security for wearable devices that will no doubt truly affect our future. We believe this deliverable may be a source of information towards the future privacy solution design in this project.

References

[1] Kevin Hung, Yuan-Ting Zhang, and B Tai. Wearable medical devices for tele-home healthcare. In *Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE*, volume 2, pages 5384–5387. IEEE, 2004.

[2] Yasser Khan, Aminy E Ostfeld, Claire M Lochner, Adrien Pierre, and Ana C Arias. Monitoring of vital signs with flexible and wearable medical devices. *Advanced Materials*, 28(22):4373–4395, 2016.

[3] Meng Zhang, Anand Raghunathan, and Niraj K Jha. Trustworthiness of medical devices and body area networks. *Proceedings of the IEEE*, 102(8):1174–1188, 2014.

[4] Upkar Varshney. Pervasive healthcare and wireless health monitoring. *Mobile Networks and Applications*, 12(2-3):113–127, 2007.

[5] Huasong Cao, Victor Leung, Cupid Chow, and Henry Chan. Enabling technologies for wireless body area networks: A survey and outlook. *IEEE Communications Magazine*, 47(12), 2009.

[6] Alexandros Pantelopoulos and Nikolaos G Bourbakis. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(1):1–12, 2010.

[7] Samaneh Movassaghi, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. Wireless body area networks: A survey. *IEEE Communications Surveys and Tutorials*, 16(3):1658–1686, 2014.

[8] Blaine Reeder and Alexandria David. Health at hand: a systematic review of smart watch uses for health and wellness. *Journal of biomedical informatics*, 63:269–276, 2016.

[9] Wearable technology market by 2025. `https://www.idtechex.com/research/articles/Wearable-technology-market-by-2025`. Accessed: 2018-02-15.

[10] Apple watch, wearables and the internet of things' potential. `http://www.aberdeenessentials.com/techpro-essentials/apple-watch-wearables-and-the-internet-of-things-potential/`. Accessed: 2018-02-15.

[11] Smartwatches: what are apple, samsung, google and microsoft up to? `https://www.theguardian.com/technology/blog/2013/sep/02/smart-watch-apple-samsung-google-microsoft`. Accessed: 2018-02-15.

[12] How many apple watches has apple sold so far? `http://bgr.com/2017/09/26/apple-watch-sales-estimate-33-million-revenue/`. Accessed: 2018-02-15.

[13] Aviva Rutkin. Pop a silicon pill, 2014.

[14] Moshaddique Al Ameen, Jingwei Liu, and Kyungsup Kwak. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, 36(1):93–101, 2012.

[15] Barbara Filkins. Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon. *SANS Institute*, page 42, 2014.

[16] David Arney, Krishna K Venkatasubramanian, Oleg Sokolsky, and Insup Lee. Biomedical devices and systems security. In *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*, pages 2376–2379. IEEE, 2011.

[17] Jin Wang, Zhongqi Zhang, Kaijie Xu, Yue Yin, and Ping Guo. A research on security and privacy issues for patient related data in medical organization system. *International Journal of Security and Its Applications*, 7(4):287–298, 2013.

[18] Shafiullah Khan and A Khan Pathan. *Wireless networks and security*. Springer, 2013.

[19] Subhas Chandra Mukhopadhyay. Wearable sensors for human activity monitoring: A review. *IEEE sensors journal*, 15(3):1321–1330, 2015.

[20] J Heikenfeld, A Jajack, J Rogers, P Gutruf, L Tian, T Pan, R Li, M Khine, J Kim, and J Wang. Wearable sensors: modalities, challenges, and prospects. *Lab on a Chip*, 18(2):217–248, 2018.

[21] Jonathan D Pegan, Jasmine Zhang, Michael Chu, Thao Nguyen, Sun-Jun Park, Akshay Paul, Joshua Kim, Mark Bachman, and Michelle Khine. Skin-mountable stretch sensor for wearable health monitoring. *Nanoscale*, 8(39):17295–17303, 2016.

[22] Kenneth A Townsend, James W Haslett, Tommy Kwong-Kin Tsang, Mourad N El-Gamal, and Krzysztof Iniewski. Recent advances and future trends in low power

wireless systems for medical applications. In *System-on-Chip for Real-Time Applications, 2005. Proceedings. Fifth International Workshop on*, pages 476–481. IEEE, 2005.

[23] Roy Want. Near field communication. *IEEE Pervasive Computing*, 10(3):4–7, 2011.

[24] Patrick Kinney et al. Zigbee technology: Wireless control that simply works. In *Communications design conference*, volume 2, pages 1–7, 2003.

[25] Jaap Haartsen, Mahmoud Naghshineh, Jon Inouye, Olaf J Joeressen, and Warren Allen. Bluetooth: Vision, goals, and architecture. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2(4):38–45, 1998.

[26] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor CM Leung. Body area networks: A survey. *Mobile networks and applications*, 16(2):171–193, 2011.

[27] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[28] Riham AlTawy and Amr M Youssef. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access*, 4:959–979, 2016.

[29] M Lemoudden, N Bouazza, B El Ouahidi, and D Bourget. A survey of cloud computing security overview of attack vectors and defense mechanisms. *Journal of Theoretical & Applied Information Technology*, 54(2), 2013.

[30] Jerome Radcliffe. Hacking medical devices for fun and insulin: Breaking the human SCADA system. In *Black Hat Conference presentation slides*, volume 2011, 2011.

[31] Ming Li, Wenjing Lou, and Kui Ren. Data security and privacy in wireless body area networks. *IEEE Wireless communications*, 17(1), 2010.

[32] Michael Rushanan, Aviel D Rubin, Denis Foo Kune, and Colleen M Swanson. Sok: Security and privacy in implantable medical devices and body area networks. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 524–539. IEEE, 2014.

[33] Yulong Zou, Xianbin Wang, and Weiming Shen. Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack. In *IEEE International Conference on Communications (ICC)*, pages 2183–2187. IEEE, 2013.

[34] Chunxiao Li, Anand Raghunathan, and Niraj K Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, pages 150–156. IEEE, 2011.

[35] Wendy D Smith, Almut G Winterstein, Thomas Johns, Eric Rosenberg, and Brian C Sauer. Causes of hyperglycemia and hypoglycemia in adult inpatients. *American Journal of Health-System Pharmacy*, 62(7):714–719, 2005.

[36] Fan Zhang, Wenbo He, and Xue Liu. Defending against traffic analysis in wireless networks through traffic reshaping. In *Distributed Computing Systems (ICDCS), 2011 31st International Conference on*, pages 593–602. IEEE, 2011.

[37] Thad Starner. The challenges of wearable computing: Part 2. *Ieee Micro*, 21(4):54–67, 2001.

[38] Charles V Wright, Scott E Coull, and Fabian Monrose. Traffic morphing: An efficient defense against statistical traffic analysis. In *NDSS*, volume 9, 2009.

[39] G Padmavathi, ?? Shanmugapriya, et al. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*, 2009.

[40] Saman Taghavi Zargar, James Joshi, and David Tipper. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE communications surveys & tutorials*, 15(4):2046–2069, 2013.

[41] Konstantinos Pelechrinis, Iordanis Koutsopoulos, Ioannis Broustis, and Srikanth V Krishnamurthy. Lightweight jammer localization in wireless networks: System design and implementation. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6. IEEE, 2009.

[42] Kanika Grover, Alvin Lim, and Qing Yang. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4):197–215, 2014.

[43] Jose M Cano-García, Eduardo Casilari, and Farah Adbib. A study on the effect of packet collisions on battery lifetime of 802.15. 4 motes.

[44] David R Raymond and Scott F Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1), 2008.

[45] Hossen Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu, and Adrian Perrig. Jamming-resilient multipath routing. *IEEE transactions on dependable and secure computing*, 9(6):852–864, 2012.

[46] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang. Jamming sensor networks: attack and defense strategies. *IEEE network*, 20(3):41–47, 2006.

[47] Virendra Pal Singh, Sweta Jain, and Jyoti Singhai. Hello flood attack and its countermeasures in wireless sensor networks. *IJCSI International Journal of Computer Science Issues*, 7(11):23–27, 2010.

[48] Jonathan Lemon et al. Resisting SYN flood dos attacks with a SYN cache. In *BSDCon*, volume 2002, pages 89–97, 2002.

[49] Bo Hang and Ruimin Hu. A novel SYN cookie method for TCP layer DDoS attack. In *BioMedical Information Engineering, 2009. FBIE 2009. International Conference on Future*, pages 445–448. IEEE, 2009.

[50] Latha Tamilselvan and V Sankaranarayanan. Prevention of impersonation attack in wireless mobile ad hoc networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 7(3):118–123, 2007.