mathematics

MDPI

Article

Security Threats and Cryptographic Protocols for Medical Wearables

Luis Hernández-Álvarez [1,2,†], Juan José Bullón Pérez [3,†], Farrah Kristel Batista [4,†] and Araceli Queiruga-Dios [3,4,*,†]

[1] Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), 28006 Madrid, Spain; luis.hdez.alvarez@iec.csic.es
[2] Computer Security Lab (COSEC), Universidad Carlos III de Madrid, 28911 Madrid, Spain
[3] Higher Technical School of Industrial Engineering, Universidad de Salamanca, 37700 Salamanca, Spain; perbu@usal.es
[4] Institute of Fundamental Physics and Mathematics, Universidad de Salamanca, 37008 Salamanca, Spain; farrah.batista@usal.es
* Correspondence: queirugadios@usal.es
† These authors contributed equally to this work.

Abstract: In the past few years, the use of several medical devices is increasing. This paper will pay attention to a device developed to get measures of the temperature of diabetic foot. These wearables usually do not have cryptographic protocols to guarantee data security. This study analyzes the existing security in these devices, and simulate malware propagation taking into account the vulnerabilities and lack of security in these highly-constrained interconnected devices. A simulation of malware spreading in a network made by 10 and 15 individuals with 6 and 34 sensors each one, respectively, is included in this study. To avoid such attacks, a lightweight cryptographic protocol could be a satisfactory solution. Considering the quick development of quantum computers, several current cryptographic protocols have been compromised.

Keywords: cryptography; security model; malware spreading; lightweight cryptography; medical wearables

MSC: 94A60; 68M10; 68M12; 68M14

Citation: Hernández-Álvarez, L.; Bullón Pérez, J.J.; Batista, F.K.; Queiruga-Dios, A. Security Threats and Cryptographic Protocols for Medical Wearables. *Mathematics* **2022**, *10*, 886. https://doi.org/10.3390/math10060886

Academic Editors: Daniel-Ioan Curiac and Qingshan Jiang

Received: 31 January 2022
Accepted: 8 March 2022
Published: 10 March 2022

1. Introduction

In the past few years, "smart" objects and products have given rise to significant progress in industry production and its security. Advances in digitization that have occurred in the industry, combined with internet technologies and future-oriented technologies in the field of so-called "smart" objects (machines and products), have led to a new and fundamental paradigm shift in industrial production and in their security.

The purpose of using cyber-structures (including detection, computing, and communication hardware/software) is the monitoring and control of our physical world. Ciber-physical systems are the consequence of the integration of embedded systems, such are sensors and control systems [1]. In general, health care devices and wearable health-monitoring systems (WHMS), in particular, are emerging as one of the critical areas in Industry 4.0, specifically portable or wearable technological devices, which are the most attractive applications in the IoT area [2,3]. Medical devices for human use are articles with medical purposes such as diagnosis, investigation, monitoring, prevention, or treatment of a disease, or control of physiological or pathological processes. These devices are regulated by the Medical Devices Regulation [4].

Many wearable systems were developed for physiological monitoring. Some of these devices are a wristband to monitor and alert patients at high cardiac-respiratory

risks [5]. A different wearable (BodyGuard) was developed to monitor several parameters in space and on the ground, which had the ability to continuously record the reading of electrocardiogram (ECG), heart rate, room or body temperature, and other variables [6]. The Georgia Tech Wearable Motherboard^{TM} characterized by a wearable motherboard allowed to measure numerous vital parameters and could be incorporated into clothing, and soldiers could wear it easily and comfortably [7,8].

The so-called MagIC (Maglietta Interattiva Computerizzata) is a fabric-based wearable system that took measures of cardiorespiratory signals in individuals with heart problems. This system was used on subjects in daily situations and collected results showed good quality data during most of the time. This allowed arrhythmia events identification in individuals using this wearable [9].

Since then, several health monitoring systems have been developed for patients home-care [10,11]. Recent developments have improved medical devices with an emphasis on characteristics of biosensors and materials such are stretchability (e.g., artificial limbs [12]), ultrathin and conformality (e.g., skin and implantable electronic products [13]), and bio-compatibility and biodegradability (e.g., silicon sensors for the brain [14]).

There are several possible classifications of health monitoring systems. In this paper, the following three categories will be considered [15]:

1. Remote health monitoring systems (RHMS) are devices situated far from the system receiving the collected data.
2. Mobile health monitoring systems (MHMS) are mobile devices such as mobile phones, computers, pocket laptops, etc., that monitor health parameters.
3. Portable health monitoring systems or wearables include WHMS, RHMS and/or MHMS. These devices can be carried by patients in such a way that the sensors are integrated into clothing or accessory. These are called wearables. Thus, these give rise to smart fabrics, smart-textiles, or e-textiles.

Mainly motivated by rising health care expenditures and because of the recent technological advances in microsensors, health monitoring systems can reduce hospitalization time, and the excessive workloads on healthcare personnel, consultation time, waiting lists, etc. An example of this case is people with diabetes, who are prone to some form of nerve damage or injury throughout their lives, especially if they suffer diabetes over a long time. The diabetic disease is considered an important health problem, due to its frequency and its enormous economic and social impact [16]. Diabetics affects the quality of life of people suffering this disease, because it causes ulcers on patients' feet. Moreover, peripheral neuropathy and vascular insufficiency are the most common chronic complications of this disease. These healthy problems in diabetic patients made some research teams work in wearables to measure different variables in these patients' feet, such as the temperature [17,18].

A wearable medical device to measure the temperature of the foot consists, fundamentally, of a series of sensors that continuously (in a given period of time) measure the temperature at different regions of interest (ROI) of the foot that have been previously selected. A sock with sensors located in specific ROI is a wearable capable of sending data to an external device and create an alarm in case of ulceration development. Furthermore, it is made up of conductive tissues that carry these measurements to a base station or sink. A health surveillance wireless sensor network designed to deliver personalized healthcare is also called a body area network (BAN) [19].

Figure 1 shows a representation of the connections of a wearable that takes measures of foot temperature, the architecture of a conventional wearable network and the main elements: the wearable itself, a base station/gateway, cloud servers, users, and their control tools. The wearable includes elements of the network that are responsible of creation, detection and (pre-)checking of basic information. On the other hand, routing protocols in a WHMS are established in four tiers: the first one is within the device, where sensors collect the data and send them to the controller through a thermal-aware routing protocol, such are ATAR [20] or WETRP [21]. Then, the controller processes the received information

and send it to the gateway. Finally, collected data are transmitted to the user mobile phone by Bluetooth Low Energy (BLE), Wi-Fi or Radiofrequency (RF), and from here to his/her computer or the corresponding health-center through Internet [22,23].

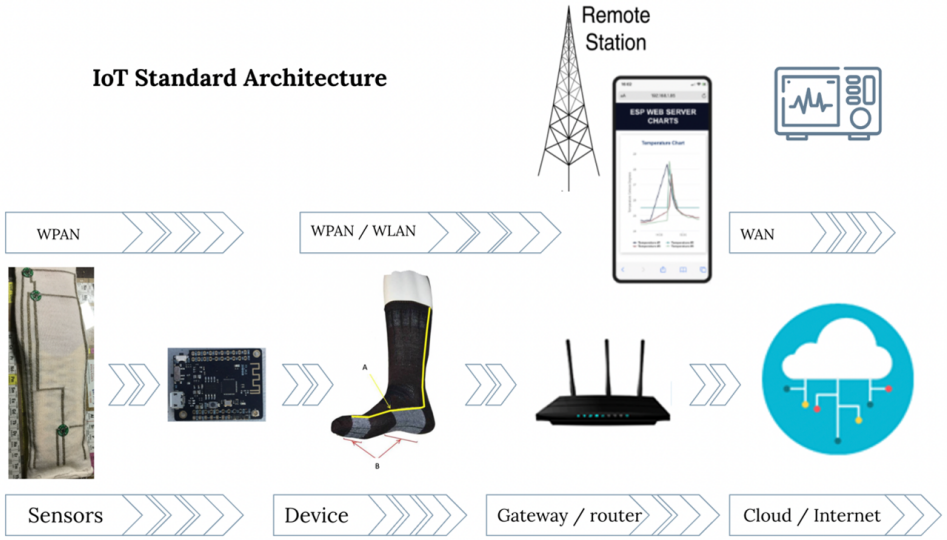

Figure 1. Overview of the architecture of an IoT-based health device to measure the foot's temperature.

The security needs for IoT-based healthcare solutions are similar to those considered in common communication scenarios: integrity (patient information cannot be altered or changed by unauthorized personnel), availability (data must be available to authorized persons upon request), confidentiality (sensitive information cannot be used by unauthorized individuals, entities or processes) and non-repudiation (individuals cannot deny an action they have carried out) [24,25].

The main limitation of medical applications is their constrained resources. This drawback makes several cryptographic protocols not appropriate for these devices with small size and memory, that require low computation power, short time battery, short memory, and low bandwidth. Lightweight cryptography (LWC) reduces computation time and complexity and assure security [26–28].

This paper is organized as follows: Section 2 includes a detailed description of the security in medical devices, with an emphasis on vulnerabilities in their design and functioning protocols. A simulation of a malware attack against medical devices is included in Section 3. As a solution to make the devices more secure, a proposal of lightweight cryptography protocol is included in Section 4. Finally, the conclusions of this study are stated.

2. Security in Medical Devices

Wearable health monitoring systems must adapt to strict medical criteria and consider ergonomic restrictions and hardware limitations [29]. Research in this field is focused on producing garments with functionalities that improve the lives of its users. These medical devices must be resistant to both natural or intrinsic failures and malicious attacks [30]. An intrinsic failure should be understood as a malfunctioning in the mechanism of the device, which could imply an incorrect reading in the sensing procedure or an error during the transmission of the data [31]. These situations are occasional and, in general, are either automatically solved in the next operation process or manually fixed by an expert. Hence, natural failures do not represent a threat, but just a momentary loss of usability. On the other hand, an attack executed on a WHMS by an adversary supposes a more dangerous scenario, even more critical than hacking any other device, such as a laptop or a mobile phone, as it can cause physical harm to the owner. For instance, hacking a diabetic smart

contact sensor from false readings can lead to the wearer not receiving warning or danger signals [32].

The limitations caused by vulnerabilities create attack vectors that might be utilized by an attacker to gain access to the information of a particular individual or to control the device itself. Several of these attack vectors can be identified, being the most important the followings [33,34]:

- Firmware vulnerabilities: an inadequate development process of the software or the lack of authentication protocols in firmware updates facilitate the introduction of an altered, malicious firmware by an attacker. This vector is usually exploited by conducting inverse engineering to the original firmware, concretely in the cases in which there are no protection techniques as code obfuscating/packing [35]. Some authors defend that this attack vector is the most powerful, as it scales better than the others, and proportionates more benefits to the adversary, only requiring one interaction with the wearable [36].
- Communication protocols: most of the current WHMS transfer data to a database server or other electronic devices is done via BLE, Wi-Fi, and RF. These channels have been demonstrated in several studies to be vulnerable and leak the information of the patients [37,38]. Especially harmful is the scenario in which the transmitted data are not encrypted and can be directly interpreted [39].
- Applications and sensors: excessive privileged apps and sensors might be used by attackers to attack WHMS. This scenario can be conducted by substituting the original app by a malicious one, specifically designed by the adversary to perform concrete actions. Likewise, leaks of sensors readings can be used to infer the activity the patient was executing at a certain time [39].

Additionally, an attacker may be interested in accessing a particular WHMS for different reasons. Depending on the purpose of the adversary, the malware (malicious software) may perform an attack identified as a passive attack or an active attack [37]. Passive attacks are performed while routing the measured data, and the adversary tries to sniff the communications of the WHMS, which leads to the interception of the patient information. Changes in the destination of storage by the attacker also belong to this type of attack. On the other hand, active attackers are capable of modifying the patients' data or introducing new, false data streams to compromise the WHMS records or control the device [40]. There exist other, more concrete attacks divisions depending on their nature, as exposed in [24,29]. The most critical and common attacks are explained below:

- Eavesdropping: this attack takes advantage of poor communication protocols to secretly stole the transmitted data [38]. By doing this, the attacker can not only obtain critical health-related information of the patient, but also know the activities he has performed, the places he has visited and the format in which the WHMS stores the data [41].
- Replay attack: the attacker can go one step further from eavesdropping, introducing previous, eavesdropped data to compromise WHMS readings or gain illegitimate access to the patient's devices. For example, if a wearable device has the permission to unlock the patient's smartphone, the adversary might be able to unlock it by replaying information that has previously eavesdropped [29].
- Data tampering/modification: this attack occurs when the attacker modifies the measured data without having the proper authorization. To do this, the attacker must know the format in which the WHMS reads and transmits information, therefore this type of attack starts with an eavesdropping attack [34].
- Denial of service (DoS): the purpose of this attack is to alter the correct functioning of the WHMS by collapsing it with continuous orders. In this way, the battery of the device will run out very rapidly, or the patient will be unable to use it. A distributed DoS (DDoS) attack performed by botnets could lead many nodes to be involved in the attack [38,42].

- Side-channel attack: in this type of attack, the adversary uses information from the implementation of a WHMS to gather critical details of the patient. For example, an electromagnetic analysis can be conducted to derive the power consumption of a WHMS and, hence, extract the activities it is executing [43]. Likewise, it has been shown that information acquired from motion sensors of wearable devices can be used to profile the patient [39].

The rest of this section was divided into three parts, one for each attack vector previously defined (firmware vulnerabilities, communication protocols, and applications and sensors). For each vector, the current literature was studied, and a brief description of the studies that have successfully executed an attack on a WHMS was included. Since some works use more than one attack vector in their methodology, each article was allocated in the group of its principal attack vector.

2.1. Firmware Vulnerabilities

Since the development of medical devices, wearables, and WHMS, several authors have claimed that security and privacy issues are not considered in the design and construction processes [29,44]. These weaknesses include the absence of software/firmware protection techniques (code obfuscating/packing) [35] and the lack of authentication processes in the gateway to update the server [33]. In fact, in [45] the authors investigate the security level of different smartbands and state that their firmware vulnerabilities enable the introduction of malicious versions, compromising the integrity of patients' information and facilitating the remote control of the wearable. The authors identified that some devices did not implement a protocol to verify firmware updates, and, when included, were easy to bypass.

One example of firmware attack can be found in [44], where an attack is implemented on the wearable medical device Nike+Fuelband, which include a USB connector to be synchronized. The authors took advantage of the lack of read and write protection on the device and designed a process to obtain the original firmware. Then, they introduced a modified version of the firmware via the USB connector, which allow them to modify the texts displayed by the wearable. Similarly, in 2016, Rieck et al. [36] showed how to successfully attack the fitness tracker Withings' Activité by introducing a false firmware update. They first located the local firmware address and performed reverse engineering to find the code structure in charge of firmware update verification. Once this was achieved, the authors introduced the modified firmware into the wearable as an update with the Health Mate app, gaining control of the device.

In the work presented in [46] the authors introduce several modified versions of the firmware by building a fake gateway on a PC. The developed methodology consisted on three steps: (1) reverse engineer of the gateway app of the device, (2) analysis of the BLE communication between both elements, and (3) reverse engineer of the original firmware.

Another example of an attack exploiting firmware vulnerabilities is [47]. In this case, with the introduction of a personalized firmware, they were able to disturb the correct functioning of the device, eliminating the encryption process and eavesdropping on the patients' information. Additionally, they were also capable of obtaining the user credentials to execute a replay attack.

2.2. Communication Protocols

WHMS usually transmit the measured data to database servers, update their configuration using a concrete smartphone app, and communicate with other devices for different purposes. These communications protocols are principally based on BLE, RF, or Wi-Fi [34], and the little attention given to these transmission options have created a critical attack vector. For example, in [48] two successful attacks against an insulin pump are executed by reverse engineering the wireless communication protocols of the delivery system. One of the attacks was passive and allowed to eavesdrop on the signals and obtain information of the insulin pump, such as the commands that it received. The second attack was active,

and enabled the adversary to remotely control the insulin pump. Similar attacks are shown in [49].

In [50], Rahman et al. construct FitBite, a tool that exploits the vulnerabilities of the medical tracker Fitbit, and attack this device tracking private data, injecting and modifying the measured data in real time, and replaying the user's account data. They demonstrated how these actions could be used to conduct DoS attacks, collapsing the functioning and draining the battery of the device. Another example of the vulnerability of BLE is included in [35], where the authors examine the security of nine different fitness trackers and explain the vulnerabilities of their communication protocols. In fact, they are able to eavesdrop and manipulate measured data and change the configuration of the devices, performing DoS attacks without changing any source code.

In 2016, several articles, such as [51–53], were published and demonstrated that BLE and Wi-Fi connections are vulnerable to eavesdropping, brute force, and man-in-the-middle (MITM) attacks. These attacks were performed on devices available in the market, such as Fitbit, Jawbone UP, Samsung smartwatches, and Pebble Watch. Apart from Fitbit, Xiaomi Huami, and Samsung Gear3 were also attacked in [54]. Although this work recognize security improvements in the Samsung Gear3, the authors are able to use the BLE connections of the wearables to eavesdrop on the information and track the identity of the patients.

Wood et al. [55] proposed a method based on Shannon entropy tests and Chi-squared tests to collect network traffic from WHMS, detecting plain messages transmission of the packet payload and compromising the security of sensitive medical information of the patients. Aliasgari et al. [56] analyzed in their research the safety of the transport layer security (TLS) protocol in 25 mHealth Android applications. Their results indicate that the majority of them present weak TLS configurations and are susceptible to MITM attacks. BLE communications between wearable devices and smartphone apps, and between these apps and servers using the Internet were examined in [57]. The authors found that these communications were not secure, sending patients credentials in clear text and allowing connections with unbounded devices. A work by Sethuraman et al. [58] uses unmanned aerial vehicles to interrupt Bluetooth and Wi-Fi data transmission of WHMS, leading to data interception, data corruption, and service unavailability (DoS).

The research presented in [59,60] execute eavesdrop, replay and DoS attacks on wearable devices, but also propose new tools based on Artificial Intelligence (AI) to find anomalies in the devices' functioning, create an intrusion detection system, and protect the wearables.

2.3. Applications and Sensors

In this attack vector, patient's critical information might be compromised by non-secure or malicious apps designed by adversaries that simulate the functioning of the legitimate ones. In this second case, the WHMS is forced to be connected to the fake app, which compromises the security of the data. In [61], different characteristics of several apps of several operating systems were analyzed, including tracker connectivity and personal information leakage. An example of a malicious app attack is included in [38], where the authors constructed a fake Android application to sniff packets, analyze commands and send fake commands. Their results showed that they were able to read and send messages between the Bong 3 HR wristband and a smartphone, perform fake authentication in MiBand2 and read messages and gain remote control of the TW64 and Mambo HR wearables.

Interestingly, the use of sensors recordings of wearable devices can lead to side-channel attacks that attacker might use to identify the activities performed or the applications employed by a concrete user. This type of attack is usually executed using AI tools, since they can identify patterns and correlate the sensorial data with the actions of a user. For example, in [62] the authors employ simple linear regression, random forests, and k-nearest neighbors to predict the words written by the user with his smartphone keyboard

(keystroke dynamics) based on his wrist movements measured with a wristband. Similar attacks are proposed in [63], using a support vector machine, and [64], using tree-based key sequence inference and backward subpath integration.

3. Simulation of a Malware Attack against Medical Devices

Attacks to WHMS are possible because of vulnerabilities in their design and functioning protocols. An attack executed on a WHMS can disturb functionality, lead the user not to receive information about vital signals and may cause severe injury or death. As users data are sensitive, attacks suppose a dangerous scenario, even more critical than hacking any other device, such as a laptop or a mobile phone [32,65].

Medical devices and their connections are similar to a wireless sensor network [24]. Figure 2 represent the scenario of a malware attack against a WHMS.

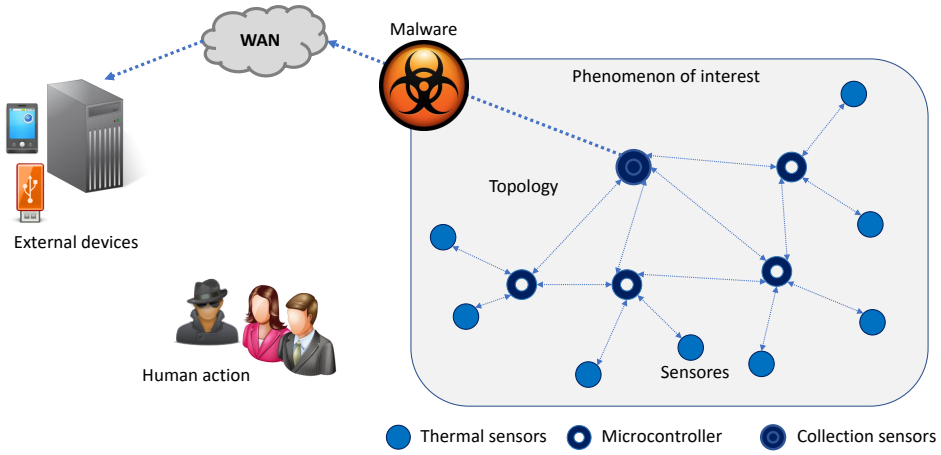

Figure 2. Scheme of the agents involved in the proposed model.

A simulation of a malware attack against medical devices with an SEIRS-D agent-based model [66] was developed. Agent-based models (ABM) are models where individuals (agents) are entities that are unique and autonomous, which interact with their neighbours and with their near environment. An ABM can be made up of different agents that represent different individuals within the system under analysis. Generally, these models are suitable for systems with heterogeneous, autonomous, and proactive actors in which individual characteristics cannot be neglected.

In this model, in each time t, the sensor nodes can assume one of the following states:

- Susceptible: the sensor has the characteristics for been infected by malware.
- Exposed: the malware has attacked the sensor, but the sensor cannot be transmitted to the sensors neighbors.
- Infected: the computational characteristics of the sensor allows it to be infected by malware and a sensor is capable of transmitting malware to its neighbors and the gateway.
- Recovered: the malware has been removed from the sensor, either by updating or fixing.
- Dead: the sensor battery life may be exhausted faster because of the infection of malware, and the sensor is no longer useful.

The states of SEIRS-D model can be determined from the characteristics of the agents involved in the transmission and infection of malware (see Table 1). The agents and their characteristics involved in this process are as follows:

Table 1. Agents with their characteristics.

Type of Agents	Characteristics
WHMS sensors	Type: Sensor or sink nodes Computational capacity: Low Energy consumption: Low or medium Capacity of transmission and reception of information: Low Security level for nodes: Low or medium Data collection method: Periodical or requested Duty cycle: Active or inactive
Malware	Type: IoT based malware Spreading mechanisms: Self-replication, exploit, or user interaction Target: DoS/DDoS or botnet attack, or information exfiltration
Network topology	Type: BAN Routing protocols: ATAR/WETRP, BLE/Wi-Fi/RF or Internet
Phenomenon of interest	Risk of malware attack: medium or high
Human action	Level: medium or high
External devices	Risk of devices infected with malware: Low, medium or high

- WHMS sensors: are responsible for measuring various vital signs of a person, such as foot temperature.
  - Type of sensors: can be sensor, sink, and cluster-head nodes. Each one performs a particular function within the device.
  - Computational capacity: each WHMS can have computational capabilities, such as a microprocessor, memory, and storage, which allow performing different measurements.
  - Energy consumption: depends on the number and the frequency of measurements.
  - The capacity of transmission and reception of information: is related to the computational capacity; for example, a device with higher computational capacity will process more data and, in turn, transmit that information to its neighbours.
  - Security level: is critical, as the health data handled by these sensors are sensitive.
  - Data collection method: refers to the technique and periodicity in which a sensor performs measurements.
  - Duty cycle: when the sensor is not taking measurements, it may be in a inactive state, while its state is active when it is taking measurements.
- Malware: are those malicious codes that seek to perform unauthorized actions on the devices.
  - Type of malware: WMHS sensors may be affected by IoT-based malware.
  - Spreading mechanism: malware can use self-replication, exploit, or user interaction to perform malicious actions.
  - Target: the most common attacks for WHMS are DoS/DDoS or botnet attacks.
- Network topology: represents the form of communication of the sensors.
  - Type of topology: WHMS is based on a body area network.
  - Routing or communication protocols: depending on the tier, the communication is established through different protocols.
- The phenomenon of interest: the environment where these devices are located is outside hospitals to monitor patients during their daily activities.
  - Risk of malware attack: can range from low to high according to exposure to unsafe networks.
- Human action refers to human intervention in the device functioning.
  - Human action level on the network: may vary according to the required patient interaction with the device or sensors.

- External devices: connections to external devices for manual data download may expose the sensors to malware.
  - Risk of devices infected with malware: those external devices that can connect to unsecured networks are at higher risk of exposure to malware, and therefore, if a WHMS connects to this external device, it may have a high probability of malware infection.

The following values have been used for the agent characteristics in both scenarios: the computational capacity is low, the energy consumption is medium, the information transmission capacity is low, the security level ranges from low to medium, and a periodical data collection.

The propagation of IoT-based malware has been simulated, using self-replication to turn the devices into a botnet. The network type for medical devices is always a personal area network; in addition, connection via BLE/Wi-Fi/RF is used for these cases. Finally, the interaction of humans with devices is high, so the risk of malware attacks is high, too, and the risk of infecting devices is also high.

Considering a scenario of 10 diabetic patients using a wearable to collect temperature data from their feet, with 6 sensors (3 per foot) distributed in specific regions of interest [18], the simulation is shown in Figure 3. This simulation was made with MESA framework, Apache2 licensed agent-based modeling environment [67]. After 168 h, the number of susceptible devices decrease, and susceptible individuals increase.

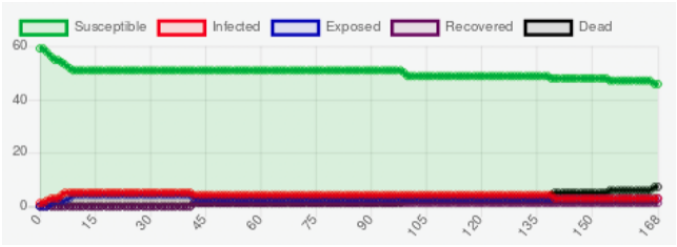

Figure 3. Simulation of malware spreading after infecting a WHMS netweork made of 10 devices with 6 sensors each one.

This behavior is even more drastic when the network is bigger. More sensors could be added to the wearable to get more measures and analyze the results. In the case of 15 diabetic patients with 17 sensors in each foot, the graph shows that the malware invades all the network. This fact can be appreciated in Figure 4, where the number of susceptible sensors decrease and after 24 h, exposed, recovered, and death sensors are bigger than susceptible ones.

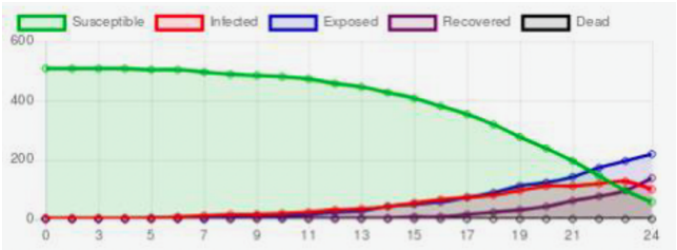

Figure 4. Simulation of malware spreading after infecting a WHMS network made of 15 devices with 34 sensors each one.

4. Cryptographic Protocols to Secure Medical Devices

Healthcare systems have reduced computation and storage capabilities and they are highly-constrained interconnected devices where current cryptographic algorithms, designed for desktop/server environments, are not suitable. Apart from the device capabil-

ities, the implementation of a cryptographic protocol considers the hardware and software characteristics and possibilities [65].

In 2015, the national institute of standards and technology (NIST) initiated a process to find a suitable standard lightweight cryptographic algorithm to be used in constrained and restricted environments where the current NIST cryptographic standards are not acceptable or are inadequate [68]. This process is called Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR). During the evaluation process, three criteria were considered to accept or discard algorithms: cryptographic security, performance, and cost in its implementation. For the second-round selection of candidates, other characteristics where analyzed: functionality, underlying components, design approaches, and supported key and tag sizes [69]. In March 2021, from the initial list of 57 proposals, a list of the following 10 finalists was announced: Ascon, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, and Xoodyak [70,71]. Several authors performed different analysis to the NIST candidates. The modes of operation and the efficiencies of the schemes were provided in [72]; the costs, performance and security were analyzed in [73]; the metrics considered in [74] were performance, area, energy, and area $\times$ energy; and the area, the time the number of cycles to encrypt one block, the energy, the block size, and power coefficients were used as input parameters for a general metric whose purpose was a comparison of lightweight algorithms [75].

In the proposal of a new LWC system, quantum threats should be considered. During the NIST selection of candidates, the post-quantum security property was considered in case multiple candidates had similar characteristics about security and performance. Integer factorization, discrete logarithm, and elliptic-curve discrete logarithm problems, which are the robustness of public key cryptography, can be efficiently broken with a quantum computer [76]. Quantum resistant algorithms are able to reduce the computation time to break symmetric cryptosystems and make their security similar to the same protocols with half-length keys [77]. In the case of asymmetric cryptography, the NIST is in the process of selecting quantum-resistant cryptographic algorithms that are not vulnerable to quantum computers [78]. In any case, LWC is based on symmetric-key cryptography with the goal of as low as possible implementation costs of hardware and the implementation efficiency as high as possible, assuring security [79].

One of the NIST LWC CAESAR competition finalists was explicitly designed for quantum resistance, and it is permutation-based lightweight, which makes the proposal to have a simple structure and fast running speed. Ascon (its variant Ascon-80pq) is resistant to side-channel attacks, with a key size $k \leq 160$ bits and a 320-bit permutation, and provides authenticated encryption with associated data (AEAD) and hashing functionality. Two more candidates from the second round provided security against quantum adversaries: Gimli (permutation-based) and SATURNIN (block cipher based), but these were not considered as finalists. Thus, Ascon is the only one that can be considered as the best option for a quantum-resistant algorithm [70].

The Mirai botnet attacked many IoT devices in 2016 and caused several damage to smart devices since infected devices were used as a launch platform for DDoS attacks [80,81]. The Ascon AEAD scheme can mitigate such vulnerabilities by improving throughput and security with a field-programmable gate array platform, which provides higher speed, lower cost, faster development time, flexibility and configurability [82]. This improvement prevents attacks and secure the hardware from attacks [83].

In Ascon cipher suite, the authenticated encryption algorithm, $\mathcal{E}$, and the decryption algorithm, $\mathcal{D}$, are parameterized by the rate (data block size) r, two internal round numbers, a and b, and the key length, k. The inputs are a k-bits secret key K, a nonce (public message number) N with 128 bits, associated data A of arbitrary length, and a plaintext M of arbitrary length, the authenticated encryption procedure output is

$$\begin{gathered}\mathcal{E} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{P} \longrightarrow \mathcal{C} \times \mathcal{T} \\ \mathcal{E}_{k,r,a,b}(K, N, A, M) \mapsto (C, T),\end{gathered}$$

where C is the authenticated ciphertext with the same length as M, and a 128-bits authentication tag, T, which can authenticate the associated data and the encrypted message.

The decryption procedure takes the same parameters, K, N, A, and adds the authenticated encryption procedure output, i.e.,

$$\mathcal{D} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T} \longrightarrow M \cup \{\perp\}$$
$$\mathcal{D}_{k,r,a,b}(K, N, A, C, T) = \{M, \perp\},$$

and it obtains the plaintext when the tag is correctly verified or an error, $\perp$, in case the tag verification fails.

Moreover, $\mathcal{E}_{k,r,a,b}(K, N, A, M) \mapsto (C, T)$ if and only if $\mathcal{D}_{k,r,a,b}(K, N, A, C, T) = M$. For encryption and decryption procedures, just one pass over the data is required.

On the other hand, the family of hash functions for Ascon is defined by parameterizing the extendable output function X with the rate, r, numbers a and b as defined before, and an output length limit h.

$$X_{h,r,a,b}(M, l) = H.$$

Thus, this function maps an input message, M, to a hash output, H, with length $l \leq h$.

Most symmetric-key protocols under NIST consideration use permutation as underlying primitive, this is also the case of Ascon Cryptosystem [84,85]. The rest of candidate algorithms are based on block-cipher, tweakable block cipher and stream cipher in less percentage.

Figure 5 shows how the Ascon suite operates. Four stages are part of this flow [84,86]:

1. Initialization: The algorithm starts with the key, K, the nonce, N, the rate, r, and the round numbers a and b as 8-bit integers. During this phase, a rounds of the round transformation π are applied to the initial state.
2. Processing associated data: during this state the data A is processed in r-bits blocks.
3. Processing plaintext/ciphertext: the plain text, P and the ciphertext, C, are processed in blocks of r bits.
4. Finalization: The encryption algorithm output consist on the tag, T, and the ciphertext blocks, C_i, and the decryption one returns the plaintext blocks, P_i (if T matches the calculated tag from the secret key).

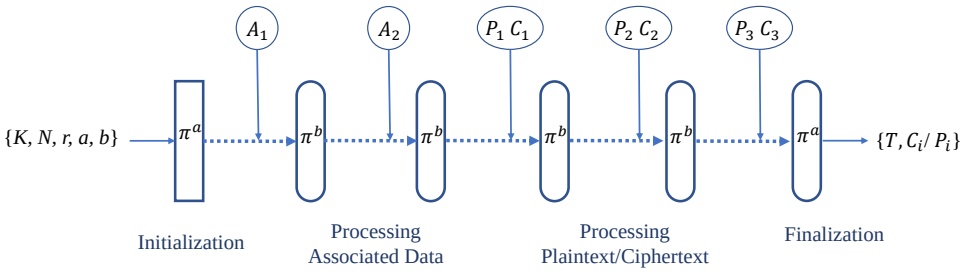

Figure 5. Ascon operation in authenticated encryption and decryption procedures.

Recommended parameters for the Ascon-80pq scheme are a key size $k = 160$ bits, a nonce and tag size $n = t = 128$ bits (lowercase letters represents the size and capital letters the corresponding parameters), a rate $r = 64$ bits, and $a = b = 12$ for the permutations (both initialization and finalization), p^a, and the intermediate permutation, p^b, respectively. For both encryption and decryption procedures, these permutations are just only evaluated in one direction, which significantly reduces the computational costs. Ascon-80pq provides 128-bit security in the AEAD, i.e., the confidentiality of the plaintext and the integrity of ciphertext are protected. The encryption algorithm protects 2^{67} bytes of processed plaintext, which make this system adequate for a lightweight application, secure against classical attacks [86].

Figure 6 shows the simulation of a secure WHMS network when the security level for nodes is medium, the phenomenon of interest (risk of malware attack) is medium, and

the external devices (risk of devices infected with malware) is low. In this case, there is a first stage where infected devices increase (between 46 and 120 h). After this time, some infected devices become death until 160 h, and then an equilibrium is reached.

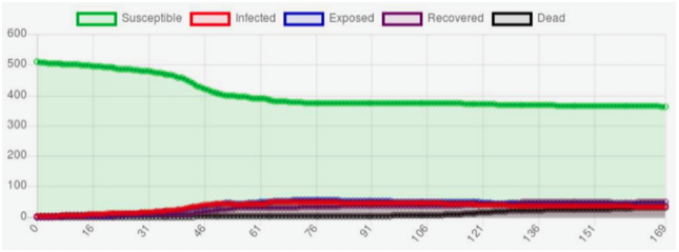

Figure 6. Simulation of malware spreading after infecting a secure WHMS network.

5. Discussion

With the massive use of wearable health–monitoring systems, security challenges are increasing rapidly. Cybercriminals use malware as their main weapon to carry out security attacks, causing significant damage and loss to IoT users. The main objectives of cybercrimes against WHMS are firmware vulnerabilities, communication protocols and applications and sensors to get users' sensitive information or to damage devices.

The analysis of the vulnerabilities of a device has the purpose of mitigating or reducing the risks to which the system is exposed, with the purpose to protect the information that is stored in the servers or transmitted through different routing protocols to the network. For this reason, cybersecurity studies for different environments are becoming more and more frequent, as is the case of medical devices, made up of microsensors whose purpose is to monitor different physical phenomenon. In this study, the physical phenomena is the temperature that is measured in diabetic foot.

In this study, the spread of malware in a medical network is simulated using an agent-based model to improve the cybersecurity mechanisms that can be applied to this type of network. One of the advantages of ABM is that it considers individual characteristics, which is particularly useful in the case of wearable health-monitoring systems because a failure in a component could cause serious health problems. This is not the case of global models, that include general characteristics of the network. Malware spreading depends on the environment; the spread is different in the military, industrial or medical sectors, Internet, Wi-Fi, BLE, or thermal-aware routing protocols, etc. Some studies suggest implementing security tools such as Honeypots for wireless sensor networks, which allow real-time data collection of a malicious attack in a controlled environment.

Three different environments were considered for this simulation. In the first one, 10 individuals wear a device made of six sensors, three per foot (considering a medical device to take foot temperature measures). In this case, the simulation showed that the malware was spreading slowly. After 168 h, there were still 45 sensors (corresponding to 7 persons) that were not infected. In the second simulation the number of devices was considerably increased. It considered 15 individuals with 34 sensors each one, i.e., a total amount of 510 sensors distributed in the corresponding regions of interest. The malware spreads rapidly. In 21.6 h, the number of susceptible are equal to the number of exposed sensors, so, these sensors will not spread the malware. Moreover, from the 11th hour, infected and exposed increase together until the 18th, where infected decrease and exposed and recovered increase. As dead sensors do not increase, devices will recovered from the malware attack. The recovery begins when infected decrease under recovered and exposed. The third simulation considered a secure network. In this case, the risk of malware attack and devices infected is medium and low, respectively. An equilibrium is reached in this simulation after 160 h. Moreover, the malware spreading is slow, with a maximum of infected nodes at 76 h.

Most medical devices do not have sufficient resources to provide complex cryptography. Limitations in their computational capacity, energy consumption, capacity of

transmission and reception of information, etc., make traditional cryptographic algorithms not suitable for them. A cryptographic protocol for constrained resources is considered an acceptable solution to secure health devices. The primary choice for the NIST protocol that could be used with all security considerations is the Ascon-80pq from the Ascon cipher suite. No weakness was found for this protocol of excellent implementation characteristics. Ascon is highly appropriate for wearable health-monitoring lightweight systems where several communications protocols are involved, it can be efficiently used for these systems where side-channel resistance is essential. Moreover, Ascon is a simple algorithm, as it only uses bitwise Boolean functions.

The security provided by all Ascon family members protects the plaintext confidentiality and the plaintext, the associated data and the public message number integrity. The use of the same underlying permutation for authenticated encryption and hashing reduces the area requirements for hardware implementations and restrict the code base and thus, the workload is reduced.

Author Contributions: Conceptualization, A.Q.-D. and J.J.B.P.; methodology, L.H.-Á. and A.Q.-D.; software, F.K.B.; validation, L.H.-Á., J.J.B.P. and A.Q.-D.; investigation, L.H.-Á. and F.K.B.; resources, L.H.-Á. and J.J.B.P.; writing—original draft preparation, A.Q.-D. and F.K.B.; writing—review and editing, L.H.-Á. and J.J.B.P.; visualization, J.J.B.P.; supervision, A.Q.-D.; funding acquisition, A.Q.-D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Spanish State Research Agency (AEI) of the Ministry of Science and Innovation (MICINN), project P2QProMeTe (PID2020-112586RB-I00/AEI/10.13039/501100011033), co-funded by the European Regional Development Fund (ERDF, EU).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: Luis Hernández-Álvarez would like to thank CSIC Project 202050E304 (CASDiM).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

WHMS	Wearable health–monitoring systems
ECG	Electrocardiogram
RHMS	Remote health monitoring systems
MHMS	Mobile health monitoring systems
ROI	regions of interest
BAN	Body area network
BLE	Bluetooth Low Energy
RF	RadioFrequency
MITM	Man-in-the-middle
TLS	Transport Layer Security
DoS	Denial-of-service
AI	Artificial Intelligence
LWC	Lightweight cryptography
ABM	Agent-based model
AEAD	Authenticated encryption with associated data
CAESAR	Competition for Authenticated Encryption: Security, Applicability, and Robustness

References

1. Sacală, I.Ş.; Moisescu, M.A. The Development of Enterprise Systems based on Cyber-Physical Systems Principles. *Rom. Stat. Rev.* **2014**, *4*, 29–39.
2. Robson, K.; Pitt, L.; Kietzmann, J.; Halvorson, W.; Wallstrom, A. Wearable Technology: Trends and Opportunities for Organizations. In *Celebrating America's Pastimes: Baseball, Hot Dogs, Apple Pie and Marketing*? Springer: Berlin/Heidelberg, Germany, 2016; p. 801.

3. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
4. European Union. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. *Off. J. Eur. Union* **2017**, *117*, 1–175.
5. Anliker, U.; Ward, J.A.; Lukowicz, P.; Troster, G.; Dolveck, F.; Baer, M.; Keita, F.; Schenker, E.B.; Catarsi, F.; Coluccini, L.; et al. AMON: A wearable multiparameter medical monitoring and alert system. *IEEE Trans. Inf. Technol. Biomed.* **2004**, *8*, 415–427. [CrossRef]
6. Mundt, C.W.; Montgomery, K.N.; Udoh, U.E.; Barker, V.N.; Thonier, G.C.; Tellier, A.M.; Ricks, R.D.; Darling, R.B.; Cagle, Y.D.; Cabrol, N.A.; et al. A multiparameter wearable physiologic monitoring system for space and terrestrial applications. *IEEE Trans. Inf. Technol. Biomed.* **2005**, *9*, 382–391. [CrossRef] [PubMed]
7. Gopalsamy, C.; Park, S.; Rajamanickam, R.; Jayaraman, S. The wearable motherboard^{TM}: The first generation of adaptive and responsive textile structures (arts) for medical applications. *Virtual Real.* **1999**, *4*, 152–168. [CrossRef]
8. Park, S.; Jayaraman, S. Enhancing the quality of life through wearable technology. *IEEE Eng. Med. Biol. Mag.* **2003**, *22*, 41–48. [CrossRef] [PubMed]
9. Di Rienzo, M.; Rizzo, F.; Parati, G.; Brambilla, G.; Ferratini, M.; Castiglioni, P. MagIC system: A new textile-based wearable device for biological signal monitoring. Applicability in daily life and clinical setting. In Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference, Shanghai, China, 17–18 January 2005; pp. 7167–7169.
10. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications of wireless sensor networks: An up-to-date survey. *Appl. Syst. Innov.* **2020**, *3*, 14. [CrossRef]
11. Qiao, L.; Benzigar, M.R.; Subramony, J.A.; Lovell, N.H.; Liu, G. Advances in sweat wearables: Sample extraction, real-time biosensing, and flexible platforms. *ACS Appl. Mater. Interfaces* **2020**, *12*, 34337–34361. [CrossRef]
12. Wang, B.; Facchetti, A. Mechanically flexible conductors for stretchable and wearable e-skin and e-textile devices. *Adv. Mater.* **2019**, *31*, 1901408. [CrossRef]
13. Lou, Z.; Wang, L.; Jiang, K.; Wei, Z.; Shen, G. Reviews of wearable healthcare systems: Materials, devices and system integration. *Mater. Sci. Eng. R Rep.* **2020**, *140*, 100523. [CrossRef]
14. Kang, S.K.; Murphy, R.K.; Hwang, S.W.; Lee, S.M.; Harburg, D.V.; Krueger, N.A.; Shin, J.; Gamble, P.; Cheng, H.; Yu, S.; et al. Bioresorbable silicon electronic sensors for the brain. *Nature* **2016**, *530*, 71–76. [CrossRef] [PubMed]
15. Baig, M.M.; Gholamhosseini, H. Smart health monitoring systems: An overview of design and modeling. *J. Med. Syst.* **2013**, *37*, 1–14. [CrossRef] [PubMed]
16. DeFronzo, R.A.; Ferrannini, E.; Zimmet, P.; Alberti, G. *International Textbook of Diabetes Mellitus*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
17. Macdonald, A.; Petrova, N.; Ainarkar, S.; Allen, J.; Plassmann, P.; Whittam, A.; Bevans, J.; Ring, F.; Kluwe, B.; Simpson, R.; et al. Thermal symmetry of healthy feet: A precursor to a thermal study of diabetic feet prior to skin breakdown. *Physiol. Meas.* **2016**, *38*, 33. [CrossRef]
18. Torreblanca González, J.; Gómez-Martín, B.; Hernández Encinas, A.; Martín-Vaquero, J.; Queiruga-Dios, A.; Martínez-Nova, A. The Use of Infrared Thermography to Develop and Assess a Wearable Sock and Monitor Foot Temperature in Diabetic Subjects. *Sensors* **2021**, *21*, 1821. [CrossRef]
19. Venkatasubramanian, K.K.; Banerjee, A.; Gupta, S.K.S. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Trans. Inf. Technol. Biomed.* **2010**, *14*, 60–68. [CrossRef]
20. Jamil, F.; Iqbal, M.A.; Amin, R.; Kim, D. Adaptive thermal-aware routing protocol for wireless body area network. *Electronics* **2019**, *8*, 47. [CrossRef]
21. Bhangwar, A.R.; Ahmed, A.; Khan, U.A.; Saba, T.; Almustafa, K.; Haseeb, K.; Islam, N. WETRP: Weight based energy & temperature aware routing protocol for wireless body sensor networks. *IEEE Access* **2019**, *7*, 87987–87995.
22. Bhanumathi, V.; Sangeetha, C. A guide for the selection of routing protocols in WBAN for healthcare applications. *Hum.-Centric Comput. Inf. Sci.* **2017**, *7*, 1–19. [CrossRef]
23. José Bulllón Pérez, J. Smart System to Monitor Temperature in Diabetic Foot. Ph.D. Thesis, Universidad de Salamanca, Salamanca, Spain, 2015.
24. Al Ameen, M.; Liu, J.; Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *J. Med. Syst.* **2012**, *36*, 93–101. [CrossRef]
25. Siponen, M.T.; Oinas-Kukkonen, H. A review of information security issues and respective research contributions. *ACM Sigmis Database* **2007**, *38*, 60–80. [CrossRef]
26. Dhanda, S.S.; Singh, B.; Jindal, P. Lightweight cryptography: A solution to secure IoT. *Wirel. Pers. Commun.* **2020**, *112*, 1947–1980. [CrossRef]
27. Fotovvat, A.; Rahman, G.M.; Vedaei, S.S.; Wahid, K.A. Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes. *IEEE Internet Things J.* **2020**, *8*, 8279–8290. [CrossRef]
28. Singh, S.; Sharma, P.K.; Moon, S.Y.; Park, J.H. Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *J. Ambient. Intell. Humaniz. Comput.* **2017**, 1–18. [CrossRef]

29. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9–12 October 2017.
30. Jain, A.; Nandakumar, K.; Nagar, A. Biometric Template Security. *EURASIP J. Adv. Signal Process.* **2008**, *2008*, 1–17. [CrossRef]
31. Hernández Álvarez, F. Biometric Authentication for Users through Iris by Using Key Binding and Similarity Preserving Hash Functions. Ph.D. Thesis, Universidad Politécnica de Madrid, Madrid, Spain, 2015.
32. Mills, A.J.; Watson, R.T.; Pitt, L.; Kietzmann, J. Wearing safe: Physical and informational security in the age of the wearable device. *Bus. Horizons* **2016**, *59*, 615–622. [CrossRef]
33. Kim, D.; Park, S.; Choi, K.; Kim, Y. BurnFit: Analyzing and Exploiting Wearable Devices. In Proceedings of the WISA 2015: Information Security Applications, Jeju Island, Korea, 20–22 August 2015; Springer: Cham, Switzerland, 2016; pp. 227–239.
34. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]
35. Clausing, E.; Schiefer, M.; Lösche, U. *Internet of Things Security Evaluation of nine Fitness Trackers Dipl*; Independent IT-Security Institue AV TEST: Magdeburg, Germany, 2015; pp. 1–19.
36. Rieck, J. Attacks on Fitness Trackers Revisited: A Case-Study of Unfit Firmware Security. *arXiv* **2016**, arXiv:1604.03313.
37. Kassem Fawaz, K.H.K.; Shin, K.G. Protecting Privacy of BLE Device Users. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016.
38. Zhang, Q.; Liang, Z. Security analysis of bluetooth low energy based smart wristbands. In Proceedings of the 2017 2nd International Conference on Frontiers of Sensors Technologies (ICFST), Shenzhen, China, 14–16 April 2017; pp. 421–425.
39. Hernández-Álvarez, L.; de Fuentes, J.M.; González-Manzano, L.; Encinas, L.H. SmartCAMPP—Smartphone-based continuous authentication leveraging motion sensors with privacy preservation. *Pattern Recognit. Lett.* **2021**, *147*, 189–196. [CrossRef]
40. Fouad, M.; El-Bendary, N.; Ramadan, R.; Hassanien, A.E. *Wireless Sensor Networks, A Medical Perspective*; CRC Press: Boca Raton, FL, USA, 2013.
41. Hernández-Álvarez, L.; De Fuentes, J.M.; González-Manzano, L.; Hernandez Encinas, L. Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review. *Sensors* **2020**, *21*, 92. [CrossRef]
42. Harbi, Y.; Aliouat, Z.; Refoufi, A.; Harous, S. Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 113292–113314. [CrossRef]
43. Kim, Y.; Lee, W.S.; Raghunathan, A.; Raghunathan, V.; Jha, N. Reliability and security of implantable and wearable medical devices. In *Implantable Biomedical Microsystems*; William Andrew Publishing: Norwich, NY, USA, 2015; pp. 167–199.
44. Arias, O.; Wurm, J.; Hoang, K.; Jin, Y. Privacy and Security in Internet of Things and Wearable Devices. *IEEE Trans. Multi-Scale Comput. Syst.* **2015**, *1*, 99–109. [CrossRef]
45. Ly, K.; Jin, Y. Security Studies on Wereable Fitness Trackers. In Proceedings of the 38th Annual International Conference IEEE Engineering Mediocal Biological Society (EMBC), Orlando, FL, USA, 16–20 August 2016; p. 1.
46. Shim, J.; Lim, K.; Jeong, J.; Cho, S.J.; Park, M.; Han, S. A Case Study on Vulnerability Analysis and Firmware Modification Attack for Wearable Fitness Tracker. *IT Converg. Pract.* **2017**, *2*, 1–24.
47. Classen, J.; Wegemer, D.; Patras, P.; Spink, T.; Hollick, M. Anatomy of a Vulnerable Fitness Tracking System: Dissecting the Fitbit Cloud, App, and Firmware. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 1–24. [CrossRef]
48. Li, C.; Raghunathan, A.; Jha, N.K. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO, USA, 13–15 June 2011; pp. 150–156.
49. Li, C.; Zhang, M.; Raghunathan, A.; Jha, N.K. Attacking and defending a diabetes therapy system. In *Security and Privacy for Implantable Medical Devices*; Springer: New York, NY, USA, 2014.
50. Mahmudur Rahman, B.C.; Banik, M. Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device. *arXiv* **2013**, arXiv:1304.5672.
51. Ching, K.; Mahinderjit Singh, M.M. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 19–30. [CrossRef]
52. Lotfy, K.; Hale, M.L. Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things. In Proceedings of the 2016 IEEE International Conference on Mobile Services (MS), San Francisco, CA, USA, 27 June–2 July 2016.
53. Goyal, R.; Dragoni, N.; Spognardi, A. Mind the Tracker You Wear: A Security Analysis of Wearable Health Trackers. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4–8 April 2016.
54. Cusack, B.; Antony, B.; Ward, G.; Mody, S. Assessment of security vulnerabilities in wearable devices. In Proceedings of the 15th Australian Information Security Management Conference, Edith Cowan University, Perth, Australia, 5–6 December 2017; pp. 42–48.
55. Wood, D.; Apthorpe, N.; Feamster, N. Cleartext Data Transmissions in Consumer IoT Medical Devices. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, TX, USA, 3 November 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 7–12.
56. Aliasgari, M.; Black, M.; Yadav, N. Security Vulnerabilities in Mobile Health Applications. In Proceedings of the 2018 IEEE Conference on Application, Information and Network Security (AINS), Langkawi, Malaysia, 21–22 November 2018; pp. 21–26.

57. Almenárez-Mendoza, F.; Alonso, L.; Marín-López, A.; Cabarcos, P. Assessment of Fitness Tracker Security: A Case of Study. *Proceedings* **2018**, *2*, 1235. [CrossRef]
58. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. *J. Med. Syst.* **2019**, *44*, 1–10. [CrossRef]
59. Newaz, A.I.; Sikder, A.K.; Babun, L.; Uluagac, A.S. HEKA: A Novel Intrusion Detection System for Attacks to Personal Medical Devices. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June–1 July 2020; pp. 1–9.
60. Thamilarasu, G.; Odesile, A.; Hoang, A. An Intrusion Detection System for Internet of Medical Things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
61. Chauhan, J.; Seneviratne, S.; Kaafar, M.A.; Mahanti, A.; Seneviratne, A. Characterization of early smartwatch apps. In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, Australia, 14–18 March 2016; pp. 1–6.
62. Maiti, A.; Jadliwala, M.; He, J.; Bilogrevic, I. (Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks Using Smartwatches. In Proceedings of the 2015 ACM International Symposium on Wearable Computers, Osaka Japan, 7–11 September 2015; pp. 27–30
63. Liu, X.; Zhou, Z.; Diao, W.; Li, Z.; Zhang, K. When Good Becomes Evil: Keystroke Inference with Smartwatch. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015.
64. Wang, C.; Guo, X.; Wang, Y.; Chen, Y.; Liu, B. Friend or Foe? Your Wearable Devices Reveal Your Personal PIN. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 30 May–3 June 2016.
65. Khan, M.N.; Rao, A.; Camtepe, S. Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet Things J.* **2020**, *8*, 4132–4156. [CrossRef]
66. Batista, F.K.; Martin del Rey, A.; Queiruga-Dios, A. A new individual-based model to simulate malware propagation in wireless sensor networks. *Mathematics* **2020**, *8*, 410. [CrossRef]
67. Masad, D.; Kazil, J. MESA: An agent-based modeling framework. In Proceedings of the 14th PYTHON in Science Conference, Austin, TX, USA, 6–12 July 2015; Volume 2015, pp. 53–60.
68. NIST. Lightweight Cryptography. On-Line Publication. 2015. Available online: https://csrc.nist.gov/projects/lightweight-cryptography (accessed on 15 February 2022).
69. Turan, M.S.; McKay, K.A.; Çalik, Ç.; Chang, D.; Bassham, L. *Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process*; NIST Interagency/Internal Rep. (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
70. NIST. Lightweight Cryptography, Finalists. On-Line Publication. 2021. Available online: https://csrc.nist.gov/Projects/lightweight-cryptography/finalists (accessed on 15 February 2022).
71. Turan, M.S.; McKay, K.; Chang, D.; Calik, C.; Bassham, L.; Kang, J.; Kelsey, J. *Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021. [CrossRef]
72. Bovy, E.; Daemen, J.; Mennink, B. Comparison of the Second Round Candidates of the NIST Lightweight Cryptography Competition. Bachelor's Thesis, Radboud University, Nijmegen, The Netherlands, 2020.
73. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access* **2021**, *9*, 28177–28193. [CrossRef]
74. Aagaard, M.D.; Zidaric, N. Asic benchmarking of round 2 candidates in the NIST lightweight cryptography standardization process. *Cryptol. ePrint Arch.* **2021**. Available online: https://eprint.iacr.org/2021/049.pdf (accessed on 15 February 2022).
75. Jadhav, S.P. Towards light weight cryptography schemes for resource constraint devices in IoT. *J. Mob. Multimed.* **2019**, 91–110. [CrossRef]
76. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
77. Díaz, R.D.; Hernández-Álvarez, L.; Encinas, L.H.; Queiruga-Dios, A. Chor-Rivest Knapsack Cryptosystem in a Post-quantum World. In *Advances in Security, Networks, and Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 67–83.
78. NIST. Post-Quantum Cryptography. On-Line Publication. 2016. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed on 15 February 2022).
79. Zhang, P. Permutation-Based Lightweight Authenticated Cipher with Beyond Conventional Security. *Secur. Commun. Netw.* **2021**, *2021*, 1468007. [CrossRef]
80. Hallman, R.; Bryan, J.; Palavicini, G.; Divita, J.; Romero-Mariona, J. IoDDoS-the internet of distributed denial of sevice attacks. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, SCITEPRESS, Porto, Portugal, 24–26 April 2017; pp. 47–58.
81. Marzano, A.; Alexander, D.; Fonseca, O.; Fazzion, E.; Hoepers, C.; Steding-Jessen, K.; Chaves, M.H.; Cunha, Í.; Guedes, D.; Meira, W. The evolution of bashlite and mirai iot botnets. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 00813–00818.
82. Hayajneh, T.; Mohd, B.J.; Imran, M.; Almashaqbeh, G.; Vasilakos, A.V. Secure authentication for remote patient monitoring with wireless medical sensor networks. *Sensors* **2016**, *16*, 424. [CrossRef]

83. Khan, S.; Lee, W.K.; Hwang, S.O. Scalable and efficient hardware architectures for authenticated encryption in IoT applications. *IEEE Internet Things J.* **2021**, *8*, 11260–11275. [CrossRef]
84. Bertoni, G.; Daemen, J.; Peeters, M.; Van Assche, G. Permutation-based encryption, authentication and authenticated encryption. In Proceedings of the Workshop Records of Dir. Authenticated Ciphers (DIAC), Stockholm, Sweden, 5–6 July 2012; pp. 159–170.
85. Bertoni, G.; Daemen, J.; Peeters, M.; Van Assche, G. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Proceedings of the International Workshop on Selected Areas in Cryptography, Toronto, ON, Canada, 11–12 August 2011; pp. 320–337.
86. Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1. 2. CAESAR Competition. On-Line Publication. 2016. Available online: https://competitions.cr.yp.to/round3/asconv12.pdf (accessed on 15 February 2022).