Listen to Your Heart: Evaluation of the Cardiologic Ecosystem

Endres Puschner
Max Planck Institute for Security and Privacy
endres.puschner@mpi-sp.org

Christoph Saatjohann
Münster University of Applied Sciences
christoph.saatjohann@fh-muenster.de

Markus Willing
University of Münster
markus.willing@ukmuenster.de

Christian Dresen
Münster University of Applied Sciences
c.dresen@fh-muenster.de

Julia Köbe
University of Münster
julia.koebe@ukmuenster.de

Benjamin Rath
University of Münster
benjamin.rath@ukmuenster.de

Christof Paar
Max Planck Institute for Security and Privacy
christof.paar@mpi-sp.org

Lars Eckardt
University of Münster
lars.eckardt@ukmuenster.de

Uwe Haverkamp
University of Münster
uwe.haverkamp@ukmuenster.de

Sebastian Schinzel
Münster University of Applied Sciences
schinzel@fh-muenster.de

ABSTRACT

Modern implantable cardiologic devices communicate via radio frequency techniques and nearby gateways to a backend server on the internet. Those implanted devices, gateways, and servers form an ecosystem of proprietary hardware and protocols that process sensitive medical data and is often vital for patients' health.

This paper analyzes the security of this Ecosystem, from technical gateway aspects, via the programmer, to configure the implanted device, up to the processing of personal medical data from large cardiological device producers. Based on a real-world attacker model, we evaluated different devices and found several severe vulnerabilities. Furthermore, we could purchase a fully functional programmer for implantable cardiological devices, allowing us to re-program such devices or even induce electric shocks on untampered implanted devices.

Additionally, we sent several Art. 15 and Art. 20 GDPR inquiries to manufacturers of implantable cardiologic devices, revealing nonconforming processes and a lack of awareness about patients' rights and companies' obligations. This, and the fact that many vulnerabilities are still to be found after many vulnerability disclosures in recent years, present a worrying security state of the whole ecosystem.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; *Hardware reverse engineering*; • **Applied computing → Life and medical sciences**; • **Social and professional topics → Privacy policies**.

KEYWORDS

Hardware Reverse Engineering, Home Monitoring, Telemetry, Implantable Medical Devices, Pacemaker, Implantable Cardioverter-Defibrillator, GDPR

ACM Reference Format:
Endres Puschner, Christoph Saatjohann, Markus Willing, Christian Dresen, Julia Köbe, Benjamin Rath, Christof Paar, Lars Eckardt, Uwe Haverkamp, and Sebastian Schinzel. 2021. Listen to Your Heart: Evaluation of the Cardiologic Ecosystem. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3465481.3465753

1 INTRODUCTION

As cardiovascular diseases continue to dominate much of the industrial world, implantable cardiological devices are indispensable for treating thousands of patients. The aging of western populations, as well as increasing indications for device therapy (e.g. primary prophylaxis of sudden cardiac death with implantable defibrillators (ICD)) will further increase the demand for these therapeutic options in the coming years [10]. With the increasing processing power in miniaturized systems and networking capability [36], these devices are capable of much more than just their enhanced therapeutic function. By tracking one's personal sport activity, they are on the verge of becoming lifestyle products [25] . But with the rise of networking and automation, Implantable medical devicess (IMDs) depend critically on a continuously generated flow of personal data. Consequently, this data is sensitive to manipulation and valuable to the companies as well. On the other hand, resources in hospitals are scarce, and more and more information must be processed and documented by the staff to provide the patient with the best possible therapy in a legally compliant manner. Medical processes are adapted to the use of networked systems, and the human decision-maker must rely on the accuracy of the presented results [14]. This and the known poor security in some of the devices makes the device itself and the ecosystem an attractive target for IT-criminals [1, 2, 21, 30].

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3465753

1.1 Related Work

In 2008, Halperin et al. published the first security analysis about Implantable Cardioverter Defibrillators (ICDs) and their Radio Frequency (RF) interface [13], pushing the academic security community into the direction of IMDs. A comprehensive overview is given in the paper from Rushanan in 2014 [31].

While the academic community is concerned about patient risk, investment companies used the fear factor of attacks against IMDs to speculate on stock courses of manufacturers [20, 26].

The SINTEF Cybersecurity Research Group published three master theses, one analysis of a programmer and two about a Home Monitoring Unit (HMU), both made by Biotronik [5, 18, 19]. During our research, we independently found similar vulnerabilities in the Biotronik HMU. Due to the responsible publication process, the analysis of the HMU was published in 2020, and we were not aware of this research.

Sørum et al. analyzed the practicability of inquiries according to the General Data Protection Regulation (GDPR) Article 15, also called Subject Access Request (SAR), and Article 20 from the user's point of view. The study compared the answers of 15 randomly selected Norwegian companies in terms of response time and quality. It was shown that, even though that the GDPR was put in place in 2018, extensive variations among the answers remain still as default for such inquiries [35].

In July 2020, the European Society of Cardiology published a report about the implications of the GDPR on remote monitoring systems for cardiac implantable electronic devices [28]. Besides recommendations for hospitals and manufacturers, they evaluated the current state of doctors and manufacturers' data privacy awareness and processes.

1.2 Responsible Disclosure

We disclosed all vulnerabilities in this paper to the vendors and intensively discussed potentials concerns of our findings during a six month disclosure period.

2 BACKGROUND

The concept of electric stimulation of human muscle tissue began over 200 years ago. In the late 1700s, Luigi Galvani realized that he could stimulate a frog's heart by passing an electrical current [11]. In the early 1950s, the concept of a non-implantable pacemaker arose in the US. It was developed further into the first wearable, battery-powered pacemaker by Earl Bakken in 1957. Further development chose to solve the problem of delivering electrical energy over a long time by integrating a radionuclide battery into the pacemaker. With the progression of more powerful and smaller battery components, pacemakers were able to treat symptomatic bradycardia arrhythmias for years before their power cell had to be changed. Parallel to this development, the first ICDs were applied to control cardiac arrhythmia and prevent sudden cardiac death with specific electric interaction. Today, the carrier of ICD and pacemaker devices often uses additional telemetric devices to connect their device with the manufacturer and the physicians in the hospital.

2.1 Implantable Cardiological Devices

In Germany, about 25K pacemaker, ICD, and monitor devices are newly implanted every year by 763 different hospitals (2017). Nearly 20k surgical interventions are done for device revisions or explantations [22]. The major difference between a pacemaker and an ICD is the ICD's ability to terminate life-threatening tachyarrhythmias by stimulation maneuvers or defibrillation. Therefore, the battery of an ICD device has to be more powerful than in a pacemaker device. Also, the electrode compartment has to be more robust to withstand the shock. Another category of ICD is formed by implantable monitor devices that log any relevant data related to heart diseases. These devices are often recommended to confirm or exclude a tentative diagnosis.

The major producers of ICDs are Abbott Laboratories – formerly St. Jude Medical –, Boston Scientific Corp., Biotronik SE & Co. KG, Medtronic PLC, and LivaNova PLC – formerly Sorin Group.

Programming implantable devices. After the implantation and during the complete lifetime, these devices are regularly checked and programmed via a vendor-proprietary RF interface. The communication is done via a dedicated computer provided by the vendor of the implanted device. With this vendor-specific programmer, the logged data is retrieved from the implanted device, and new configuration like thresholds for an automatic shock or triggers for typical logging operation is set. There is no common communication standard established for the programmers, but every vendor uses proprietary protocols and hardware.

Remote monitoring. Starting around the early 2000s, the first vendors introduced a remote monitoring system that collects logged data from the implanted device and forwards it to the manufacturer's backend server [27]. The treating physicians of the patient can directly examine recorded device information and heart-related medical data via a web service. Depending on the manufacturer, alarm messages or color-coding for specific or dangerous values can be configured [3].

Typical recorded information includes irregular heart rhythm, device activities like impulses or shocks, Electrocardiograms (ECGs), and technical information about the reliability of the leads and the device, such as the remaining battery power. Depending on the vendor, this data can also be used – normally in an anonymized form – for statistics and research studies to improve their products.

The newest ICDs, monitors, and pacemakers communicate via Bluetooth with the patients' smartphone directly and allow them to track vital data like the daily activity level, measured by the implanted device [6, 25].

An overview of the patients' data flow between the hospital, the manufacturer, and the patient itself is described in Fig. 1. The patient's pacemaker, ICD, or the implanted monitor generates data that includes the applied electric power, the patient's personal data, and the remaining battery capacity. This data is sent via a proprietary radio protocol to a Home Monitoring Unit (HMU). This station pushes the data via a mobile or a landline phone network to a web service hosted by the device manufacturer, which the physicians also use via a web log-in. The physicians can access the patient's cardiac device via RF communication with the proprietary

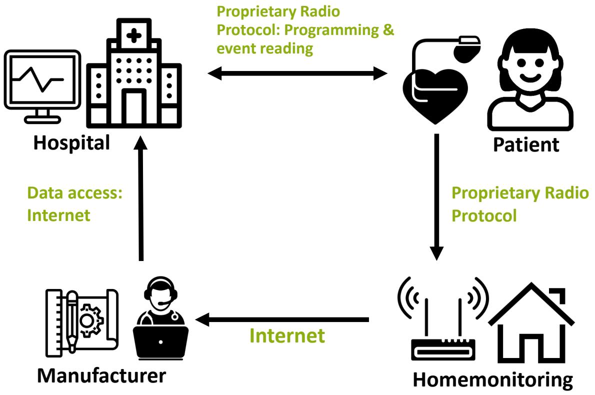
Proprietary Radio Protocol: Programming & event reading
Hospital
Patient
Data access: Internet
Proprietary Radio Protocol
Internet
Manufacturer
Homemonitoring

Figure 1: Data flow of patients' data between the hospital, manufacturer, and the patient.

programmer device directly. For this purpose, the programmer has to be in immediate proximity to the implanted device.

2.2 Technical Analysis

We used a broad set of different analysis techniques for this research. The most important ones are explained in the following.

Home Monitoring connection via GSM. Modern HMUs use mobile cell phone networks to communicate with the backend server. While all currently available cell phone technologies use encryption algorithms to secure over-the-air communication, the security of the used protocols and algorithms are rather different. Where Universal Mobile Telecommunications System (UMTS) and newer standards require mutual authentication, the authentication for Global System for Mobile Communications (GSM) and GPRS is done on the base station side only. Consequently, the mobile device cannot differentiate between a base station of a valid GSM provider and a rogue station operated by an attacker.

In case of the absence of UMTS or LTE networks, conventional mobile devices will automatically downgrade the connection and connect to GSM networks. The attacker can enforce such an environment by jamming frequencies used by the regular UMTS and LTE networks, or by isolating the device in a shielded Faraday cage while providing a GSM network with a high signal-to-noise ratio [8].

With this attack, a classic Man-in-the-Middle scenario is achieved where the attacker, if no further security mechanism on the backend is deployed, can listen to the communication between the device and backend or even manipulate or send new messages to both parties.

Embedded Device Reversing. Even before the age of the internet, researchers and hackers opened and reverse engineered all kinds of devices, like game consoles or video recorders, to improve functions or circumvent security mechanisms [15]. Common reversing techniques are bus probing, bus sniffing, or memory dumping. Buses, e.g. JTAG or UART, can often be identified and data sniffed with standard reversing hardware like the *Bus Pirate*. After finding the correct pins on the circuit board, it is possible to sniff data between two components during run time or to actively communicate with the microprocessor on the board. Memory dumping is often possible using such a JTAG bus if present. If not, direct communication with EEPROM or FLASH memory is feasible for many devices.

Radio Frequency Analysis. Medical implants such as ICDs or pacemakers often rely on RF communication for programming physiological parameters, as well as fetching logged events or statistics. For this, a connection that only works in the near surroundings of the patient is desired to protect against malicious attackers and unintentional re-programming. An inductive RF head is used to couple the implant with a programming device or a HMU, similar to Radio Frequency Identification (RFID) applications. Halperin et al. showed in 2008 [13] that it is easily possible to analyze such low-frequency RF communications.

Observing more modern implants, the communication at initialization is then switched to a far-field RF communication mode, where a greater transmission range can be achieved. This behaviour is referred to as Medical Implant Communication Service (MICS) [9] or MedRadio. But these standards only specify the used radio band, however gives neither information about used communication protocols nor the security of the transmitted data. The actual transmission protocols are developed by the medical device manufacturers and thus kept as proprietary protocols.

The trend is going to implants connected via Bluetooth Low Energy (BLE) [6]. However, even in the Bluetooth standards, no communication profile or recommendation specifically designed for ICDs and pacemakers can be found.

2.3 Processing of Patients' Personal Data

The EU GDPR [7], put in force in 2018, introduced a large set of rights to control one's personal data and regulate it's processing. Article 15, *Right of access by the data subject*, introduces the right to obtain information about the processing of one's own personal data. This information includes, but is limited to:

- The purpose of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular, recipients in third countries or international organizations

Such Subject Access Requests (SARs) must be answered immediately, but at least within one month. In complex cases, it is possible to extend the answer for two months, but the inquirer must be informed about the delay and it's reason.

Article 20, *Right to data portability*, gives a person the right to retrieve data concerning themselves, which was provided beforehand, in a machine-readable format.

In chapter 4, the GDPR introduces the roles of the data controller and the data processor. The first determines the purposes for which and how personal data is processed. The data processor processes personal data on behalf of the controller and is bound by controller's instructions. The directives in which way the data is processed and the processor's duties must be specified in a contractual agreement, the so-called Data Processing Agreement (DPA).

3 METHODOLOGY

We structured the analysis as follows: First, we looked at the related literature and published technical analyses of recent years. Furthermore, an extensive market survey was produced and reviewed. The market analysis aimed to estimate the distribution of the individual products and the impact of vulnerabilities therein. We then continued with a mixed-methods analysis concept.

3.1 Selection of Devices

Our research group cooperates with the Department of Cardiology and Angiology of the University Hospital Münster (UKM). With the informed consent of the patients, they provided us several explanted pacemakers, ICDs, and the related home-monitoring stations. We chose the devices that were not yet analyzed in the academic literature.

3.2 Attack Model

Rushanan et al. provided a generic attacker model for IMDs in their paper in 2014 [31]. We adapted this generic approach towards a specified one based on the actual processes used in the hospital and from the patient. This resulted in a structure in which the following parameters evaluate the potential attacker:

- Level of technical knowledge
- Possibility of data manipulation
- Expertise on the specific medical and technical processes

We complemented the evaluation result with a valuation and rating from the physicians of the UKM to obtain the following real-world scenario of an attacker. Our three scenarios were rated as follows:

(1) Attackers have access to an ICD programmer device. A programmer can be used to harm patients easily, and the attackers do not need special knowledge for this but need to be in direct proximity to the victim. This scenario changes when the implant is already paired with the programmer (over near-field radio), and parameter changes can be achieved via the far-field radio interface. This communication spans in the range of around ten meters. When the attackers have access to special cardiological knowledge, they can perform several types of covert attacks to effectively disable the implant (e.g.: Usage of the programmer test mode to induce ventricular fibrillation or the change of stimulus thresholds).

(2) A modified programmer with access to the underlying hardware and operating system can be used to harm patients more effectively and with a greater coverage because the attackers do not have to be in direct proximity to the patients. This requires more attacker capabilities compared to (1) as the attackers need to demonstrate significantly more technical expertise.

(3) A modified home monitoring unit with access to the underlying hardware and operating system can be used to harm patients indirectly by manipulating the transmitted data. This could lead to the wrong medication of the patient on the based on the tampered data. As in scenario (2), this scenario requires significant technical expertise compared to scenario (1).

Our assessment concludes that passive attackers are not relevant in a scenario where a patient should be physically harmed by the adversary. The attacker would only be able to listen to the transmitted data with a potential privacy violation, but not with a direct physical injury.

3.3 Technical Analysis

We obtained several accessory devices for implantable electronic cardiac devices, namely HMUs from different vendors and one portable pacemaker programmer. For the technical analysis, we opened the devices and searched for possible attack vectors like debug pins, bus lines, or memory Integrated Circuits (ICs). We retrieved the firmware from the main microprocessor on the device and analyzed it with a focus on security-relevant functionalities.

Besides hardware reversing, we mounted a communication analysis on the devices. Our focus during the analysis was to find non-invasive attacks in which attackers do not need to open up the device casing and only access external connectors or radio communication. We analyzed the traffic between the monitoring unit and the backend server with a fake GSM base station as a Man-in-the-Middle. We also analyzed how an adversary can gain information about the communication between the programmer and the pacemaker. Furthermore, we analyzed how the external ports, namely the Universal Serial Bus (USB) port, are secured against intruders.

After we found the backend server's URLs through reverse engineering and communication analysis, we analyzed the server for open ports with reachable services and their presented TLS certificates. As we are dealing with production servers for life-saving devices, we did not use invasive or potentially harmful analysis techniques.

3.4 Analysis of Patients' Data Processing

Parallel to the technical analysis, we contacted patients who have electronic cardiac devices implanted and asked them to request their personal data from the associated company. We provided SAR forms according to the GDPR, Article 15 and 20, and guided the patients through the process. With the requests based on these two articles, the vendor must inform the patient about the scope of data processing of personal data and a machine-readable copy of data that is provided by themselves. This includes retrieved data from the implanted device, gathered by the remote monitoring system.

Our initial plan was to find one cooperative patient for each of the five major producers of pacemakers and ICDs. After the beginning of the COVID-19 pandemic, several hygiene measures were introduced at our partner hospital, which limited our sample of participants.

4 EVALUATION OF HOME MONITORING

As part of our research project, we analyzed the HMUs, which retrieve medical data from the implantable device and forward it to the manufacturer's backend server.

4.1 Biotronik

We analyzed the HMU CardioMessenger II-S from Biotronik. This unit communicates with the implanted device via an RF connection and retrieves the collected medical data such as device activities or technical device information. The CardioMessenger initiates a connection to the backend server over the GSM cellular network and forwards the obtained data. After registration to the Biotronik Home Monitoring system and the specific HMU, the physician can see any information previously transmitted to the backend server.

Home Monitoring Unit. Firstly, we eavesdropped on the GSM communication between the device and the Biotronik backend server. We found that the device communicates with the IP address 172.16.14.1, which belongs to a private network that is not reachable from the public internet. Such configuration is typically done for cellular connections of Internet of Things (IoT) devices and is a protection layer against attacks on the backend system of a vendor. Usually, such network separation is done via a specific Access Point Name (APN) that requires dedicated credentials for the GSM-connected device.

Our analysis showed that the initial communication is done via a Text-based protocol. This first packet contains human-readable text in a standard user-password format (see Listing 1) and is sent from the HMU to the backend server on port 2323. Further packets sent to the backend server contain not human-readable binary payloads.

Listing 1: Text-based protocol message with credentials sent by the Biotronik SmartMessenger II-S.

```
<serial number>@cm3-homemonitoring.de
    jw6oD4GPL6
```

The next step was to apply classic hardware reversing techniques. We could successfully identify debug ports on the Printed Circuit Board (PCB) as JTAG connectors. We did this by tracing the debug connectors to the microcontroller's pins via a multimeter and comparing them with the chip datasheet. The results can be seen in Figure 2.

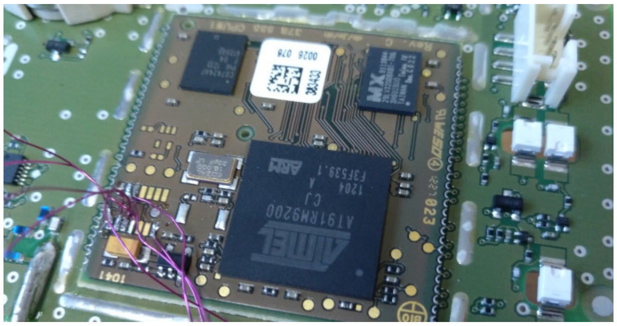

Figure 2: Soldered Connections to the JTAG port of the Biotronik HMU

With the JTAG connection, we revealed the firmware of the controller, and analyzed it with *Ghidra*. Besides the plaintext credentials that were sent via the GSM connection, we found APN settings and the AES CBC encryption routine, which we assume is used by the device to encrypt data sent after the plaintext credentials.

We identified the UART bus pins of the GSM modem by checking the manual of the Motorola G24 modem. By sniffing on the UART line, we successfully identified the PIN number used to unlock the Subscriber Identity Module (SIM) Card connected to the modem.

At this point, we adapted our research for this HMU, because SINTEF published their analysis results about the same device [5, 19], which was done in parallel and independent from us. A careful evaluation of these master theses shows that their results are in line with our observations, as they found the same attack vectors and results as we did.

Backend. The backend server is only reachable via the internal GSM network. Since the login data reveals the domain *cm3-homemonitoring.de*, we suspected that the backend server can also be reached via internet on this domain. According to public information, the server is hosted by provider IONOS. A scan revealed the open ports 22, 80, 443, and 9391, and 9392. The HTTP ports 80 and 443 showed an Apache 2 Test page, whereby the TLS connection could not be validated because of a missing issuer certificate. The certificate's common name contains the term `(Test)`, revealing that this certificate was certainly not meant to be used for a production system. The email address and organization field assured us that the owner of this domain is Biotronik. The port 9391 and 9392 present an internal self-signed TLS certificate with the common name incinga-3.hss.int. Via the latter port, we could open the login interface of a Greenbone Security Assistant instance. After the publication of the analysis from SINTEF, the domain does not lead to this server anymore. Nevertheless, the IP address (87.106.132.29) and the reverse DNS names (s15254823.onlinehome-server.info, s205072904.online.de) were still reachable. Also, the port scan shows the same results as before. Therefore we assume that the domain name was unregistered, but the server is still reachable.

Outcome and Disclosure. At the time of our disclosure process, the found device vulnerabilities were already known from the SINTEF coordinated disclosure that resulted in the Cybersecurity & Infrastructure Security Agency (CISA) ICS Medical Advisory ICSMA-20-170-05.

Biotronik initially claimed that the still accessible backend server was setup by IONOS and was never used by Biotronik. After we provided a more detailed report of our server scan results, Biotronik stated that the server was actually used to monitor the Biotronik infrastructure from the public reachable internet. Finally, the IP address and the reverse DNS names are not reachable anymore.

4.2 Medtronic

Similar to the HMU analysis of a Biotronik device, we analyzed an HMU from Medtronic. The HMU model is MyCareLink 24950. Its features are very similar to the Biotronik CardioMessenger II-S. We focused our work more on the device during analysis than the communication with the server backend due to the absence of a Medtronic registered SIM card.

Home Unit. To understand how the HMU communicates with implants and how data is processed and sent to the server, we first needed to find out the device's basic functions. However, the device we got could not communicate with the server backend as the included Vodafone SIM card was disabled. We assume that is automatically done once the HMU is de-registered from the remote monitoring system.

Similar to the approach in Section 4.1, we identified a pin header, depicted in Figure 3, with a UART serial interface, operating at 1.8 V.

Connecting a serial adapter revealed that a Linux-based operating system ran on this HMU and provided us with a login shell.

The file system of the HMU is stored on an internal Micro Secure Digital (SD) card and thus could also be dumped using a conventional SD card reader. The internal SD card slot is shown in Figure 3. Examining the contents, unencrypted boot, and root partitions could be found besides two encrypted partitions: "app" and "data". Replacing the `/bin/mount` program with a shell script and running the original mount program afterward, one can extract the keyphrases for the encrypted partitions. This was previously found out by James Stanley and published in his weblog[1]. Actually, the used encryption keys are stored in an EEPROM IC on the PCB of the device and read out over an I^2C bus during boot time. Consequently, they could also be extracted there.

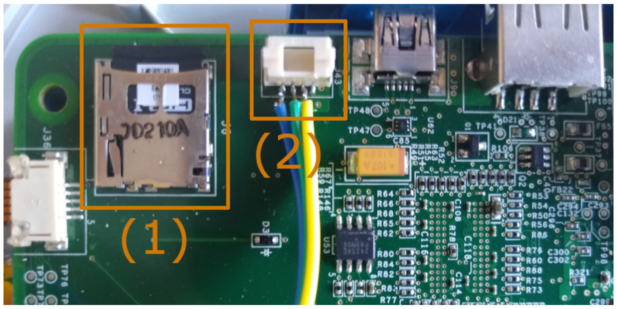

Figure 3: Micro SD card slot (1) and UART header (2) of the Medtronic HMU with soldered cables

Also, we could get root access by merely adding another user with user ID zero to the `/etc/passwd` file. Using this root access, we could influence any behavior of the device. We could also override the device's display content using DBUS access or modify data on the file system during run time. There already was a privileged user "medtronic" without any password with which basic information could be retrieved directly over the UART interface.

During a firmware analysis, we found out that the HMU contacts several HTTPS websites, posts some data that seems to be configuration data, and acknowledges information to the server.

Backend. As we contacted the found websites from the firmware analysis, we found an HTTP authentication prompt and an untrusted TLS connection due to the self-signed Medtronic CA certificate. By trying out some strings from the EEPROM, which looked like user and password combinations, we found the correct credentials with a 16 character password that consists of lower and capital letters plus numbers. The analysis of a second device showed that these credentials are device-specific.

We tried to send data via two forms for non-critical configuration parameters, but the submitted data did not show up in the Medtronic web interface.

Outcome and Disclosure. The access to the memory and filesystem, and the possible connection to the UART and I^2C bus was already known by two non-public reports which resulted in the CISA ICS Advisory ICSMA-18-179-01. The access to the backend server will be restricted by further mechanisms that are not finally decided at the time of writing.

5 EVALUATION OF PROGRAMMER

To analyze a programming computer for ICDs, we needed to acquire a device used inside cardiological clinics. Often, hospitals and clinics do not purchase but rent these devices from manufacturers. Implant programmers are not officially purchasable for individuals, as that might face the risk of misuse. However, in an online shop for second-hand medical devices, we bought a used Boston Scientific (BSC) 3120 programming computer for under 3000 USD.

We sought a model that is still used in hospitals, as, for instance, it is at the UKM. It turned out that it consists of fairly old technology. The programmer was designed in 2004 [12], and the software version is from late 2011. Interestingly, it still supports current implant models at the time of this writing. Even after more than nine years, the same software of the device can be used to program the majority of ICDs of the same manufacturer. An explanation for the long cycle of hospital hardware might be that manufacturers are practically bound to develop and plan technology for multiple decades. The reason for this is the high cost of developing critical health devices and their regulations and required certifications globally.

5.1 Functional Analysis

Analyzing the device's case, it turns out that the external interfaces are USB, IEEE 1284-A, VGA, IrDA, RF antenna, near-field RF, floppy disk, and medical extension ports such as ECG measurement probes, analog output, and stimulator input. In contrast to many medical devices that face security issues [34], it is not intended to connect the device to a hospital network, and thus it is not equipped with an Ethernet port.

The device turned out to be fully functional and compatible with all our explanted pacemakers and ICD devices of Boston Scientific. However, first, there was a discrepancy between the set RF region and some of our implants, which could be resolved after the procedure described later in Section 5.2. Thus, we could read out any implant that is supported by the programmer and could even change their configuration as well as run tests like inducing shocks or disable the implant's therapy features. This poses a threat to the implantable devices and their carriers that should not be underestimated.

5.2 Invasive Analysis

To understand the internal device's functionality and to give us ideas about attack vectors for adversaries, we used invasive Reverse Engineering techniques. However, the results can be used to mount more powerful non-invasive attacks.

Determining System Architecture. To find out which system hardware architecture our device has, we looked at the device's internals. We opened up the device, and the inner of the case revealed a custom stripped-down Intel Celeron x86 PC mainboard with soldered RAM and an attached 2.5 inch IDE Hard Disk Drive (HDD). Furthermore, a second attached PCB exists and is connected to the mainboard via an edge connector. It contains two Digital Signal Processor (DSP) chips and a Field Programmable Gate Array (FPGA).

[1] https://incoherency.co.uk/blog/stories/medtronic-mycarelink.html

As we feared data loss, the first step was to back up the HDD with an external adapter designed to connect standard IDE hard disks via USB. This, allowed us to sneak into the stored data revealing, amongst others, a Linux file system. Also, we could easily change files on the HDD and re-install the manipulated disk in the device to change any behavior in the software. The Linux Kernel version is 2.4.18, released in February 2002. Larger userland applications guessed to be the main user interface "mau" and the medical application "app_FrontierFalcon" were compiled with an ahead of time compiler for Java. Ahead of time compiling is a concept to make reverse engineering more difficult by compiling the Java bytecode into a static executable containing obfuscated machine code. The original source code of not preprocessed Java bytecode instead could be easily reconstructed [29].

Gaining Root Access. If the password for the root user of the Linux system would be required, we were able to extract the salted MD5 hash value of this password in the md5crypt format. Using *hashcat* in a brute force mode with two Tesla K80s graphic cards, we cracked the correct password in less than 5 minutes. Thus, the password was effectively chosen too short and was obviously not created by random[2].

However, it turned out that the root password was not required as all applications are run by the root user. We found out that we can replace the "FrontierFalcon" app with a shell script that launches the preinstalled tiling window manager "twm" beforehand to break out of the usual kiosk mode styled user interface whenever the medical application was started from the main menu. From this window manager, we were able to run the terminal emulator "xterm", which presents a shell terminal to us on display.

Input can then be given through an externally connected USB keyboard. By this approach, an invasive attacker has the ability to analyze the device statically as well as dynamically making use of the now available root shell. Furthermore, it would be possible to read out, alter, or inject persistent data such as health data or to install malicious software.

Hardware Dongle. After analysis of scripts and binaries on the HDD, we found a utility that detects the presence of a hardware dongle. Also known as hard lock or hardware key, these dedicated hardware elements enable access to a certain application or to specific software features [16]. In this case, Ghidra could decompile the program "checkDongle", and we deduced the function of the hardware dongle. The dongle must be present in the IEEE 1284-A port and consists of only static wiring with no logic elements inside[2].

Using a recreated dongle, we were able to enter the BIOS setup of the programmer by pressing the F2 key on an attached USB keyboard during boot. If not entering the BIOS set-up, the programmer tries to boot from a floppy disk or attached USB device instead of the normal system. This can be seen as an attack entry point, as the attacker could plug in a dongle and a boot medium in an unnoticed moment and thus gain full access to the whole system automatically.

Region Lock. The programming computer also features a region setting that limits the functionality to be compatible only with implants used in a certain region. In practice, there are two valid regions only depending on the used Industrial, Scientific and Medical (ISM) radio frequency bands. They are 869 MHz in the United States and the band between 902 and 928 MHz in the rest of the world. A deeper analysis of the files on the HDD revealed a single configuration option that could be set to either "SrdBand", "IsmBand", or to a third value effectively disabling long-range RF. Changing this value followed by a renewal of the file integrity checksum with an MD5 hash, the programmer is effectively changed to connect with the implants of the now set radio region.

Alternatively, this can be reached with a hardware dongle present on the IEEE 1284-A port instead. In this case, the option dialog provides the telemetry region as an additional setting. We figured this out by using the previously built hardware dongle.

5.3 Possible Non-Invasive Attacks

Our main focus is on non-invasive or attacks with the least physical impact on the device. This allows us to select an attacker model where only a little interaction with the actual device is required. For instance, one requirement could be for the attacker to be in the nearer surroundings to mount RF attacks within the respective communication range or to plug in a USB flash drive in an unnoticed situation or through social engineering.

Software Upgrade Feature. During the analysis of the software stored on the HDD, we found a software module called the Installation Utility (IU). Further analysis showed that it actually is a Linux operating system specifically for upgrading software modules or the whole specialized operating system on the HDD. Reading through the script file run after the start of the IU revealed that once triggered with the correct conditions, it scans a plugged-in USB mass storage device for files ending with ".bin" in the root directory and executes the most recent of these files as root user giving full read and write access to all peripherals such as the HDD. Notably, we did not find any cryptographic authenticity or integrity checks like signatures executed on the binary update file. Thus, a potential attacker can install malicious software with a prepared USB flash drive and the knowledge of how to trigger the IU.

Stored Treatment Data. The programmer has the option to store implant configurations and logging history in combination with the personal data of the implant's wearer on either a floppy disk, a USB flash drive, or on the internal HDD. This data is not cryptographically protected. So an attacker, given root access on the device, can access the data from either storage medium. This could lead to manipulated implant configurations, respectively, wrong treatment, and thus potentially dangerous situations for the patient. Also, medical information of the patient can be extracted by the attacker. This does not lead to direct physical harmful attack vectors but must be handled as critical privacy issues with potential non-physical damage to the patient.

Inducing Known Exploits. The software version of various Open Source software parts is more than 19 years old. Thus, there is a huge potential that known security vulnerabilities collected in the

[2] We agreed with the manufacturer to not publish specific hashes, passwords and schematics.

Common Vulnerabilities and Exposures (CVE)[3] list can be used to exploit the programmer over various external interfaces. Especially USB has gone through extensive development back at this time. Allowing to plug in USB devices could lead to security risks.

5.4 Outcome and Disclosure

The analyzed programmer will not be updated, but at the time of this research it is in the process of getting replaced with the newer BSC 3300 model. At the time of writing, BSC is planning to work with the CISA to disclose these vulnerabilities.

6 DATA PROCESSING

To analyze the data processing of patients' personal data, we sent Subject Access Requests (SARs) in the name of a collaborating patient to the vendors and hospitals and evaluated the answers.

6.1 Biotronik

Inquiry to the Vendor. For sending the SAR, we picked the contact address, *BIOTRONIK Vertriebs GmbH & Co KG*, from a Biotronik privacy policy document that states that personal patient data is stored to invoice the costs of the implantable device directly with the health insurance company. In response, at the end of the period of one month, Biotronik explained that this company does not store or process personal patient data. However, if Home Monitoring Services are used, a different legal Biotronik entity might process such data by order of the hospital. Biotronik stated that, in general, the hospital or the physician respectively has the role of the data controller, and we should contact our hospital or doctors directly.

Our second inquiry was sent to the BIOTRONIK SE & CO KG, which has the same postal address as the contacted Biotronik Vertriebs GmbH, responsible for the Home Monitoring Services. The answer arrived two months after our request, one month later as allowed by the GDPR, justified by internal postal delivery issues due to the COVID-19 pandemic. We were informed that the implantable device was not connected to the Home Monitoring System, and therefore no personal patient data is stored or processed. After a consultation with the patient, we assessed this information as valid since the patient has confirmed that no HMU was provided by the hospital.

Inquiry to the Hospital. Since Biotronik forwarded us to the hospital, we sent the inquiry to the clinic where the Bio-Monitor was implanted in 2015. The response was in time but claimed that we ask only for the data regarding the time of the implantation and that due to insolvency and an ownership change in 2016, the new current hospital operator is not responsible for this inquiry, and we should contact the previous operator. Notably, the responsible contact at the former liquidated operator company is also listed as a contact person for the administration of the current hospital company, which we already contacted.

We sent the SAR to the mentioned former operator company that answered after one and a half months, exceeding the one-month time limit set by the GDPR. The answer contains a copy of an analog implantation card with the indication and date of the implantation and a printout of the configuration of the BioMonitor.

Since every surgery in a German clinic must be documented and the records must be archived for at least ten years, we can conclude that our request is not fully answered. At this point, we stopped the request and disclosed our study during a personal meeting with the legal and data privacy department of the hospital.

6.2 Boston Scientific

After our initial inquiry to Boston Scientific (BSC), our patient was asked to verify his identity by a copy of his ID card or by using an online form for the SAR.

After sending the copy of the ID card via email, our patient received the answer at the end of the one-month time period of our initial request via an unencrypted email. According to Art. 9 (GDPR), medical data is categorized as data with a special need for protection. In general, emails are not encrypted by default and do not fulfill the privacy standards if no additional safeguard like End-to-End encryption is used. Additionally, the German *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder* (Conference of the Independent Federal Data-privacy Agencies) stated that emails with a *high risk to the right and freedoms of the data subject* must be secured with End-to-End encryption [17]. We conclude, sending such medical data via plaintext emails does not conform to the GDPR.

The answer stated that the personal data is *generally* stored on US servers, which conforms to GDPR by an active certification for the *Privacy Shield* [4] For the Article 20 inquiry, we received seven ECG reports as PDF files.

After informing the patient, we sent a follow-up request with the following claims (C) and the corresponding responses (R) from BSC:

C: A concretization of the countries where personal data is stored and processed besides the statement about the *general storage*.
R: The personal data is stored on servers in the USA.
C: A confirmation that Boston Scientific stores only the provided seven ECG reports.
R: Except for the provided seven reports, no personal data is stored by BSC.
C: BSC shall provide the stored data, especially the ECG reports, in a machine-readable format as defined in Article 20.
R: The PDF files should be classified as a machine-readable file format.

The treating physicians validated the statement of the stored reports by accessing the patient's file via the web interface of the home monitoring system. They acknowledged that more than seven reports are available for the patient, and the remote monitoring system is active.

With this information and the statement of the European Commission that PDF files are not sufficient to exercise the right of data portability according to Article 20 [5], we sent a third inquiry to BSC. BSC answered this request along with an apology, for the incomplete answer and confirmed the presence of further data in the

[3] https://cve.mitre.org/

[4] At the time of the investigation, the Privacy Shield framework negotiated between the European and the United States was valid but later declared invalid by the European Court of Justice.

[5] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_en

LATITUDE NXT home monitoring system. The email's attachment contained all PDF reports from the web interface and the last three reports as IDCO formatted HL7 messages [4]. With reference to Article 12 of the GDPR, BSC reserved the right to extend the period for two months and ensured that they would provide all the reports in a machine-readable format.

Within the extended time limit, BSC provided the remaining IDCO formatted reports from the Home Monitoring system and an Excel sheet, which contains further personal data such as ECG raw data and patient's contact information from the BSC internal database. Notably, this data was not sent via a plaintext email, instead our patient had to use the BSC privacy management platform, where she could download the files via a secure TLS connection. Notably, instead of sending the data via plaintext email, our patient had to use the BSC privacy management platform, where she could download the files via a secure TLS connection.

To summarize, we needed four letters, the help of the treating physician, and had to wait several months to get the requested information the patient was asking for.

Comparison with public information. We compared the provided information with the consent form that is provided to the patients in the UKM[6] and with the answers that BSC gave to the questionnaire of the European Society of Cardiology [28]:

• Whereby BSC informs us in the initial answer that the personal data is stored in the USA, the consent form explains that the patient's data is stored in Ireland with a back-up in the USA, which is the same answer as given in [28]. In a later answer, they confirm the storage system explained in the consent form. According to our short analysis with public whois and geographical databases, at least the web interface of BSC is hosted in Ireland.

• In the third answer, BSC stated that they are a data processor, whereby the hospital is the data controller. This statement is in contrast to the consent form and to [28]. In both, BSC states that they are, besides the hospital, also a data controller, which would result in a joint controllership constellation (Article 26 [7]).

During the disclosure process, BSC clarified that they are typically in the role of a processor in situations where a BSC device is implanted by a hospital without any post-operational support by BSC (e.g. Home Monitoring) while they are in the role of a controller, as is the hospital, for any remote monitoring of the device.

6.3 Medtronic

Comparable with the BSC process, our patient was asked to send a copy of her identification Card, either via the Medtronic email portal or via a registered letter. We created an account for the email portal and sent the copy to the named address. Notable, the sent email was not visible in the `Sent` folder. The answer, and all following emails from Medtronic, were sent via standard plaintext emails and not via the TLS secured portal. Even if no medical data was sent from Medtronic, it is questionable why the email portal is not used in further communication.

Medtronic asked for additional information, which should be given in a Microsoft Word (.doc) file. After answering the relevant data, the serial number of the device, and that we aim for the data from the Carelink Home Monitoring system, Medtronic stated that we should send our request to the hospital that is the data controller whereby Medtronic is the data processor and cannot give us the requested information.

7 CONCLUSION

The discovered results and the available technical literature draw a critical picture of an industry that is beginning to deal with the new challenges of digital implantation medicine. We discovered several severe vulnerabilities within the cardiologic ecosystem of the analyzed manufacturers that could harm a patient by manipulating the data that serve as the basis for the therapy.

The analysis showed, in some cases, a base layer of security measures taken but, in other cases, a fundamental lack of security. It is critical that we were able to get our hands so easily on a functional programming device. Due to the outdated but still usable software version, there are various attack scenarios, and the attack threshold is lowered. This would enable attackers in close proximity to the victim to perform various attacks to harm the patients by altering their data or pacemaker parameters. In some cases, the clinical decision-making process does not provide double-check mechanisms, so that erroneous data directly leads to critical medical decisions like medications. We consider the attack vectors via a purchased programmer device as important because of little necessary knowledge and the possibility of good attack coverage here.

An attack with a modified home monitor unit requires more technical expertise and close proximity to the patients. Therefore, we consider this attack unlikely. However, a large-scale attack would be possible under certain circumstances via this vector.

The data processing analysis showed a critical state for GDPR inquiry processes. In all cases, we could not get a correct and complete statement of the data storage and processing in time. This matches the results of Sørum and Presthus [35].

7.1 Countermeasures

We propose the following steps to improve this state. At first, medical professionals should be included in the development process to avoid failures due to techniques and processes that are incompatible with daily clinic routines. Further, the implementation of official guidelines and recommendations (e.g. [23, 24]) would significantly improve security status. These measures proved to be effective in other industries to help the manufacturers apply security by design. One well-known security policy model for wireless network devices was proposed in 1999 by F. Stajano and R. Anderson [32] as a secure key exchange method for small devices communicating over a short range. Also, obvious attacks would not be possible on the programmer anymore. Lastly, a good product cycle, including maintenance and regular software updates, is fundamental for establishing security. Also, more open standards can be used to overall optimize the whole product. In the best case, only professionals are allowed to modify any configuration of an IMD to maximize the safety for the wearer minimizing the risk of a security issue. One way to approach this criterion could be implementing a Public Key Infrastructure (PKI) that authenticates any requested access through a multi-factor authentication protocol with the requesting

[6] Patient Data Authorization, 2018-07-09

individual. However, it is an open problem of ensuring that a patient can be treated anywhere when well-established key exchange methods like over the internet are not available everywhere.

Implementation-wise, every implant would need its own cryptographic key or key pair, which can be used to communicate sensitive data and program configurations. There are ideas of using encrypted bio-material like iris patterns for generating keys [33]. If this is not given, the weakest link in the chain remains the programming device that could still be attacked. Summarizing our results, we discovered several findings that reflect a worrying image of the implantable device ecosystem. Physicians depend on secure cardiological technology to value the patient's trust in treating them in the best possible way and working under the premise of their Hippocratic oath.

ACKNOWLEDGMENTS

The authors would like to thank the patients who sent and received inquiries to their corresponding medical device manufacturer.

This work was supported in part by DFG Excellence Strategy grant 39078197 (EXC2092, CASA), through ERC grant 695022 and NSF grant CNS-1563829, the research project "MITSicherheit.NRW" funded by the European Regional Development Fund North Rhine-Westphalia (EFRE.NRW), and the research project "Medisec-Nerd.NRW" funded by the state of North Rhine-Westphalia.

REFERENCES

[1] S. D. Applegate. 2013. The dawn of Kinetic Cyber. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. 1–15.

[2] Jake Beavers and Sina Pournouri. 2019. *Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions.* Springer International Publishing, Cham, 249–267. https://doi.org/10.1007/978-3-030-11289-9_11

[3] Biotronik Inc. 2016. *BIOTRONIK Home Monitoring - Patient information.* https://biotronik.cdn.mediamid.com/cdn_bio_doc/bio28825/42305/bio28825.pdf.

[4] Boston Scientific Corporation 2016. *LATITUDE LINK SYSTEM.* Boston Scientific Corporation, https://www.bostonscientific.com/content/dam/Manuals/us/current-rev-en/359485-001_LATITUDE_LINK_SPECIFICATION_en-USA_S.pdf.

[5] Guillaume Bour. 2019. *Security Analysis of the Pacemaker Home Monitoring Unit: A BlackBox Approach.* Master's thesis. Norwegian University of Science and Technology.

[6] Ronpichai Chokesuwattanaskul, Abdul Rahman Safadi, Randy Ip, Harsimran Kaur Waraich, Olivia Madison Hudson, and John H. Ip. 2019. Data Transmission Delay in Medtronic Reveal LINQTM Implantable Cardiac Monitor: Clinical Experience in 520 Patients. *Journal of Biomedical Science and Engineering* 12, 8 (Aug. 2019), 391–399. https://doi.org/10.4236/jbise.2019.128030

[7] Council of European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union* (2016).

[8] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference* (New Orleans, Louisiana, USA) *(ACSAC '14)*. Association for Computing Machinery, New York, NY, USA, 246–255. https://doi.org/10.1145/2664243.2664272

[9] Federal Communications Commission. 1999. 47 CFR 95.601-95.673 Subpart E.

[10] David K. Foot, Richard P. Lewis, Thomas A. Pearson, and George A. Beller. 2000. Demographics and cardiology, 1950–2050. *Journal of the American College of Cardiology* 35, 4 (2000), 1067–1081. https://doi.org/10.1016/S0735-1097(00)00561-1

[11] L. Galvani and G. Aldini. 1792. *De Viribus Electricitatis In Motu Musculari Commentarius Cum Joannis Aldini Dissertatione Et Notis ; Accesserunt Epistolae ad animalis electricitatis theoriam pertinentes.* Apud Societatem Typographicam.

[12] Guidant Corporation. 2004. *Operator's Manual, Zoom® Latitude^{TM}, Programming System, Model 3120 PRM.* https://fccid.io/ESCCRM312004/Users-Manual/User-Manual-532938.

[13] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *2008 IEEE Symposium on Security and Privacy (S&P 2008), 18-21 May 2008, Oakland, California, USA*. IEEE Computer Society, 129–142. https://doi.org/10.1109/SP.2008.31

[14] C. W. Israel, D. Bänsch, O. Breithardt, C. Butter, T. Klingenheben, C. Kolb, B. Lemke, U. Wiegand, and B. Nowak. 2015. Kommentar zu den neuen ESC-Leitlinien zur Schrittmacher- und kardialen Resynchronisationstherapie. *Der Kardiologe* 9, 1 (Feb. 2015), 35–45. https://doi.org/10.1007/s12181-014-0650-4

[15] Ryan Russel Joe Grand. 2004. *Hardware Hacking: Have Fun while Voiding your Warranty.* Syngress Publishing Inc.

[16] Kingpin. 2000. Attacks on and Countermeasures for USB Hardware Token Devices. In *Proceedings of the Fifth Nordic Workshop on Secure IT Systems.* Reykjavik University.

[17] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. 2020. Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail.

[18] Eivind Skjelmo Kristiansen and Anders Been Wilhelmsen. June 2018. *Security Testing of the Pacemaker Ecosystem.* Master's thesis. Norwegian University of Science and Technology.

[19] Anniken Wium Lie. June 2019. *Security Analysis of the Wireless Home Monitoring Units in the Pacemaker Ecosystem.* Master's thesis. Norwegian University of Science and Technology.

[20] Carl D. Livitt. 23.10.2016. Preliminary Expert Report. Stach & Liu, LLC d/b/a Bishop Fox.

[21] Eduard Marin, Dave Singelée, Flavio D. Garcia, Tom Chothia, Rik Willems, and Bart Preneel. 2016. On the (in)Security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them. In *ACSAC '16: Proceedings of the 32nd Annual Conference on Computer Security Applications* (Los Angeles, California, USA) *(ACSAC '16)*. Association for Computing Machinery, New York, NY, USA, 226–236. https://doi.org/10.1145/2991079.2991094

[22] Andreas Markewitz. 2019. Jahresbericht 2017 des Deutschen Herzschrittmacher- und Defibrillator-Registers – Teil 2: Implantierbare Kardioverter-Defibrillatoren (ICD). *Herzschrittmachertherapie + Elektrophysiologie* 30 (11 2019), 1–15. https://doi.org/10.1007/s00399-019-00648-9

[23] Medical Device Coordination Group. 2019. MDCG 2019-16 - Guidance on Cybersecurity for medical devices. European Commission.

[24] Medical Device Cybersecurity Working Group. 2020. Principles and Practices for Medical Device Cybersecurity. International Medical Device Regulators Forum.

[25] Medtronic 2019. *User Guide: My CareLink Heart App.* Medtronic, https://www.medtronic.com/content/dam/medtronic-com/de-de/patients/documents/carelink/mycarelink-heart-app_user-guide_medtronic.pdf.

[26] Muddy Waters Capital LLC. 25.08.2016. MW is Short St. Jude Medical (STJ:US).

[27] A. Müller, K. Rybak, T. Klingenheben, B. Schumacher, C. Israel, T.M. Helms, M. Oeff, C. Perings, S. Sack, C. Piorkowski, R. Preissler, C. Zugck, and J.O. Schwab. 2013. Empfehlungen zum Telemonitoring bei Patienten mit implantierten Herzschrittmachern, Defibrillatoren und kardialen Resynchronisationssystemen. *Der Kardiologe* (2013).

[28] Jens Cosedis Nielsen, Josef Kautzner, Ruben Casado-Arroyo, Haran Burri, Stefaan Callens, Martin R Cowie, Kenneth Dickstein, Inga Drossart, Ginger Geneste, Zekeriya Erkin, Fabien Hyafil, Alexander Kraus, Valentina Kutyifa, Eduard Marin, Christian Schulze, David Slotwiner, Kenneth Stein, Stefano Zanero, Hein Heidbuchel, and Alan G Fraser. 2020. Remote monitoring of cardiac implanted electronic devices: legal requirements and ethical principles - ESC Regulatory Affairs Committee/EHRA joint task force report. *EP Europace* (07 2020). https://doi.org/10.1093/europace/euaa168 euaa168.

[29] Todd A. Proebsting and Scott A. Watterson. 1997. Krakatoa: Decompilation in Java (Does Bytecode Reveal Source?). In *Third USENIX Conference on Object-Oriented Technologies and Systems (COOTS 97)*.

[30] Laurie Pycroft and Tipu Z. Aziz. 2018. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices* 15, 6 (2018), 403–406. https://doi.org/10.1080/17434440.2018.1483235

[31] Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, and Colleen M. Swanson. 2014. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks.. In *IEEE Symposium on Security and Privacy.* IEEE Computer Society, 524–539. https://doi.org/10.1109/SP.2014.40

[32] Frank Stajano and Ross Anderson. 1999. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *International workshop on security protocols.* Springer, 172–182.

[33] B. Struif and D. Scheuermann. 2002. Smartcards with biometric user verification. 589 – 592 vol.2. https://doi.org/10.1109/ICME.2002.1035688

[34] Julian Suleder, Andreas Dewald, and Florian Grunow. 2018. Medical Device Security: A Survey of the Current State (Whitepaper). ERNW Research.

[35] Hanne Sørum and Wanda Presthus. 2020. Dude, where's my data? The GDPR in practice, from a consumer's point of view. *Information Technology & People* ahead-of-print (06 2020). https://doi.org/10.1108/ITP-08-2019-0433

[36] M. Mitchell Waldrop. 2016. The chips are down for Moore's law. *Nature* 530 (Feb. 2016), 144–147. https://doi.org/doi:10.1038/530144a