Security-by-design challenges for medical device manufacturers

Karin Bernsmed
SINTEF Digital
Trondheim, Norway
karin.bernsmed@sintef.no

Martin Gilje Jaatun
SINTEF Digital
Trondheim, Norway
martin.g.jaatun@sintef.no

ABSTRACT

The European health care system is moving toward personalised, distributed, and home-based services, made possible via new and improved connected medical devices (CMDs). Cyber security will clearly be important in this context. In this paper we present 15 challenges that the manufacturers of CMDs face when trying to "build security in" for the devices that they produce. The challenges have been identified in a qualitative research study, including interview data from healthcare stakeholders combined with document analysis of four relevant CMD case studies.

CCS CONCEPTS

• **Security and privacy** → **Software security engineering**; • **Applied computing** → **Health care information systems**.

KEYWORDS

connected medical devices, IoT, embedded security, security-by-design, cyber security, healthcare

1 INTRODUCTION

Cyber security by design and the need to "build security in" has been recognised in the software community for decades [5], and although a large number of software security activities have been enumerated [2, 10], many developers are still either not aware of or not prioritising cyber security by design, particularly in smaller enterprises [9]. While cyber security of connected medical devices and in-vitro diagnostic devices connected to the Internet (together, CMDs) is clearly important, there is no reason to believe that the manufacturers of such devices are more aware and more willing to prioritise cyber security than the general crowd, even though the failure to do so may introduce risk, incur cost and ultimately impair the key medical purpose of delivering patient care. An investigation performed by the FBI in 2022, revealed that there is an average of 6.2 vulnerabilities per medical device, and this includes vulnerabilities in critical devices, such as pacemakers and insulin pumps [4].

In the healthcare domain, all new medical devices to be commercialised in the EU must comply with the Medical Devices Regulation (EU) (EU) 2017/746 (IVDR) (as of May 26th, 2022). To assist practitioners in complying with the regulatory requirements, the Medical Device Coordination Group (MDCG) has been established. In 2019, they published the MDCG 2019-16 guidelines on cybersecurity of medical devices [6], covering the cybersecurity requirements of both MDR and IVDR. However, whereas the MDCG guidance is useful and fit for purpose in that it distils process and general advice on how to address the cyber security requirements from multiple sources (e.g. MDR / IVDR), it does not contain specific advice on how to "build security in". For example, it says little about how the CMD manufacturers should identify threats and address risks to the devices they develop. To be in a better position to propose improvements to the MDCG guidance, and ultimately to help CMD manufacturers to produce more secure devices, we therefore decided to investigate the source of the problem. Therefore, the main research question that we strive to answer in this paper is: *What are the main cyber security challenges for manufacturers of connected medical devices*?

This paper is organised as follows. In Section 2 we present the background methodology that was followed to derive the results. The identified challenges are detailed in Section 3 and 4. Finally, discussion and conclusions are provided in Section 5.

2 METHODOLOGY

In this study, we aimed to extract in-depth information on the cyber security challenges faced by a specific stakeholder group: the CMD manufacturers. To answer the research question, we chose a qualitative research method in the form of interviews with a selected group of participants, combined with document analysis, which enabled us to perform a rich and detailed analysis of the gathered data. The selection criteria for the interviews were stakeholders with practical experience from medical device manufacturing, or integrators or operators of such devices. In total six stakeholders were interviewed, whereof three defined themselves as medical device operators, two as medical device manufacturers, and one as a medical device integrator. All six stakeholders came from companies in the European health care sector. Five of the interviewed stakeholders were part of the ongoing Horizon Europe project NEMECYS[1].

Since we wanted extract and understand the problems faced by the interviewees, rather than trying to verify our own hypotheses, we used an inductive research approach [7]. We used in-depth semi-structured interviews, which allowed us to gather data from the respondents based on their own experiences and specific situations that they had encountered. The laddering technique [11] was

---

[1]https://nemecys.eu

used during the interviews, where respondents were repeatedly asked "*why?*", with follow-up questions to understand the underlying motivations behind their perceptions and opinions. To ensure that the respondents felt comfortable during the interviews, we set up an interviewing environment that was non-threatening, and used open-ended questions to foster a sense of safety and encourage introspection. Furthermore, before starting each interview, we made it clear to respondents that their responses would be kept confidential. One researcher led the interviews, while the others mainly listened in, took notes and supplemented with questions if something was missed. We used Microsoft Teams to conduct and record the interviews. Our aim was not to seek statistical generalisations but to achieve a thorough understanding of the issues faced by the interviewed stakeholders.

The interview guide was designed to cover various aspects of the stakeholders' activities related to CMDs. It consisted of seven different sections, on the following topics. 1) Their company, the problem(s) they are trying to solve in the market, and the types of devices they manufacture or use. 2) Their company's design process for their devices and how regulation fits into the process. This section also aimed to identify potential problems that the company may face during the design, integration and operation of their devices. 3) CMD cyber security, including identifying the company's assets, worst nightmares regarding breaches/attacks/cyber security risks, and the company's current approaches and tools for securing their CMDs. 4) Whether their company offers courses or training material for employees to raise awareness about cyber security and whether they have positions dedicated to cyber security at any level. 5) Compliance with standards, regulations, and guidelines relevant for CMDs. The section explored the company's experience with the certification process, how and if they use any security guidance, and any challenges they may have faced. 6) Comparison of the security challenges in the healthcare sector compared with other sectors where similar IoT/connected devices are used, and how the company overcomes those challenges. 7) How the company prioritises the problems identified in the previous sections. As can be seen, the scope of the interview guide was wider than the research question formulated in Section 1, but for this paper we have only analysed and reported the results relevant in our context.

All the interviews lasted approximately 90 minutes. The audio files from the interviews were transcribed by OpenAI Whisper [8] running locally on one of the researchers' computer. The transcriptions were then reviewed and cross-checked against the original audio files by the researcher. The coding and analysis of the transcribed interviews were done in accordance with the recommendations provided by Saldaña [12], using the software Nvivo [1]. This process resulted in ten distinct challenges.

In addition to the interviews, we also performed a document analysis of a selected set of scenarios for developing CMDs. More specifically, the document analysis was performed by scrutinising the textual descriptions and initial risk models of the four case studies that are being used in the Horizon Europe project NEMECYS. These case studies are: 1) Development of a home dialysis system, 2) Development of a sensor system for motion disorders, 3) Development of a mobile phone based "software as a medical device", and 4) Procurement of a continuous glucose monitoring system from a third-party vendor (reflecting the common situation where a hospital acquires a medical device from a vendor with which they have no control of the development process). These four case studies represent real-world scenarios that are of particular interest to the project's industry partners. In the rest of the paper, we will refer to these four case studies as CS1, CS2, CS3 and CS4, respectively. The document analysis of these case study descriptions allowed us not only to confirm several of the ten challenges identified from the interviews, but also to identify five additional challenges that will be relevant for CMD manufacturers, but which had not been mentioned by any of the interviewed stakeholders.

3 IDENTIFIED CHALLENGES FROM THE INTERVIEWS

Here we present the ten security-by-design challenges for medical device manufacturers that we identified from the interviews.

3.1 Lack of standardised protocols for data exchange

CMDs often employ an array of different hardware and software components with varying capabilities, functionalities, and communication interfaces. The lack of a standardised set of protocols for data exchange in embedded systems was therefore identified as a daunting challenge for CMD manufacturers. Similarly, constraints typically associated with embedded systems, such as power consumption, memory limitations, and real-time processing were also identified as complicating factors. According to the interviewed stakeholders, healthcare is particularly impacted by these issues, as manufacturers struggle to create devices that can seamlessly integrate with a diverse range of healthcare systems, while hospitals are taxed with finding devices that meet their integration requirements.

3.2 Lack of testing tools for firmware

Manufacturers face difficulties testing embedded firmware due to the lack of standardised testing tools, which results in longer development times, higher costs, and lower product quality. Developing comprehensive testing tools requires specialised knowledge and expertise, which can be time-consuming and costly for small teams with limited resources. This was highlighted as a challenge by both the interviewed manufacturers. In particular, they have built their own testing pipelines, but reported that the lack of standardised test suites or standards made it hard to know "how much testing is enough". Furthermore, without standardised tools, they are forced to maintain their own test rigs, including making updates to them based on factors such as regulatory changes, which increases the burden on them.

3.3 Generation and maintenance of documentation

Generating documentation about how security has been implemented in the CMDs was identified as a challenge, mainly because of the complex nature of such implementations, which tends to make the documentation error-prone and was seen as a tedious task requiring attention to detail. Additionally, ensuring traceability

and comprehensive documentation when you do not have a good overview of what documentation is required was considered a difficult task. Both the interviewed manufactures claimed they struggle with this. Further, they both explained they had been forced to develop their own tools to generate the required documentation from their CI/CD pipelines.

3.4 Security requirements from the hospitals

An interesting point raised by both the interviewed medical device manufacturers and by the medical device operators was that most hospitals do not manage to formulate clear requirements in terms of cyber security for medical devices. From the manufacturers' point of view, this makes it difficult to define proper security requirements for their devices; for example, they have to guess how statements such as "we are concerned about security" should be translated into technical requirements. The operators' point of view was also interesting here; one of the interviewees explained that even though their hospital has strong security and integration requirements, as it is a paperless hospital, this may not be the case in other hospitals. A typical example is devices which require a private VLAN to function, which induces bad integration and difficult monitoring of the device for the hospital. The lack of "demand" for security features means that manufacturers will also not invest a lot in it and will prioritise other features. Overall, the market still seems immature from a cyber security perspective.

The interviewed manufacturers also highlighted an additional challenge in the development and integration of CMDs: the strict security requirements imposed by hospitals. This may seem contradictory to what is written in the paragraph above, but there is a subtle difference. While the previous paragraph emphasises the lack of clear security requirements manufacturers get from hospitals when manufacturing CMDs, this new insight sheds light on the difficulties manufacturers face in meeting the rigorous security standards set by hospitals when they have a product. The difference lies in the gap that exists between the strict security requirements hospitals systems usually have, versus the lack of clear security requirements they seem to communicate to the manufacturers of their CMDs.

3.5 Deployment scenarios and architecture

When developing a new medical device, manufacturers have to consider how it will be deployed after it has been delivered. The interviewed manufacturers considered this as a major hurdle, since they rarely know how their devices will be integrated in the target systems. Often there are numerous ways to use the device, with different use cases requiring varying integration methods. For example, in one use case the device may require the manufacturer's gateway and cloud, while another may involve using their gateway to push data to the hospital EMR (Electronic Medical Record) system, and a third may require a 3rd party gateway provided by a system integrator. These complexities create security challenges, particularly when additional features, such as roaming between gateways or the use of an optimised communication protocol to reduce battery usage, are factored in. One interviewee commented that the healthcare industry faces integration issues similar as in smart home solutions, where many different products are integrated

into one or more gateways. However, the stakes are higher here, as patient safety and the security of their medical data are paramount. The interviewed medical device integrators also highlighted the difficulty of getting data *into* the hospital system, which is not as straightforward as retrieving it *from* a monitoring device, because of the strict rules hospitals might apply.

3.6 Trade-offs between security and other properties

Several of the interviewed stakeholders also highlighted the different trade-offs that had to be made. Security versus usability was mentioned as a typical example. One interviewee claimed that healthcare professionals often prefer solutions that are easy to use, without considering security. Security measures, such as strong user authentication, can therefore make the technology less user-friendly and seen as too time-consuming from the healthcare professionals perspective. Conversely, prioritising usability over security can compromise patient data confidentiality and expose healthcare facilities to cyber threats.

Further, cost was also mentioned as a trade-off by the interviewed stakeholders. Security is frequently perceived as an expendable cost that can be easily cut rather than an essential investment, primarily because its benefits are not directly visible in improving patient care. The financial resources allocated towards enhancing security could alternatively be used to recruit additional medical staff, such as nurses or doctors, thus making the choice difficult and posing a challenging dilemma. In the public sector, the argument for fostering security is even less strong, further complicating the matter and decision-making processes. The lack of a widely recognised return-of-investment for security measures underlines the complexity of achieving an effective balance between cost and security when manufacturing devices for the healthcare sector

Finally, the interviewed medical device operators also mentioned the quality of the healthcare as a trade-off. The clinical aspects of healthcare always take priority, and patient care should be prioritised above other considerations, including privacy or security. While physicians may be aware of security issues, they may not have the time or resources to undergo extensive security training as their priority always is to treat their patients. Additionally, if a device provides excellent patient care but lacks security features, it will be prioritised over a secure device that does not have the same functionalities. This trade-off can create challenges for the manufacturers, as they need to consider both patient care and security needs when they design their products.

3.7 Race to market

The need for speed was also identified as a challenge. Particularly for small manufacturers, the risk of losing their first mover advantage can be crippling. Approval and certification requirements mean that it can take months, or even years, before the manufacturer can begin selling their medical devices in a certain market, and larger competitors could therefore leapfrog them in this time. This implies that it is easy to overlook aspects that do not directly impact the clinical approval, and unfortunately this means that security often suffers.

3.8 Complex routes to certification

Another identified challenge was the complexity of the certification process. The interviewed manufacturers both explained that there are many ways to get a device certified by the US Food and Drug Administration (FDA), depending on how novel it is. For instance, if a device is equivalent to an existing product already on the market, there is a fast-track option available. However, if it is novel, the bar is set higher, making it more difficult to get certified because you have to prove everything about the novel product from scratch. This variability in the certification process can cause confusion for manufacturers and may delay the release of innovative devices.

In addition, the manufacturers also highlighted the lack of a unified process for certification as a major obstacle. Specifically, there are different processes for certification in Europe and the US, with the MDR and the FDA, respectively. The MDR does not have a fast-track route, which means that manufacturers must submit all evidence that the device works as intended. This variation in the certification processes creates additional complexity and uncertainty for manufacturers, making it difficult for them to operate in multiple markets and increase the time and cost of certification.

3.9 Applying standards in practice

Both the interviewed manufacturers and operators agreed that applying standards in practice is difficult. They explained that it is often very challenging to transfer the generic high-level requirements in a standard into concrete requirements for their products. In particular, it is difficult for the manufacturers to know where the bar has been set, in terms of security, especially if it is their first time they implement a particular standard. Standards can be open to interpretation, which some interviewees believed is done on purpose to avoid constraining companies too much, particularly the larger companies that often already have a good process in place.

3.10 Documenting the state of the art

Finally, the interviewed manufacturers reported that the regulatory requirement to perform a state-of-the-art survey for each new device is a real challenge for them. According to the regulations, manufacturers are required to perform such a survey to ensure that their devices meet the required security standards. However, the interviewees highlighted that the task of compiling the survey seems unnecessary and could instead be done by a governmental body, thereby saving resources and reducing the burden on manufacturers. Moreover, performing a state-of-the-art survey is a significant challenge for start-ups and SMEs, which often lack the necessary resources for such activities. The cost and effort can be significant, thereby creating a barrier for smaller companies looking to develop innovative medical devices.

The CMD manufacturers also mentioned that they need to relate to a large number of standards, regulations and guidelines, and unfortunately these are not always internally consistent. They reported that frustration often occurs, for example when a recommended guideline refers to other documentation which turns out to be obsolete.

4 IDENTIFIED CHALLENGES FROM THE CASE-STUDIES

Here we present the five security-by-design challenges for medical device manufacturers that we identified when analysing the case-studies.

4.1 Post-market surveillance

The first two case studies from the project (CS1 and CS2) that were analysed shed light on an additional key challenge that many CMD manufacturers may face: ensuring the secure post-market surveillance of their product to verify usage according to the intended purpose, while also being able to collect feedback from users. Once a medical device is released to the market, this case study showed that it will be essential to monitor its performance and gather information on any potential risks or issues that may arise during usage. This will be a crucial step in ensuring patient safety and compliance with regulatory requirements. However, this process may also involve the collection of sensitive personal data (patient data), which needs to be handled securely and in compliance with applicable data protection regulations.

4.2 Uncontrolled environments

Often, medical devices are installed and used in the patients' own homes where they can be subject to theft, tampering, destruction or other similar threats, performed by either the patient itself or by someone else with physical access to the device. Securing the device in uncontrolled environments was therefore identified as a challenge when analysing the three case studies CS1, CS2 and CS3, which show how vulnerabilities can be exploited to gain unauthorised access to confidential information (included, but not limited to, sensitive patient data) or to perform unauthorised modifications or deletion of device software or firmware.

4.3 Vulnerabilities and external dependencies

Both case study CS1 and CS2 highlighted the challenges posed by the potential vulnerabilities in source code and libraries. Both case studies showed that such vulnerabilities can be exploited by attackers to perform malicious activities such as modifying, deleting or stealing data. In addition, vulnerabilities could lead to system crashes or disruptions, which could have serious consequences in the healthcare sector. Keeping all libraries and software components up to date, as well as keeping track of newly discovered vulnerabilities, is a therefore a daunting challenge for the manufacturers.

4.4 Protection against privacy leaks, data poisoning and malware

Closely related to the previous challenge is the need for securing the devices against exploitation of identified vulnerabilities. In case study CS3, the use of the associated mobile application may raise privacy concerns for the patient. The use of the app itself may reveal that the user has been diagnosed with Parkinson's disease, which may have unintended consequences such as discrimination or stigmatisation. The challenge is to strike a balance between the

need for patient privacy and the need for effective disease management using technology. In case study CS2 the need to protect the device against data poisoning was identified. In one of the identified scenarios, an attacker could inject malicious data into the device, leading to an inaccurate diagnosis or treatment plan. Finally, the fourth case study (CS4) highlighted the challenge of protecting systems from malware. In a healthcare setting, malware can be particularly dangerous, as it can compromise the confidentiality, integrity, and availability of sensitive patient information. It can also compromise the performance and reliability of medical devices, leading to potential patient harm. Protecting against malware requires a multi-layered approach, including implementing security controls such as firewalls, intrusion detection and prevention systems, anti-malware software, and access control mechanisms. It also involves keeping software and systems up to date with the latest patches and security updates. All measures can be tricky and costly to implement in the context of embedded systems.

4.5 Cyber security watch

Finally, the second case study (CS2) highlighted the importance of having up-to-date tools to notify those manufacturers who are responsible also for maintaining their devices after deployment about evolving cyber security risks. Without proper knowledge and tools, it will be difficult for the manufacturers to stay ahead of potential threats and to take the necessary actions to mitigate them.

5 DISCUSSION AND CONCLUSION

In this paper, we have presented 15 challenges that the manufacturers of CMDs face when trying to "build security in" for the devices that they produce. Table 1 shows a mapping of the challenges to their source of information. As can be seen, the analysis of the case studies also confirmed several of the challenges identified from the interviews.

To overcome these challenges, the Horizon Europe project NEMECYS aims to benefit CMD manufacturers in their efforts to develop cyber secure devices. The project takes a three-fold approach, where manufacturers will be helped to (1) comply with relevant healthcare regulations by providing recommendations for best practice and guidelines for cyber security by design, along with compliance assurance tooling; (2) to be able to apply proportionate cyber security (too little security risks exposure, too much is costly and can obstruct clinical care) by providing a risk-benefit scheme to address cyber security risk balanced with clinical benefit; and (3) to build in cyber security by design for both their devices and the connected scenarios they operate in, by providing a set of specific tools that address the challenges identified and presented in this paper.

Regarding validity of the results, qualitative findings are highly context- and case dependent, and this is also true for our study. We interviewed six stakeholders, whereof only two came from organisations that are actually *manufacturing* medical devices. While the remaining four came from the same industry, where they were involved in either integration and/or operation of such devices, the fact that they did not produce the devices themselves, is likely to have influenced the results, at least to some degree. Still, all

four claimed to have good insights in the challenges that "their" manufacturers face, and we therefore believe their opinions are a valuable contribution to the results. Further, common criticisms to case studies, which also apply to our study, are uniqueness, difficulty to generalise the results, and the introduction of bias by the participants and/or the researchers [3]. We recognised these as potential limitations of our results, and will therefore, in the next step, broaden our study by performing a second round of data collection from a larger group of CMD stakeholders, and by evaluating the relationships between our findings and relevant literature.

In our study, we have focused on challenges that are relevant for CMD manufacturers, but it is important to keep in mind that cyber security does not stop when the devices have been produced and released into the market. Most notably, additional challenges will arise when the devices are integrated into existing healthcare systems, and when they are operated in their use case scenarios. While the focus in this paper is on manufacturers specifically, the three-folded approach for cyber secure CMDs applied in the NEMECYS project will also include recommendations, risk assessment schemes and tools for medical device integrators and medical device operators.

REFERENCES

[1] Alfasoft. 2024 (accessed April 5th, 2024). *Nvivo - Qualitative Datenanalyse leicht gemacht.* Alfasoft GmbH. https://www.nvivo.de/en/
[2] Jamie Boote, Eli Erlikhman, Stephen Gardner, and Sammy Migues. 2022. BSIMM13 Foundations report. https://bsimm.com
[3] Daniela S Cruzes and Lotfi ben Othmane. 2017. Threats to validity in empirical software security research. In *Empirical research for software security.* CRC Press, Boca Raton, FL, USA, 275–300.
[4] Federal Bureau of Investigation. 2022. Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities. Private Industry Notification 2022912-001.
[5] Gary McGraw. 2004. Software security. *Security & Privacy, IEEE* 2, 2 (Mar 2004), 80–83. https://doi.org/10.1109/MSECP.2004.1281254
[6] Medical Device Coordination Group. 2020. MDCG 2019-16 - Guidance on Cybersecurity for medical devices. https://ec.europa.eu/docsroom/documents/41863
[7] Briony J Oates. 2006. *Researching Information Systems and Computing.* Sage Publications Ltd., London, UK.
[8] OpenAI. 2024 (accessed April 5th, 2024). *OpenAI Whisper.* OpenAI. https://openai.com/research/whisper
[9] Hela Oueslati, Mohammad Masudur Rahman, Lotfi ben Othmane, Imran Ghani, and Adila Firdaus Bt Arbain. 2016. Evaluation of the challenges of developing secure software using the agile approach. *International Journal of Secure Software Engineering (IJSSE)* 7, 1 (2016), 17–37. Publisher: IGI Global.
[10] OWASP. 2020. Software Assurance Maturity Model (SAMM). https://owaspsamm.org/
[11] Thomas J Reynolds and Jonathan Gutman. 1988. Laddering theory, method, analysis, and interpretation. *Journal of advertising research* 28, 1 (1988), 11–31.
[12] David Wicks. 2017. The Coding Manual for Qualitative Researchers (3rd edition)The Coding Manual for Qualitative Researchers (3rd edition) Johnny Saldaña Sage 2015 ISBN-13: 978-1473902497. *Qualitative Research in Organizations and Management: An International Journal* 12 (06 2017), 169–170. https://doi.org/10.1108/QROM-08-2016-1408

Table 1: Mapping the identified challenges to their source of information.

Challenge	Identified in				
	Interviews	**Document analysis**			
		CS1	CS2	CS3	CS4
1: Lack of standardised protocols for data exchange	X				
2: Lack of testing tools	X	X	X		
3: Generation and maintenance of documentation	X				
4: Security requirements from the hospitals	X			X	
5: Deployment scenarios and architecture	X			X	
6: Trade-offs between security and other properties	X			X	X
7: Race to market	X	X	X	X	
8: Complex routes to certification	X	X	X		
9: Applying standards in practice	X	X	X		
10: Documenting the state of the art	X	X	X		
11: Post-market surveillance		X	X		
12: Uncontrolled environments		X	X	X	
13: Vulnerabilities and external dependencies		X	X		
14: Privacy leaks, data poisoning and malware			X	X	X
15: Cyber security watch			X		