IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 11, 2020, accepted March 25, 2020, date of publication March 30, 2020, date of current version May 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2984376

Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review

TOM TERVOORT[1], MARCELA TULER DE OLIVEIRA[2], WOLTER PIETERS[3], PIETER VAN GELDER[4], SILVIA DELGADO OLABARRIAGA[2], AND HENK MARQUERING[1]

[1]Department of Biomedical Engineering and Physics, Amsterdam UMC, University of Amsterdam, 1105 Amsterdam, The Netherlands
[2]Department of Epidemiology, Biostatistics and Bioinformatics, Amsterdam UMC, University of Amsterdam, 1105 Amsterdam, The Netherlands
[3]Department of Multi-Actor Systems, Faculty of Technology, Policy and Management, Delft University of Technology, 2600 Delft, The Netherlands
[4]Department of Values, Technology and Innovation, Faculty of Technology, Policy and Management, Delft University of Technology, 2600 Delft, The Netherlands

Corresponding author: Tom Tervoort (t.tervoort@amsterdamumc.nl)

This work was supported in part by the SAFECARE project (SAFEguard of Critical heAlth infrastructure), and in part by the ASCLEPIOS project (Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare) from the European Union's Horizon 2020 research and innovation program respectively under Grant 787002 and Grant 826093.

ABSTRACT Cyberattacks against healthcare institutions threaten patient care. The risk of being targeted by a damaging attack is increased when medical devices are used which rely on unmaintained legacy software that cannot be replaced and may have publicly known vulnerabilities. This review aims to provide insight into solutions presented in the literature that mitigate risks caused by legacy software on medical devices. We performed a scoping review by categorising and analysing the contributions of a selection of articles, taken from a literature set discovered through bidirectional citation searching. We found 18 solutions, each fitting at least one of the categories of intrusion detection and prevention, communication tunnelling or hardware protections. Approaches taken include proxying Bluetooth communication through smartphones, behaviour-specification based anomaly detection and authenticating signals based on physical characteristics. These solutions are applicable to various use-cases, ranging from securing pacemakers to medical sensor networks. Most of the solutions are based on intrusion detection and on tunnelling insecure wireless communications. These technologies have distinct application areas, and the decision which one is most appropriate will depend on the type of medical device.

INDEX TERMS Healthcare, security, medical devices, legacy software.

I. INTRODUCTION

In recent years, the healthcare sector has increasingly been affected by cyberattacks. Ransomware attacks against hospitals have caused significant financial damage and negatively affected patient care [1]. Moreover medical data breaches cost the industry billions, endanger patient privacy and enable large scale identity theft [2], [3]. Attackers have discovered healthcare to be an attractive target: medical information can be more than ten times more valuable than credit card numbers on the black market, because it can for example be used to get access to drugs or to perform insurance fraud [4]. Additionally, extortion attempts of hospitals have shown to be successful [5]. Medical devices in hospitals, such as blood gas analyzers, MRI scanners and X-Ray equipment, have been found to be compromised by attackers. These devices have been subsequently abused as a stepping stone to laterally move through the hospital networks [6].

In the future 'physical ransomware' could be used to conditionally disable critical (medical) hardware. That such an attack is feasible is demonstrated by an incident in which an Austrian hotel was targeted by a strain of ransomware that deactivated room keys and kept all doors locked until the ransom was paid [7]. Furthermore, vulnerabilities have been demonstrated in wearable medical devices, like mobile infusion pumps and implantable cardiac devices, which could allow attackers to wirelessly harm or even kill patients [8].

One of the reasons why medical devices are particularly vulnerable is because they frequently lack basic security features and run legacy operating systems and software

The associate editor coordinating the review of this manuscript and approving it for publication was Tai-Hoon Kim.

with publicly known vulnerabilities [9]. This is caused by equipment in use that no longer receives vendor support, or because of the difficulty of applying patches to device software [10]. Certification requirements can make patching medical devices particularly difficult: for example, when an update to a CE certified device is considered a *major revision* it is mandatory to perform extensive testing before this patch can be released [11].

In situations where patching is not possible, the simple solution of replacing the vulnerable hardware entirely can be unacceptably expensive. Therefore, we desire to find other solutions to cope with the security issues that are introduced when a healthcare provider has to rely on medical devices that run legacy software.

Bennett [12] and Bisbal *et al.* [13] proposed various software engineering solutions for coping with legacy software. However, they addressed the issue from the perspective of maintainability rather than security. Altawy and Youssef [10] discussed the trade-offs of various security technologies specifically aimed at implanted medical devices, and identify 'legacy compatibility' as an important challenge. To our knowledge, no literature review has yet been performed that is specifically aimed at medical legacy software.

With this study, we aim to find and categorize literature that contributes to the following research question: *what solutions, other than full replacement, address security issues caused by legacy software in medical devices?*

For this review, we considered systems that do some form of communication and processing and that fall under the definition of 'medical device' used by the European Medical Device regulation: namely a device intended by the manufacturer to be used for a medical purpose [11].

II. METHODOLOGY

We conducted a scoping review using the methodological framework proposed by Arksey and O'Malley [14]. A scoping review seeks to present an overview of a specific topic, whereas a systematic review aims to collect empirical evidence supporting a focused research question.

Within the framework by Arksey and O'Malley, a scoping study is divided within the following stages: identifying a research question, identifying relevant studies, making a selection from those studies, charting data and finally collating, summarizing and reporting the results.

When applicable to this study, we followed PRISMA guidelines [15].

A. IDENTIFYING RELEVANT STUDIES

We searched for studies that propose a security solution that addresses medical software vulnerabilities without requiring the vulnerable (legacy) software to be replaced or redesigned. These studies should either be focused at (a class of) medical devices, or specifically mention that the solution applies to medical devices.

We collected studies with a *bidirectional citation searching* method, in a manner described by Hinde and Spackman [16]. Here, the starting point of a search is a small set of relevant studies: the 'pearls'. The literature set is subsequently expanded by adding new studies that either cite, or are cited by, any of the pearls. We performed one iteration of this search with three pearls.

We selected pearls by manually browsing the literature for three highly cited studies, which we also expect to be cited by studies that introduce new solutions. We chose the following three pearls:

1) *They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices* by Gollakota *et al.* [17].
   - This study proposes a security solution specifically aimed at legacy medical devices. It attempts to protect otherwise unencrypted and unauthenticated radio signals from an implanted medical device.
2) *Security Challenges for Medical Devices* by Sametinger *et al.* [18].
   - This study summarizes general challenges for medical device security. We expect it to be cited by studies that build on this summary, or which introduce solutions. This may provide insight in security properties that set medical devices apart from other areas affected by legacy issues.
3) *Challenges for Securing Cyber Physical Systems* by Càrdenas *et al.* [19].
   - This study discusses security issues unique to *cyber-physical systems*, a category of systems that includes medical devices. It explicitly states that these types of systems can be difficult to patch due to certification problems or interference with system availability. Related studies may expand on this or provide solutions that apply to the medical domain.

The three pearls increase in the level of generality: from a specific class of medical devices to medical devices in general, to general cyber-physical systems.

In order to find studies that cite the three studies mentioned above, we used the search engine Google Scholar, which offers 'cited by' searches, and indexes a comprehensive number of scientific databases [20]. We performed the Google Scholar searches on May 15, 2019.

These searches resulted in a literature set consisting of 849 studies (3 pearls, 121 studies cited by pearls and 725 studies citing pearls). The number of results per search are listed in Table 1. References to all studies within this set are listed in Supplement S1.

TABLE 1. Number of collected studies, by method.

Pearl	No. of studies cited by pearl	No. of studies citing pearl
[17]	56	315
[18]	37	82
[19]	28	328
Total	121	725

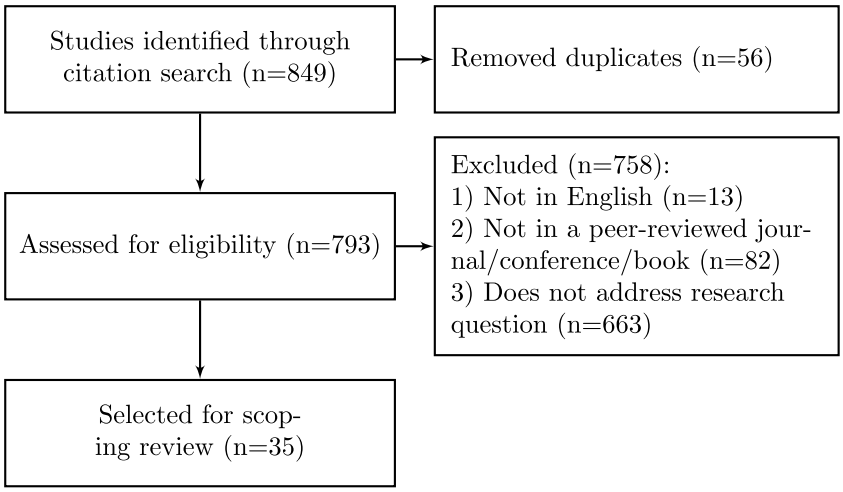

FIGURE 1. Stages of study selection.

B. STUDY SELECTION

After obtaining the bibliographic data (title, source, author, publication year and abstract) of the 849 studies in the literature set, we manually determined eligibility for this review.

First, duplicates were removed. When multiple versions of the same study were found (in case of papers being revised, for example), the most recent version was included.

Next, we used the following criteria to decide whether a study was eligible:

1) The text must be in English.
2) Studies must have been published in peer-reviewed journals, conferences or books.
3) The study must contribute to the research question. We consider this to be the case when the following holds:
   a) The study proposes or discusses one or more security solutions to existing vulnerabilities.
   b) These solutions are *legacy compatible*; i.e. they do not require the vulnerable software to be rewritten or replaced.
   c) The study specifically mentions that its solutions apply to (types of) medical devices.

The number of studies excluded by each criterion is illustrated in Fig. 1.

For each study, its eligibility according to these criteria was assessed by one author, based on the title, abstract and source of the study. When the study's eligibility was still unclear, this author retrieved and examined the full-text.

Their decision regarding criteria 3 (whether the study contributes to the research question), was reviewed by another author. In case of disagreement, we made a consensus decision on whether to include the study after a round of discussion.

After applying these criteria, a total of 35 studies were included. The included studies are listed in the first column of Table 2.

C. CHARTING THE DATA

We categorized studies using the following taxonomy:

1) The types of systems to which the study is applicable:
   - wearable or implantable medical devices brought home by patients;
   - non-wearable medical devices physically located within a healthcare institution.
2) The types of risks that are addressed, broadly categorized as the negative forms of the elements of the CIA (confidentiality, integrity and availability) triad used in information security [21]:
   - these are *disclosure* (of sensitive information), *alteration* (of system behavior) and *denial* (of service).
3) The type of security-enhancing solutions that are discussed, as one or more of the following categories:
   - intrusion detection;
   - intrusion prevention (intrusion detection with the additional capability to block or interfere with malicious communications);
   - communication *tunnelling* (i.e. relaying messages, that use an insecure legacy protocol, through an alternative secure channel);
   - hardware protections.
4) The manner in which the solution is analysed, as one or more of the following categories:
   - theoretical introduction;
   - description of an implementation;
   - experimental evaluation;
   - literature review;
   - security analysis of solutions introduced by a distinct study.

For each selected study, we decided its categorization by manually analysing the full text. This analysis was performed by the first author. For each study, the second author reviewed

TABLE 2. Properties of the 35 reviewed studies.

Study	Authors	Publication year	Application area		Risk types			Solution types				Method of analysis				
			wearable/implantable devices	non-wearable devices	disclosure	alteration	denial	intrusion detection	intrusion prevention	communication tunnelling	hardware protections	theoretical introduction	implementation description	experimental evaluation	security analysis of existing solution	literature review
[10]	Altawy and Youssef	2016	●		●	●				●	●				●	●
[17]	Gollakota et al.	2011	●		●	●				●	●	●	●	●		
[18]	Sametinger et al.	2015	●		●	●		●		●	●					●
[19]	Càrdenas et al.	2009		●		●	●	●								●
[22]	Mitchell and Chen	2013		●		●	●	●	●			●				
[23]	Humayed et al.	2017	●		●	●	●	●		●	●					●
[24]	Mitchell and Chen	2015		●		●		●				●		●		
[25]	Song et al.	2014		●	●	●	●	●								●
[26]	Ahmed et al.	2018	●			●		●	●			●		●		
[27]	Alpano et al.	2017		●		●		●				●		●		
[28]	Rushanan et al.	2014	●		●	●		●		●	●					●
[29]	Camara et al.	2015	●		●	●		●		●	●				●	●
[30]	Zhang et al.	2013	●			●		●	●		●	●	●	●		
[31]	Tippenhauer et al.	2013	●		●						●				●	
[32]	Shen et al.	2013	●		●	●				●	●	●	●	●		
[33]	Skowyra et al.	2013	●	●		●	●	●				●				
[34]	Zheng et al.	2017	●		●	●		●		●	●					●
[35]	Marin et al.	2016	●			●					●	●				
[36]	Pournaghshband et al.	2013	●		●	●				●	●	●				
[37]	Ankarali et al.	2015	●		●	●				●	●					●
[38]	Steinmetzer et al.	2015	●		●	●				●	●				●	
[39]	Rathore et al.	2017	●		●	●		●		●	●					●
[40]	Wang et al.	2018	●			●	●	●	●		●	●	●	●		
[41]	Ellouze et al.	2013	●		●	●	●			●	●				●	●
[42]	Ankaralı et al.	2014	●		●	●		●		●	●					●
[43]	Zheng et al.	2016	●		●						●			●	●	
[44]	Kyaw and Cusack	2014	●	●	●	●				●	●					●
[45]	Kulaç	2017	●		●					●	●	●				
[46]	Pournaghshband et al.	2015	●		●	●	●			●		●	●			
[47]	Kulaç	2019	●		●					●	●	●				
[48]	Rathore et al.	2019	●			●	●	●				●		●		
[49]	Kulaç et al.	2018	●		●	●		●		●	●					●
[50]	Lu and Lysecky	2019	●			●		●			●	●	●	●		
[51]	Pinisetty et al.	2018	●			●		●			●	●	●			
[52]	Burnik et al.	2019		●	●	●	●			●		●	●	●		
Total			29	8	23	31	10	20	4	20	25	18	8	11	6	14

the selected categories per property. In case of disagreement we made a consensus decision on how to classify each property after a round of discussion.

We found that all selected studies fell into at least one of the categories for each property in the taxonomy.

D. COLLATING, SUMMARIZING AND REPORTING THE RESULTS

After we determined the properties of each study, we counted the number of studies within each classification per property. Subsequently, we summarized the different types of solutions. When two or more studies address the same problem, or use a similar approach, we examined their differences. We also identified some potential areas in which the research from the selected studies can be expanded.

III. RESULTS

A. CATEGORIZATION

1) APPLICATION AREA

Table 2 shows how we categorized the 35 selected studies. Solutions applicable to implantable and wearable medical devices are covered most frequently, namely by 29 of

the studies. 8 studies cover medical devices that are not wearable but instead remain placed within a healthcare institution. All studies fit in at least one of these two application areas, and 2 of the studies fit in both.

2) RISK TYPES

The risk of malicious alteration of data or device behaviour is addressed by 31 of the studies, 10 of which also address denial-of-service. Disclosure risks are considered by 23 studies, 4 of which only focus on eavesdropping attacks but not alteration.

3) SOLUTION TYPES AND METHODS OF ANALYSIS

New solutions are proposed in 18 studies, and 14 studies are literature reviews of prior publications. The remaining studies examine specific solutions introduced by other publications.

Of the studies classified as 'theoretical introduction', 10 use intrusion detection methods (4 of which also provide intrusion prevention), and 7 make use of communication tunnelling. One study (Marin *et al.* [35]) introduces a solution which uses neither approach. Of all solutions, 10 require the introduction of specialized hardware.

Of the studies proposing a new solution, 8 also describe the implementation of a system that applies the solution in a realistic setting. 10 studies provide some experimental evaluation of a solution they introduce, either based on an implementation or a simulation thereof.

B. SOLUTIONS PROVIDING INTRUSION DETECTION

One approach of coping with legacy software is to introduce an additional, external, monitoring system that tries to determine whether a device is being attacked. While this mechanism alone does not protect against attacks, it does allow patients or practitioners to respond immediately, for example by turning the device off.

Such a monitoring system is known as an IDS (intrusion detection system). An IDS needs to be able to monitor some aspect of the device to be protected (for example, message contents or physical characteristics of a wireless signal), and it needs to apply some sort of *detection technique* to distinguish regular behaviour from attacks.

We subdivide detection techniques in the three categories used by Mitchell and Chen [53]:

- *Knowledge-based*: the IDS will detect predefined signatures of known attacks. It will not be able to detect attacks that are unknown, or not in the IDS' attack database.
- *Behaviour-based*: the IDS will observe how a device operates under normal conditions, and will yield an alert when its behaviour suddenly deviates from this. This has the capability of detecting attacks that are not predefined. However, such an IDS is more sensitive to false positives than a knowledge-based one, because anomalous behaviour does not necessarily mean an attack is taking place. Some of the techniques for anomaly detection for cyber-physical systems are discussed by Han *et al.* [25].
- *Behaviour-specification-based*: the IDS is preconfigured with a specification of how a device should behave and detects cases where the observed behaviour diverts from this specification. Unlike behaviour-based systems, it will not dynamically adjust its definition of what behaviour is considered normal. The false positive and negative rates depend on the accuracy of the specification, which requires manual effort to define per device.

Once a security event is registered, an IDS needs to register a *response* in some way. Typically, this takes the form of an alert to an organisation's security operation centre (SOC), but that may not be sufficient in cases where a patient takes a medical device home, for example. When part of the response is to actively interfere with the monitored system in an attempt to stop the attack, the IDS is considered to be an intrusion prevention system (IPS).

An overview of the IDS solutions proposed by the literature can be found in Table 3. We found that the solutions monitor various different aspects of a medical device or its environment in order to detect malicious behaviour. We identified that each solution monitors one of the following aspects of a medical device: the wireless communications of implanted medical devices (IMDs), the physical actuators of IMDs, the readings from sensor network nodes, IP network packets or software execution characteristics.

1) MONITORING WIRELESS COMMUNICATIONS OF IMDs

Zhang *et al.* [30] proposed an IDS they coin MedMon. MedMon is a separate physical device that acts as a wireless traffic monitor. No changes to a programmer or IMD need to be made before it can be used. This approach uses anomaly detection based on physical (e.g. signal strength or angle of arrival) or behavioural (e.g. type of command, parameters) indicators. When an anomalous message is observed, the patient is alerted. Optionally, MedMon can also be configured to act as an IPS. In this mode, all communications with the IMD (both legitimate and malicious) are temporarily jammed after an alarm is raised.

Wang *et al.* [40] proposed a specialized IDS and IPS for protecting on-body devices that communicate with each other. They take advantage of how human tissue and body shape affect radio propagation characteristics, to identify whether a signal is sent from an on-body device. If the signal is instead sent through the air from a distance, it is considered to be malicious.

2) MONITORING PHYSICAL ACTUATORS OF IMDs

Two studies describe how the physical actuators of an IMD can be monitored to detect the effect of successful device compromise, rather than detecting the attack attempt itself. This method of intrusion detection would also be effective in cases where a device is compromised through another method

TABLE 3. A comparison of the IDS-based solutions. The response cell is left empty when this aspect is not discussed by the study.

Study	Target system	Attacker capabilities	Monitored aspect	Detection technique	Response
[22]	Sensor network	Control over subset of nodes	Sensor readings	Behaviour-specification	Ignore untrusted nodes
[24]	Sensor network	Control over subset of nodes	Sensor readings	Behaviour-specification	–
[26]	Sensor network	Can impersonate nodes	Signal noise	Behaviour	Ignore untrusted nodes
[27]	Generic CPS	Connected to network	(IP) network traffic	Knowledge	–
[30]	Wearable/implanted devices	Wireless message spoofing/tampering	Wireless communications and signal characteristics	Behaviour	Patient notification or message jamming
[33]	Moving wireless devices within a geographic area	Wireless message spoofing/jamming	Wireless messages with time and location metadata	Behaviour	–
[40]	On-body devices	Send wireless signals from a distance	Signal propagation patterns	Behaviour-specification	–
[48]	Deep brain implant	Control over implant software	Brain stimulation patterns	Behaviour-specification	–
[50]	Embedded/implanted device	On-device code execution	Trace port output	Behaviour	–
[51]	Pacemaker	Control over pacemaker software	ECG signals	Behaviour-specification	Audio alarm

than a spoofed command, such as a supply-chain attack where malware is added to a software update.

Pinisetty *et al.* [51] proposed a smartwatch that monitors ECG signals from a pacemaker. The watch sounds an alarm when the observed signals do not match the pacemaker specification. Rathore *et al.* [48] take a similar approach and examine stimulation patterns from a deep brain implant. They use a deep learning strategy to train an attack classifier.

3) MONITORING READINGS FROM NODES IN A SENSOR NETWORK

Five of the studies examine the situation in which an attacker compromises a node within a medical sensor network, causing this node to provide faulty readings. In these cases, the IDS is added to a central control unit that processes the readings.

Mitchell and Chen [22] proposed a specification-based IDS that scores nodes based on how well they comply with the specification. Nodes that score below a certain threshold will be automatically ignored, so the system also acts as an IPS. Mitchell *et al.* also propose a similar system that uses a behaviour-rule specification technique [24]. The rules that specify how a node is supposed to behave can be altered dynamically during system operation, to increase their accuracy.

Ahmed *et al.* [26] took a different approach: their IDS creates a fingerprint of the sensor and process noise that uniquely identifies each specific sensor. This allows sensors to be identified even when a legacy communication protocol is used that does not provide (strong) authentication. This assumes that spoofed sensor readings from an attacker have a distinct noise fingerprint.

Skowyra *et al.* [33] considered the case where a variety of sensors give readings while moving around within a specific area, such as a hospital. They assume that the location of a message's originator can be determined within this area and explain how this location information can be used as input for an anomaly-detecting IDS.

4) MONITORING STANDARD IP NETWORKS

Alpaño *et al.* [27] proposed a solution for monitoring cyber-physical devices connected to a standard (wired) IP network.

Instead of instructing an IDS what normal operations look like and treating deviations as an attack, they make it recognize a number of attacks against general-purpose software, by examining the content of network packets. They trained a multilayer perceptron neural network to recognize 22 different attack patterns based on a public dataset. The authors state that classifying attacks using a model trained through this method is less time- and resource-intensive than other similar approaches, making it more suitable for resource-constrained cyber-physical systems. A drawback of this approach is that new attacks, or attacks that were not considered during the training phase, can not be detected.

5) MONITORING SOFTWARE EXECUTION CHARACTERISTICS

The methods discussed above treat the device software as a *black box* of which inputs and outputs can be monitored. Lu and Lysecky [50] use a different approach: they directly monitor the *software execution*. They achieve this by connecting a monitoring device to an exposed trace or debug port of a pre-existing embedded system (such as a pacemaker). This allows them to monitor software timing characteristics that are influenced by e.g. interrupts, cache misses and branch mispredictions. They use support vector machine learning to distinguish the characteristics of regular software operation, from anomalies that may have been caused by an attack.

C. SOLUTIONS FOR TUNNELLING WIRELESS LEGACY PROTOCOLS

Some solutions focus on adding some form of cryptographic protections to a legacy protocol to prevent message forgery,

spoofing or eavesdropping. These solutions focus specifically on IMDs, and address the problem that many existing IMDs employ no or broken cryptography [54]–[56]. Because insecure devices can already be implanted in many patients, it is desirable to be able to secure their communications without having to replace them.

1) SELECTIVE JAMMING

Gollakota *et al.* [17] considered the case of legacy IMDs that use an insecure radio communication protocol in which commands are not authenticated and device readings are not encrypted. They propose that the patient carries an additional device called a *shield*. In order to protect outgoing messages from the IMD, the shield transmits a jamming signal that renders them unreadable for attackers. The shield also acts as a receiver, which is aware of the jamming signal and can cancel it. Subsequently, received messages will be forwarded to the controller over a secure channel using standard cryptography. Additionally, the shield transmits a jamming signal when it detects any plaintext command that does not originate from the shield itself, causing the message to be ignored due to a checksum failure.

Kulaç [45], [47] proposed two solutions similar to the shield by Gollakota *et al.* These solutions involve embedding a jamming device in respectively a belt and a jacket. They address the scenario of on-body sensors insecurely communicating with an IMD, and try to prevent eavesdropping attacks from passively listening attackers.

Shen *et al.* [32] addressed a limitation of the shield: namely that multiple shields in close proximity can block each other's legitimate messages. They describe a method for jammers to authenticate themselves using a shared secret key, and to synchronize with each other to prevent interference.

Altawy and Youssef [10] and Ellouze *et al.* [41] described a denial-of-service attack against the shield: because unauthorised messages are scrambled but still processed by the IMD, the IMD's battery can be exhausted by repeatedly sending it arbitrary messages.

Zheng *et al.* [34] discussed some practical drawbacks of externally worn security devices such as the shield: having to constantly wear and charge these devices is inconvenient, and can easily be forgotten. Furthermore, it reminds them of their condition and can reveal the presence of the condition to others. Altawy and Youssef [10] discuss a general problem with jamming devices: operating them can unexpectedly interfere with other radio frequency devices; furthermore, performing any kind of jamming may be illegal in the location where the device is used.

Tippenhauer *et al.* [31] described an eavesdropping attack against selective jamming-based techniques such as the shield: they demonstrate that an attacker is still able to separate the jamming signal from the message data by using two antennas, therefore breaking confidentiality. Steinmetzer *et al.* [38] and Zheng et. al [43] provide a multi-antenna attack against a different selective jamming technique, called orthogonal blinding.

2) SMARTPHONE-BASED BLUETOOTH PROXIES

Pournaghshband *et al.* [36], [46] proposed a method to protect legacy IMD's that insecurely communicate using an insecure Bluetooth-based protocol. Similarly to the shield solution (Gollakota *et al.* [17]), an intermediate device is used to proxy the legacy protocol over a secure channel. Their approach does not require specialized hardware, however, but instead uses an application for a general-purpose smartphone. Because Bluetooth is used, the app can impersonate a device programmer and then use a secure channel to forward messages to the actual programmer.

The authors acknowledge that this approach does not protect against attackers that manage to insert themselves between the IMD and the phone, but argue that this is difficult in practice when the device and phone are physically very close to each other.

D. SOLUTION BASED ON INDISCRIMINATE JAMMING

Marin *et al.* [35] described vulnerabilities in a communication protocol used by implantable cardiac defibrillators (ICDs). They describe a countermeasure that could be implemented in the short-term without having to extract existing ICDs. The measure is to have the device programmer constantly jam the wireless channels the ICD listens to, at any time the programmer is not communicating with the ICD itself.

This solution does not attempt to provide intrusion detection or to add authentication, but instead exploits the fact that in this use-case the programmer initiates all communication. This does not completely mitigate attacks, but does reduce the time window in which they can be carried out.

E. SOLUTION FOR SECURE REMOTE MAINTENANCE

Burnik *et al.* [52] describe how they added secure remote maintenance functionality to an existing medical device. The device in question already provided an application extension platform, on which the authors built a software-based maintenance module that was carefully constructed as to not interfere with the primary functionalities of the device (meaning it would not be necessary to re-certify it) while also not introducing new security vulnerabilities.

The maintenance module would be connected to a support server using an authenticated and encrypted VPN tunnel, protecting communications from unauthorised attackers. The core device, however, would have no exposed network interfaces. This means that vulnerabilities in the core device (assuming a secure maintenance module) could not be exploited by a network-level attacker. With this solution continued remote management of a vulnerable legacy device is possible, without the need to expose a vulnerable device to a network.

IV. DISCUSSION

Solutions for securing legacy software in medical devices primarily focus on two areas: providing intrusion detection and tunnelling insecure wireless protocols. The proposed

intrusion detection techniques primarily use behaviour and behaviour-specification based detection methods, and focus on wearable/implanted devices and sensor networks. The tunnel-based solutions are aimed at securing IMDs that do not cryptographically protect their communications.

Among the different types of solutions, most concentrate on intrusion detection systems. These studies address varied medical application areas, and some of them describe practical implementations and experimental results. However, we have not found independent evaluations of the effectiveness of these techniques. Further independent assessments of the false positive and negative rates of these systems, in practical settings, could give a better insight into the strengths and weaknesses of each solution.

The solutions based on communication tunnelling by selective jamming are vulnerable to multi-antenna attacks. We have not found techniques that mitigate these vulnerabilities. More research is necessary in this area to determine whether secure selective jamming is feasible through some other method. Furthermore, we have not found independent security analyses of the Bluetooth proxy solutions, of which security is based on the assumption that man-in-the-middle attacks are not possible when an IMD communicates with a close on-body device over Bluetooth. Further research could build confidence in the effectiveness of this solution.

To our knowledge, this is the first scoping review that specifically identifies legacy-compliant solutions to medical device security issues. Altawy and Youssef [10] and Ellouze *et al.* [41] have discussed the concept of legacy-compliant solutions, but specifically focused on the area of implantable devices. Bennett [12] and Bisbal *et al.* [13] examined the legacy problem from a software engineering perspective, but did not consider security or the medical domain.

This review identifies solutions and their application areas, but does not provide a comprehensive technical analysis of the different solutions. Such an analysis could be provided by future (systematic) reviews.

Because we used a citation searching methodology, the studies we included strongly depended on the selection of pearls. Because the pearls varied in their level of generality, this choice may have biased the included literature set towards studies about a subtopic closer to the most specific paper (in this case the study by Gollakota *et al.* [17], which focuses on wireless communications security of IMDs).

We did not follow citations recursively during our search. Due to this, we may have missed relevant studies because they did not cite and were not cited by one of the pearls directly. Nonetheless, we have found 35 studies on various topics and did not identify a single case where a second iteration of citation searching would have added a new study that satisfied the selection criteria.

Because the selection and charting processes were manual, author biases could have influenced the selection and classification of studies. Furthermore, because selection criterion 3 is difficult to assess objectively, it is possible that the authors may have mistakenly excluded relevant studies. Supplement S1 indicates the criterion based on which each study was excluded and allows readers to verify the selection choices we made.

A selection criterion excluded any studies that did not mention the medical use case; this may have excluded broader studies that introduce solutions which are still applicable to the medical domain. However, using this criterion has the advantage that the healthcare relevance of the selected studies is clear.

V. CONCLUSION

We found 18 studies addressing risks caused by legacy software in medical devices. These are primarily based on intrusion detection or on providing encrypted communication tunnels, and provide a promising set of options to cope with insecure devices of which the software cannot be replaced.

Most of these solutions either focus on wirelessly communicating implanted and wearable devices, or on sensor networks that are part of a larger system. The solutions can be used by adding additional hardware on top of the legacy devices, by routing messages through an intermediary system, by updating programmers or by taking advantage of pre-existing software add-on interfaces.

We find that there is a variety of application areas and attacker models used by each solution, meaning that deciding which is most appropriate strongly depends on the type of medical device that should be protected.

Some of the tunnelling techniques are circumventable by attackers, and usability issues have been identified in solutions requiring additional hardware. Furthermore, intrusion detection systems have not yet been independently tested experimentally. Future research could reveal more about the effectiveness of these solutions, and how to apply them in practice.

If legacy-compliant security technologies such as those described in this review will be incorporated into security products, healthcare institutions will have more options to improve their security despite the presence of legacy medical devices.

SUPPLEMENTARY MATERIAL

S1: LITERATURE SET

CSV table containing details of the 849 studies discovered through bidirectional citation searching. Marks which of these studies have been included in the review and based on which criteria studies were excluded. File name: `legacy-review-literature-set.csv`.

REFERENCES

[1] S. Ghafur, A. Darzi, J. Kinross, C. Hankin, and G. Martin, "WannaCry—A year on," *BMJ*, vol. 2381, p. k2381, Jun. 2018, doi: 10.1136/bmj.k2381.

[2] Ponemon Institute LLC, "Fifth annual benchmark study on privacy & security of healthcare data," *Annu. Benchmark Study Privacy Secur. Healthcare Data*, vol. 5, pp. 1–42, May 2015.

[3] D. Mancilla, "Exploring medical identity theft," *Perspect. Health Inf. Manage.*, vol. 6, pp. 1–11, Sep. 2009.

[4] A. Sulleyman, "NHS cyber attack: Why stolen medical information is so much more valuable than financial data," Independent, May 2017. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html
[5] R. Winton, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating," *Los Angeles Times*, Feb. 2016. [Online]. Available: https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
[6] D. Storm, "MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks," Computerworld, Jun. 2015. [Online]. Available: https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html
[7] D. Bilefsky, "Hackers use new tactic at austrian hotel: Locking the doors," The New York Times, Jan. 2017. [Online]. Available: https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html
[8] B. Rios and J. Butts, "Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies," WhiteScope, Half Moon Bay, CA, USA, Tech. Rep., 2017. [Online]. Available: http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html
[9] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, pp. 305–316, Jul. 2015.
[10] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.
[11] European Parliament and Council of the European Union, "Regulation (EU) 2017/745 of the European parliament and of the council of 5 April 2017 on medical devices," *Off. J. Eur. Union*, vol. 60, pp. 1–175, Apr. 2017. [Online]. Available: http://data.europa.eu/eli/reg/2017/745/oj
[12] K. Bennett, "Legacy systems: Coping with success," *IEEE Softw.*, vol. 12, no. 1, pp. 19–23, Jan. 1995.
[13] J. Bisbal, D. Lawless, B. Wu, and J. Grimson, "Legacy information systems: Issues and directions," *IEEE Softw.*, vol. 16, no. 5, pp. 103–111, Sep. 1999. [Online]. Available: http://ieeexplore.ieee.org/document/795108/
[14] H. Arksey and L. O'Malley, "Scoping studies: Towards a methodological framework," *Int. J. Social Res. Methodol.*, vol. 8, no. 1, pp. 19–32, Feb. 2005.
[15] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *J. Clin. Epidemiol.*, vol. 7, no. 9, pp. 889–896, 2009.
[16] S. Hinde and E. Spackman, "Bidirectional citation searching to completion: An exploration of literature searching methods," *PharmacoEconomics*, vol. 33, no. 1, pp. 5–11, Jan. 2015.
[17] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, p. 2, Oct. 2011.
[18] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2749359.2667218
[19] A. Càrdenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Proc. Workshop Future Directions Cyber-Phys. Syst. Secur.*, 2009, pp. 1–9. [Online]. Available: http://chess.eecs.berkeley.edu/pubs/601/cps-security-challenges.pdf
[20] M. Gusenbauer, "Google Scholar to overshadow them all? Comparing the sizes of 12 academic search engines and bibliographic databasess," *Scientometrics*, vol. 118, no. 1, pp. 177–214, 2019, doi: 10.1007/s11192-018-2958-5.
[21] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Rockland, MA, USA: Syngress, 2014.
[22] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.
[23] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.
[24] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan. 2015.
[25] S. Han, M. Xie, H.-H. Chen, and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE Syst. J.*, vol. 8, no. 4, pp. 1052–1062, Dec. 2014.
[26] C. M. Ahmed, J. Zhou, and A. P. Mathur, "Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in CPS," in *Proc. 34th Annu. Comput. Secur. Appl. Conf.*, Dec. 2018, pp. 566–581.
[27] P. V. S. Alpano, J. R. I. Pedrasa, and R. Atienza, "Multilayer perceptron with binary weights and activations for intrusion detection of cyber-physical systems," in *Proc. IEEE Region Conf. (TENCON)*, Nov. 2017, pp. 2825–2829.
[28] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 524–539.
[29] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015, doi: 10.1016/j.jbi.2015.04.007.
[30] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.
[31] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 160–173.
[32] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 174–188.
[33] R. Skowyra, S. Bahargam, and A. Bestavros, "Software-defined IDS for securing embedded mobile devices," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2013, pp. 1–7.
[34] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical devices: A review," *IEEE Sensors J.*, vol. 17, no. 3, pp. 562–576, Feb. 2017.
[35] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl. (ACSAC)*, 2016, pp. 226–236.
[36] V. Pournaghshband, M. Sarrafzadeh, and P. Reiher, "Securing legacy mobile medical devices," in *Proc. Int. Conf. Wireless Mobile Commun. Healthcare*, in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 61, 2013, pp. 163–172.
[37] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare-Transforming Healthcare Through Innov. Mobile Wireless Technol. (MOBIHEALTH)*, Jun. 2016, pp. 246–249.
[38] D. Steinmetzer, M. Schulz, and M. Hollick, "Lockpicking physical layer key exchange: Weak adversary models invite the thief," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2015, pp. 1–11, doi: 10.1145/2766498.2766514.
[39] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1495–1501.
[40] W. Wang, L. Yang, Q. Zhang, and T. Jiang, "Securing on-body IoT devices by exploiting creeping wave propagation," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 696–703, Apr. 2018.
[41] N. Ellouze, M. Allouche, H. B. Ahmed, S. Rekhis, and N. Boudriga, "Security of implantable medical devices: Limits, requirements, and proposals," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2475–2491, Dec. 2014.
[42] Z. E. Ankaralı, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the security research for wireless implantable medical devices," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare (Mobihealth)*, 2014, pp. 246–249.
[43] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Profiling the strength of physical-layer security," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, 2016, pp. 21–30.
[44] A. K. Kyaw and B. Cusack, "Security challenges in pervasive wireless medical systems and devices," in *Proc. 11th Annu. High Capacity Opt. Netw. Emerg./Enabling Technol. (Photon. Energy)*, Dec. 2014, pp. 178–185.

[45] S. Kulaç, "Security belt for wireless implantable medical devices," *J. Med. Syst.*, vol. 41, no. 11, Nov. 2017, Art. no. 172.
[46] V. Pournaghshband, M. Sarrafzadeh, D. Meyer, M. Holyland, and P. Reiher, "Adrasteia: A smartphone app for securing legacy mobile medical devices," in *Proc. 17th IEEE Int. Conf. Comput. Sci. Eng. (CSE), Jointly 13th IEEE Int. Conf. Ubiquitous Comput. Commun. (IUCC), 13th Int. Symp. Pervas. Syst.*, Jan. 2015, pp. 758–763.
[47] S. Kulac, "A new externally worn proxy-based protector for non-secure wireless implantable medical devices: Security jacket," *IEEE Access*, vol. 7, pp. 55358–55366, 2019.
[48] H. Rathore, A. K. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "A novel deep learning strategy for classifying different attack patterns for deep brain implants," *IEEE Access*, vol. 7, pp. 24154–24164, 2019.
[49] S. Kulac, M. H. Sazli, and H. G. Ilk, "External relaying based security solutions for wireless implantable medical devices: A review," in *Proc. 11th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Sep. 2018, pp. 3–6.
[50] S. Lu and R. Lysecky, "Data-driven anomaly detection with timing features for embedded systems," *ACM Trans. Design Automat. Electron. Syst.*, vol. 24, no. 3, pp. 1–27, Jun. 2019.
[51] S. Pinisetty, P. S. Roop, V. Sawant, and G. Schneider, "Security of pacemakers using runtime verification," in *Proc. 16th ACM/IEEE Int. Conf. Formal Methods Models Syst. Design (MEMOCODE)*, Oct. 2018, pp. 1–11.
[52] U. Burnik, Š. Dobravec, and M. Meža, "Design of a secure remote management module for a software-operated medical device," *Biomedizinische Technik*, vol. 64, no. 1, pp. 67–80, 2019.
[53] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–29, Apr. 2014.
[54] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. e-Health Netw., Appl. Services*, Jun. 2011, pp. 150–156.
[55] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.
[56] M. Green. (Feb. 2018). *A Few Notes on Medsec and St. Jude Medical*. [Online]. Available: https://blog.cryptographyengineering.com/2018/02/17/a-few-notes-on-medsec-and-st-jude-medical/

TOM TERVOORT received the M.S. degree in computing science from Utrecht University, The Netherlands. He is currently pursuing the Ph.D. degree in medical cybersecurity with Amsterdam UMC, Location AMC, while working as a Security Specialist for Secura.

He has participates in the SAFECARE H2020 project. His research interests include medical device security, security trade-offs, access control, cryptographic engineering, and protocol verification.

MARCELA TULER DE OLIVEIRA graduated in Telecommunications Engineering from the Universidade Federal Fluminense in Rio de Janeiro, in 2017, and has participated in a student exchange program at the University of Florida, Florida, USA. She received the M.S. degree in electrical and telecommunications engineering from the Graduate Program in Electrical and Telecommunications Engineering, Universidade Federal Fluminense in Rio de Janeiro, Brazil. She is currently pursuing the Ph.D. degree with Amsterdam UMC, Location AMC, where she has participates in the ASCLEPIOS H2020 project (Trusted digital solutions and Cybersecurity in Health and Care). In her Ph.D., she researches the usage of data encryption for securing and sharing healthcare and medical research data. Her main areas of interest are new-generation networks, sensor networks, network security, and blockchain and computational intelligence.

WOLTER PIETERS received the M.S. degree in computer science and philosophy of science, technology and society from the University of Twente, The Netherlands, in 2002 and 2003, respectively, and the Ph.D. degree in information security from Radboud University Nijmegen, The Netherlands, in 2008.

After his Ph.D., he was a Policy Advisor for the Dutch Ministry of the Interior and Postdoctoral Researcher at the University of Twente. Working for both TU Delft and the University of Twente, he was the Technical Leader of the TREsPASS European project on socio-technical security models, from 2012 to 2016. Since 2015, he has held a full-time position on cyber risk at the Technology, Policy and Management faculty of TU Delft, The Netherlands, since 2017 as an Associate Professor. His research interests include behavioural aspects of cybersecurity, cybersecurity risk management, cybersecurity governance, and cyber ethics.

Dr. Pieters has co-organized two Dagstuhl seminars and two Lorentz seminars on cybersecurity topics, including socio-technical security metrics and cyberinsurance, and was the program Co-Chair of the New Security Paradigms Workshop, in 2018 and 2019.

PIETER VAN GELDER is currently a Professor with the Safety Science in the Safety and Security Science Section, TU Delft. He has been involved in research and education on safety and reliability since 1991. He teaches 4th and 5th year courses at TU Delft and conducts research on new methods and techniques in risk analysis, in particular on decompositioning techniques and probabilistic analytics. He has published a large number of highly cited articles in the field of infrastructure safety, the statistical modelling of high impact Low Probability (HILP) events and the consequent decision making processes, with applications to natural hazards and infrastructures. His research interests are in risk analysis and optimisation of systems, processes and structures.

SILVIA DELGADO OLABARRIAGA is currently an Assistant Professor with the Department of Clinical Epidemiology, Biostatistics and Bioinformatics of the Amsterdam UMC, location AMC, University of Amsterdam. She leads the e-science research line, supervises Ph.D. students, and teaches courses at the AMC Graduate School and Medical Informatics Bachelor and Master Programs. She is mainly interested in the usage of advanced information technology for scientific biomedical research.

HENK MARQUERING received the Ph.D. degree from the Geophysics Department, Utrecht University, The Netherlands, in 1996. After a post-doc in Princeton University, USA, he changed careers to work at the R&D Department of Océ, currently Canon, where he worked on document image analysis. He switched between academia and industry a couple of times after which he moved to the Amsterdam UMC, Department Radiology and Nuclear Medicine, and Department of Biomedical Engineering and Physics. He is currently an Associate Professor focusing on cardiovascular imaging and image processing. He is also a co-founder of the AMC spinoff Nico.lab in which AI techniques are used to support diagnosis of stroke patients.