The Key Elements of a Risk-based Product Security Program for Medical Devices: A Scoping Study

Nadica Hrgarek Lechner
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
nhrgarek@foi.hr

Abstract. *One of the main challenges facing medical device manufacturers is to design and develop secure products and services that can successfully withstand evolving cybersecurity threats. Building security and privacy considerations into medical devices and managing privacy and security risks proactively throughout the entire product life cycle requires a structured and systematic approach.*
The purpose of this paper is to identify in the existing research literature the key elements which are needed to establish a risk-based product security program in order to protect connected medical devices, the healthcare systems, and end users who use them against cybersecurity threats. A scoping study of available IEEE Xplore database literature was used to identify the key elements which are listed in this paper.

Keywords. cybersecurity, FDA, medical devices, medical device software, privacy, product security program, security, security risk management

1 Introduction

Medical devices and digital health technologies can be truly life-changing, and in many cases, life-saving for millions of people around the world. A range of emerging technologies, wireless communication, remote connectivity, and miniaturisation, enabled the development of innovative, portable, connected, and smart medical devices that can generate, collect, analyse, and transmit health data, creating the Internet of Medical Things (IoMT) ecosystem. In general, IoMT connects various medical devices, medical equipment, biosensors, wearables, Application Programming Interfaces (APIs), and software applications to healthcare systems and services using networking technologies.

Connected medical devices (e.g., continuous glucose monitors, wearable blood pressure monitors, wearable ECG monitors, pills with ingestible sensors, smart pacemakers, smart thermometers, etc.) are becoming a cornerstone for predictive, preventive, and personalized patient care. For example, some network-connectable devices and wearables can be used at home and on the go to accurately diagnose, treat, and monitor a range of medical conditions, and to improve patient experience and patient outcomes. A research from the Deloitte Centre for Health Solutions (2018) examined how connected medical devices are transforming health care and found that medical device manufacturers face challenges to maintain the cybersecurity of their devices.

Cybersecurity concerns around the rapidly growing use of connected “things” are increasing across all sectors and the healthcare sector is no exception. In the healthcare sector, connecting medical devices and introducing new valuable digital assets expands the threat landscape and makes medical devices more vulnerable to various types of cybersecurity threats and attack vectors. The safety, security, and effectiveness of medical devices are the main concerns of global regulators, standards organizations, and healthcare delivery organizations. To address these concerns, medical device manufacturers should collaborate with key stakeholders, fully address security and privacy considerations during an early stage of design and development, and effectively manage safety, security, and privacy risks during the whole product life cycle from medical device conception to obsolescence.

If marketed and distributed medical devices do not have adequate security controls because cybersecurity risks have not been properly addressed during design and development, lack of such controls may adversely affect device functionality, disrupt the delivery of healthcare, and lead to unauthorized disclosure and the risk of multi-patient harm. Medical devices should be designed and built with cybersecurity resilience and future cybersecurity threats and vulnerabilities in mind. Therefore, building robust security into medical devices requires a clear understanding of the current and future security challenges as well as using a defence-in-depth approach to cybersecurity. The idea behind this approach is to use several, independent security mechanisms and controls in a layered fashion to protect medical devices and sensitive information.

There is a number of papers (Easttom & Mei, 2019), (Jagannathan & Sorini, 2015), (Martinez, 2018), (Mertz, 2018), (Razaque et al., 2019), (Skierka, 2018), (Tervoort et al., 2020), (v. Stockhausen & Rose, 2020) focusing on understanding cybersecurity risks and mitigating cybersecurity threats to medical devices. However, much less research (Hegde, 2018), (Wirth et al, 2020) has been made on identification of key elements which are needed to establish a risk-based product security program for medical devices. Wirth et al. (2020) identified the following five elements of a comprehensive risk-based security program for medical devices: 1) strong governance, 2) ongoing testing, 3) coordinated vulnerability disclosure, 4) SBOM (Software Bill of Materials), and 5) maturity road map. The authors provide comprehensive information about a robust medical device cybersecurity program from a broad perspective. These high-level elements are not mapped to elements of the FDA's (Food and Drug Administration) cybersecurity guidances (FDA, 2014, 2016, 2018) and broken down into smaller pieces to ensure that all key elements have been considered. Our paper attempts to identify and address this research gap in the existing literature.

The paper is organized as follows. First, we provide the research question and research methodology in section 2. Section 3 presents the results from the conducted scoping study and discussion of the findings. The final section of the paper gives a brief summary and identifies areas for further research.

2 Methodology

The aim of the research was to discover in the existing IEEE Xplore database literature the key elements which are needed to establish a risk-based product security program for medical devices. The research was guided by the following qualitative and explorative research question: What are the key elements of a risk-based product security program for medical devices?

To answer the research question, in a first step we identified key elements in one draft and one final cybersecurity guidance for medical devices issued by the FDA. FDA is a federal agency of the United States responsible for protecting the public health. These guidance documents were selected because they address management of cybersecurity in medical devices throughout the premarket phase (FDA, 2018) and the postmarket phase (FDA, 2016). Thus, the complete medical device life cycle was covered. Table 1 outlines 16 key elements of a risk-based product security program for medical devices that were identified in the FDA's cybersecurity guidances. Elements are divided into two main phases of a medical device life cycle from a regulatory point of view.

Table 1. Key elements of a risk-based product security program for medical devices according to the FDA's cybersecurity guidances (FDA, 2018, 2016) covering the entire product life cycle

Key element	Premarket phase	Postmarket phase
Cybersecurity Bill of Materials (CBOM) cross referenced with the National Vulnerability Database (NVD) or similar known vulnerability database	•	•
Analysis of threat sources	•	•
Threat modeling	•	•
Vulnerability characterization and assessment	•	•
Security risk management	•	•
Secure design architecture	•	
Security/privacy requirements	•	
Security/privacy controls	•	•
Verification, validation, testing	•	•
Relevant security information for end users	•	•
Secure supply chain	•	•
Monitoring third party software/firmware components for new vulnerabilities	•	•
Coordinated vulnerability disclosure (vulnerability intake and handling)		•
Voluntary participation in an Information Sharing Analysis Organization (ISAO) that shares vulnerabilities and threats that impact medical devices		•
Compliance with the regulatory reporting requirements		•
Software/firmware updates and patches to remediate vulnerabilities	•	•

In the next step we conducted a scoping study using the methodological framework proposed by Arksey and O'Malley (2005). The scoping study is a type of rapid literature review that can be used to identify gaps in the existing research literature. The framework for conducting a scoping study proposed by Arksey and O'Malley comprises the following stages: 1) identifying the research question, 2) identifying relevant studies, 3) study selection, 4) charting the data, and 5) collating, summarizing and reporting the results.

2.1 Identifying relevant Studies

We searched for studies about medical devices that are focused at product security and that were published in the time period from 2014 to April 2021. 2014 was chosen because the FDA released a first guidance document that addresses management of cybersecurity in medical devices throughout the premarket phase.

We collected the studies using the IEEE Xplore search engine which provides full text access to the technical literature in engineering and technology. IEEE Xplore advanced search was performed on May 2, 2021. ‘product security’, and ‘medical devices’ were searched in all metadata under the AND condition. The search resulted in a literature set consisting of total 63 studies published in the IEEE Xplore digital library. After refining the search results by excluding 4 magazines and 2 standards, the search returned 57 studies.

2.2 Study Selection

After obtaining the bibliographic data (i.e., title, abstract, author(s), publication year) and full text of 57 studies (i.e., papers) in the literature set, we reviewed all studies and manually determined eligibility for our research topic. At this point, three out of a total 57 studies were excluded from further consideration: one was a title page, one was a table of contents, and one was a list of plenary speakers.

We used the following eligibility criteria to decide whether a study was eligible for inclusion into the scoping study:

1. The text of the study must be in English language.
2. The study must be published in conference proceedings or a journal.
3. The study must contribute to the research question and apply to any type of medical device (including legacy devices and devices that are considered part of an interoperable system).
4. The study must cover the activities from the premarket phase and/or postmarket phase of a medical device.

The relevance of each study for the research topic and its eligibility was assessed based on these criteria. First, we read the title and the abstract of every study. When abstracts did not provide enough information and the study's eligibility was unclear, the full text was read.

After applying the pre-specified eligibility criteria, a total of 20 studies was found to be relevant for the research topic and was included into the scoping study. The included studies are listed in Table 2.

2.3 Charting the Data

The studies were categorized according to a medical device type and product life cycle phase by manually analysing the full text. The results are listed in Table 2. In one study (Hager et al., 2020) we identified an additional element which we named “Security/privacy education for end users and manufacturers”. This element is not explicitly mentioned in FDA’s guidances, but it should be included into key elements because general training is important to raise awareness of the end users and manufacturer’s personnel to ensure that everyone is aware of the impacts that poor security/privacy practices can have. The study from v. Stockhausen and Rose (2020) mentions the SBOM for security enhancement within the context of medical device software. SBOM lists all parts that a piece of software consists of and allows end users to be more aware of potential risks of discovered vulnerabilities in underlaying software components. For this reason, SBOM was added to an existing key element describing a similar concept. Added items are highlighted in grey colour in Table 2.

Table 2. Key elements of a risk-based product security program for medical devices

Key element	Study	Medical device type	Life cycle phase
Cybersecurity/Software Bill of Materials (CBOM/SBOM) cross referenced with the National Vulnerability Database (NVD) or similar known vulnerability database	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Analysis of threat sources	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Hariharan et al, 2021)	Wireless body area network	Premarket
	(Jagannathan & Sorini, 2015)	Hypothetical embedded	Premarket
	(Joshitta & Arockiam, 2017)	Devices in smart healthcare environment	Premarket
	(Rughoobur & Nagowah, 2017)	Battery operated IoT devices for healthcare	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket

Key element	Study	Medical device type	Life cycle phase
	(Yasin et al., 2017)	IoT platform	Premarket
	(Zhai et al., 2015)	Embedded	Premarket
	(Zheng et al., 2017)	Implantable	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
	(Wu et al., 2017)	Implantable	Premarket
Threat modeling	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(Yasin et al., 2017)	IoT platform	Premarket
	(Zhai et al., 2015)	Embedded	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
	(Wu et al., 2017)	Implantable	Premarket
Vulnerability characterization and assessment	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Zhai et al., 2015)	Embedded	Premarket
	(Zheng et al., 2017)	Implantable	Premarket
	(Zheng et al., 2019)	Implantable, wearable	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
	(Jagannathan & Sorini, 2015)	Hypothetical embedded	Premarket
	(Jagannathan & Sorini, 2016)	Medical device software (legacy device)	Postmarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
	(Wu et al., 2017)	Implantable	Premarket
Security risk management	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Jagannathan & Sorini, 2015)	Hypothetical embedded	Premarket
	(Jagannathan & Sorini, 2016)	Medical device software (legacy device)	Postmarket
	(Rughoobur & Nagowah, 2017)	Battery operated IoT devices for healthcare	Premarket
	(Shen et al., 2017)	Wireless stethoscope	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Secure design architecture	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Han et al., 2020)	Medical device software	Premarket
	(Kolasa et al., 2020)	Medical device	Premarket
	(Rughoobur & Nagowah, 2017)	Battery operated IoT devices for healthcare	Premarket
	(Saha & Anvekar, 2017)	Wireless body area network	Premarket
	(Shen et al., 2017)	Wireless stethoscope	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(Yasin et al., 2017)	IoT platform	Premarket
	(Zhai et al., 2015)	Embedded	Premarket
	(Zheng et al., 2017)	Implantable	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
	(Wu et al., 2017)	Implantable	Premarket
Security/privacy requirements	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Han et al., 2020)	Medical device software	Premarket
	(Joshitta & Arockiam, 2017)	Devices in smart healthcare environment	Premarket
	(Peng et al., 2016)	Wearable	Premarket
	(Saha & Anvekar, 2017)	Wireless body area network	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(Zheng et al., 2017)	Implantable	Premarket
	(Zheng et al., 2019)	Implantable, wearable	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
Security/privacy controls	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Hager et al., 2020)	Smart healthcare devices	Premarket

Key element	Study	Medical device type	Life cycle phase
	(Hariharan et al, 2021)	Wireless body area network	Premarket
	(Jagannathan & Sorini, 2015)	Hypothetical embedded	Premarket
	(Jagannathan & Sorini, 2016)	Medical device software (legacy device)	Postmarket
	(Joshitta & Arockiam, 2017)	Devices in smart healthcare environment	Premarket
	(Kolasa et al., 2020)	Medical device	Premarket
	(Rughoobur & Nagowah, 2017)	Battery operated IoT devices for healthcare	Premarket
	(Saha & Anvekar, 2017)	Wireless body area network	Premarket
	(Shen et al., 2017)	Wireless stethoscope	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(Yasin et al., 2017)	IoT platform	Premarket
	(Zhai et al., 2015)	Embedded	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
	(Zheng et al., 2017)	Implantable	Premarket
	(Zheng et al., 2019)	Implantable, wearable	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
	(Wu et al., 2017)	Implantable	Premarket
Verification, validation, testing	(Fernandes et al., 2018)	IoT-based health monitor	Premarket
	(Joshitta & Arockiam, 2017)	Devices in smart healthcare environment	Premarket
	(Rughoobur & Nagowah, 2017)	Battery operated IoT devices for healthcare	Premarket
	(Zhai et al., 2015)	Embedded	Premarket
	(Zheng et al., 2017)	Implantable	Premarket
	(Zhang et al., 2014)	Implantable, wearable	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Relevant security information for end users	(Jagannathan & Sorini, 2015)	Hypothetical embedded device	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Secure supply chain	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Monitoring third party software/firmware components for new vulnerabilities	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Coordinated vulnerability disclosure (vulnerability intake and handling)	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Voluntary participation in an Information Sharing Analysis Organization (ISAO) that shares vulnerabilities and threats that impact medical devices			
Compliance with the regulatory reporting requirements	(Jagannathan & Sorini, 2016)	Medical device software (legacy device)	Postmarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Software/firmware updates and patches to remediate vulnerabilities	(Jagannathan & Sorini, 2015)	Hypothetical embedded	Premarket
	(Jagannathan & Sorini, 2016)	Medical device software (legacy device)	Postmarket
	(Rughoobur & Nagowah, 2017)	Battery operated IoT devices for healthcare	Premarket
	(Supriya & Padaki, 2016)	Medical imaging	Premarket
	(v. Stockhausen & Rose, 2020)	Medical device software	Premarket, postmarket
Security/privacy education for end users and manufacturers	(Hager et al., 2020)	Smart healthcare devices	Premarket, postmarket

2.4 Collating, Summarizing and Reporting the Results

After we determined the key elements in each study, we counted the number of studies per key element to get an overview which elements are the most frequently used. The results are illustrated in Fig. 1.

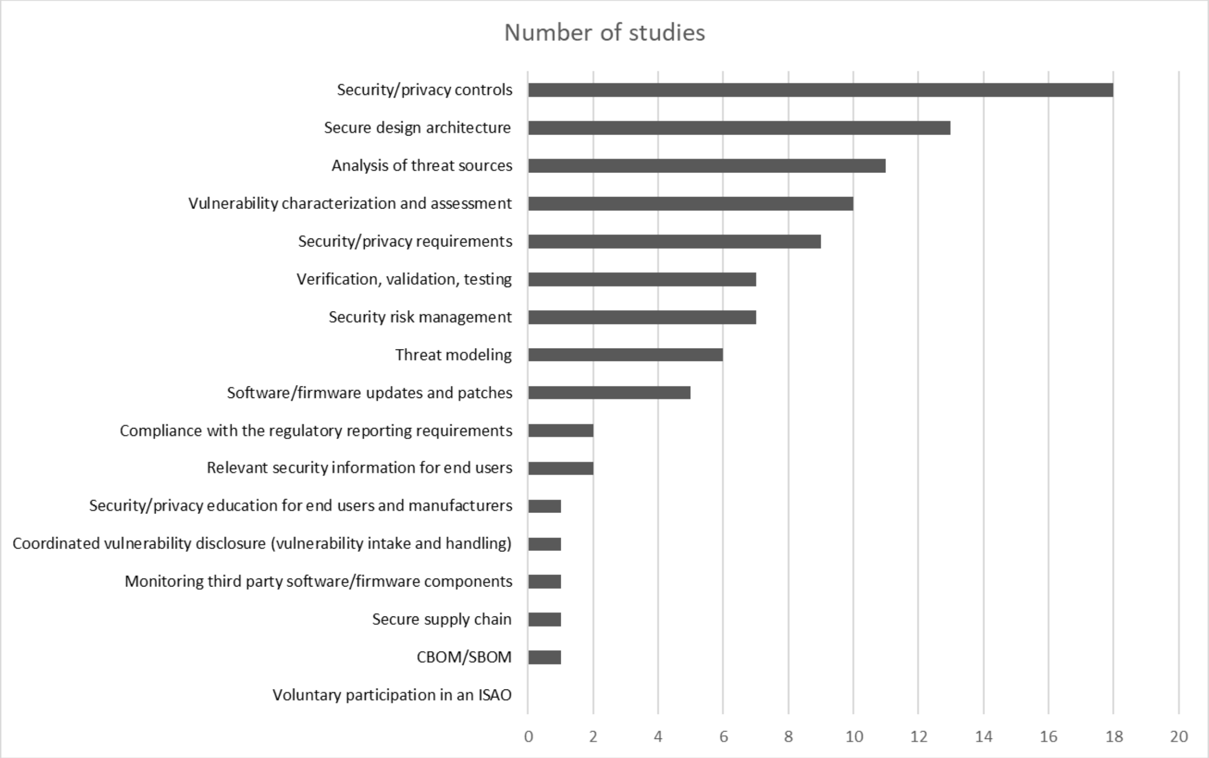

Figure 1. Number of studies per identified key elements of a risk-based product security program for medical devices

3 Results and Discussion

Table 2 shows how the 20 selected studies were categorized according to a medical device type and product life cycle phase. Selected studies cover different types of medical devices and the premarket phase is covered most frequently. Two studies cover both premarket and postmarket phases. A total of 17 key elements of a risk-based product security program for medical devices were identified. Since the majority of the studies cover the premarket phase, key elements from the premarket phase are most frequently addressed. For example, security/privacy controls are addressed by 18 of the studies as shown in Fig. 1. Voluntary participation in an ISAO such as MedISAO (https://www.medisao.com) or Health-ISAC (https://h-isac.org/) was not found in any study. At the time of research, there was quite a small number of medical device manufacturers participating in ISAOs – it is expected that future studies will address this gap. All other key elements of a risk-based product security program for medical devices were addressed in one or more studies.

To the best of the author's knowledge, this is the first scoping study that specifically identifies key elements of a risk-based product security program for medical devices. However, we must also acknowledge potentially important study limitations. The studies were collected using one research database. Future research could conduct literature searches in other academic research databases such as Scopus, Web of Science, PubMed, or ScienceDirect. Since the study selection and charting the data were conducted manually, author’s biases could have influenced the selection and classification of studies.

4 Conclusion

A robust risk-based product security program in the medical device industry needs to ensure that security and privacy considerations of a medical device are planned and built into it from its conception and that the security and privacy risks are proactively managed throughout the whole product life cycle without having a negative impact on patient health and safety. As demonstrated in this paper, there is a variety of key elements that need to be addressed and can guide a risk-based product security program for medical devices. Medical device manufacturers need to ensure translation of these elements into specific practices. We found 20 studies addressing 16 of totally identified 17 key elements of a risk-based product security program for medical devices.

This paper contributes to the existing literature on the topic of risk-based product security program for medical devices. This paper may assist scientists as well as regulatory affairs, cybersecurity, privacy, and software professionals in the medical device industry who are involved in medical device cybersecurity activities. Software engineers who develop medical devices that are subject to cybersecurity need to be aware of security and privacy risks and have specific skills such as threat modeling, cryptography, secure coding, secure code reviews, etc.

Further research should explore other global guidances that address cybersecurity across all stages of a medical device's life cycle such as the IMDRF's (International Medical Device Regulators Forum) guidance (IMDRF, 2020) and MDCG's (Medical Device Coordination Group) guidance (MDCG, 2019), and identify additional key elements that need to be considered when designing a risk-based product security program for medical devices.

References

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology*, 8(1), 19–32. doi:10.1080/1364557032000119616

Deloitte Centre for Health Solutions. (2018). Medtech and the Internet of Medical Things: How connected medical devices are transforming health care. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf

Easttom, C., & Mei, N. (2019). Mitigating Implanted Medical Device Cybersecurity Risks. *Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0145–0148). IEEE, New York, USA.

FDA. (2014). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/86174/download

FDA. (2016). Postmarket Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/95862/download

FDA. (2018). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Draft Guidance for Industry and Food and Drug Administration Staff. Retrieved from https://www.fda.gov/media/119933/download

Fernandes, A. M., Pai, A., & Colaco, L. M. M. (2018). Secure SDLC for IoT Based Health Monitor. *Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1236–1241). IEEE, Coimbatore, India.

Hager, A., Goland, T., Sapio, N., & Hurt, I. (2020). Securing private medical data, and influencing medical device design to prioritize privacy: A Systems Analysis Approach. *Proceedings of the 2020 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 1–3). IEEE, Charlottesville, USA.

Han, S., Sinha, R., & Lowe, A. (2020). Assessing Support for Industry Standards in Reference Medical Software Architectures. *Proceedings of the IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society* (pp. 3403–3407). IEEE, Singapore.

Hariharan, U., Rajkumar, K., & Ponmalar, A. (2021). WBAN for e-Healthcare Application: Systematic Review, Challenges, and Counter Measures. *Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–7). IEEE, Coimbatore, India.

Hegde, V. (2018). Cybersecurity for Medical Devices. *Proceedings of the 2018 Annual Reliability and Maintainability Symposium (RAMS)* (pp. 1–6). IEEE, Reno, USA.

IMDRF. (2020). Principles and Practices for Medical Device Cybersecurity. Retrieved from http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

Jagannathan, S., & Sorini, A. (2015). A cybersecurity risk analysis methodology for medical devices. *Proceedings of the 2015 IEEE Symposium on Product Compliance Engineering (ISPCE)* (pp. 1–6). IEEE, Chicago, USA.

Jagannathan, S., & Sorini, A. (2016). Self-authentication in medical device software: An approach to include cybersecurity in legacy medical devices. *Proceedings of the 2016 IEEE Symposium on Product Compliance Engineering (ISPCE)* (pp. 1–5). IEEE, Anaheim, USA.

Joshitta, R. S. M., & Arockiam, L. (2017). Device authentication mechanism for IoT enabled healthcare system. *Proceedings of the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)* (pp. 1–6). IEEE, Chennai, India.

Kolasa, Y., Bastogne, T., Georges, J.-P., & Kubler, S. (2020). Quality-by-Design-engineered pBFT Consensus Configuration for Medical Device Development. *Proceedings of the 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)* (pp. 5709–5713). IEEE, Montreal, Canada.

Martinez, J. B. (2018). Medical Device Security in the IoT Age. *Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 128–134). IEEE, New York, USA.

MDCG. (2019). MDCG 2019-16 Guidance on Cybersecurity for medical devices. Retrieved from https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_cybersecurity_en.pdf

Mertz, L. (2018). Cyberattacks on Devices Threaten Data and Patients: Cybersecurity Risks Come with the Territory. Three Experts Explain What You Need to Know. *IEEE Pulse*, 9(3), 25–28. doi:10.1109/MPUL.2018.2814258

Peng, G., Sepulveda Garcia, L. M., Nunes, M., & Zhang, N. (2016). Identifying user requirements of wearable healthcare technologies for Chinese ageing population. *Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2)* (pp. 1–6). IEEE, Trento, Italy.

Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. *IEEE Access*, 7, 168774–168797. doi:10.1109/ACCESS.2019.2950849

Rughoobur, P., & Nagowah, L. (2017). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. *Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)* (pp. 811–817). IEEE, Dubai, United Arab Emirates.

Saha, S., & Anvekar, D. K. (2017). A poly_hop message routing approach through node and data classification for optimizing energy consumption and enhanced reliability in WBAN. *Proceedings of the 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (pp. 788–792). IEEE, Bangalore.

Shen, S., Lin, S., Kang, T., & Chien, W. (2017). A Public-Key Protection Scheme Using in the Wireless Module of the Digital Stethoscope. *Proceedings of the 2017 International Conference on Information, Communication and Engineering (ICICE)* (pp. 228–230). IEEE, Xiamen, China.

Skierka, I. M. (2018). The governance of safety and security risks in connected healthcare. *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT – 2018* (pp. 1–12). IET, London.

Supriya, S., & Padaki, S. (2016). Data Security and Privacy Challenges in Adopting Solutions for IOT. *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 410–415). IEEE, Chengdu, China.

Tervoort, T., De Oliveira, M. T., Pieters, W., Van Gelder, P., Olabarriaga, S. D., & Marquering, H. (2020). Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review. *IEEE Access*, 8, 84352–84361. doi:10.1109/ACCESS.2020.2984376

v. Stockhausen, H., & Rose, M. (2020). Continuous security patch delivery and risk management for medical devices. *Proceedings of the 2020 IEEE International Conference on Software Architecture Companion (ICSA-C)* (pp. 204–209). IEEE, Salvador, Brazil.

Wirth, A., Gates, C., & Smith, J. (2020). *Medical Device Cybersecurity for Engineers and Manufacturers*. Boston: Artech House.

Wu, L., Du, X., Guizani, M., & Mohamed, A. (2017). Access Control Schemes for Implantable Medical Devices: A Survey. *IEEE Internet of Things Journal*, 4 (5), 1272–1283. doi:10.1109/JIOT.2017.2708042

Yasin, M., Tekeste, T., Saleh, H., Mohammad, B., Sinanoglu, O., & Ismail, M. (2017). Ultra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(9), 2624–2637. doi:10.1109/TCSI.2017.2694968

Zhai, X., Appiah, K., Ehsan, S., Howells, G., Hu, H., Gu, D., & McDonald-Maier, K. D. (2015). A Method for Detecting Abnormal Program Behavior on Embedded Devices. *IEEE Transactions on Information Forensics and Security*, 10(8), 1692–1704. doi:10.1109/TIFS.2015.2422674

Zhang, M., Raghunathan, A., & Jha, N. K. (2014). Trustworthiness of Medical Devices and Body Area Networks. *Proceedings of the IEEE*, 102(8), 1174–1188. doi:10.1109/JPROC.2014.2322103

Zheng, G., Shankaran, R., Yang, W., Valli, C., Qiao, L., Orgun, M. A., & Chandra S. (2019). A Critical Analysis of ECG-Based Key Distribution for Securing Wearable and Implantable Medical Devices. *IEEE Sensors Journal*, 19 (3), 1186–1198. doi:10.1109/JSEN.2018.2879929

Zheng, G., Zhang, G., Yang, W., Valli, C., Shankaran, R., & Orgun, M. A. (2017). From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices. *Proceedings of the 2017 17th International Symposium on Communications and Information Technologies (ISCIT)* (pp. 1–5). IEEE, Cairns, Australia.