Architecture for Self-protective Medical Cyber-Physical Systems

Michael Riegler[1(✉)], Johannes Sametinger[1], and Jerzy W. Rozenblit[2]

[1] LIT Secure and Correct Systems Lab and Institute of Business Informatics, Johannes Kepler University Linz, Linz, Austria
{michael.riegler,johannes.sametinger}@jku.at
[2] Department of Electrical and Computer Engineering and Department of Surgery, University of Arizona, Tucson, USA
jerzyr@arizona.edu
https://www.jku.at/en/lit-secure-and-correct-systems-lab, https://www.se.jku.at, https://ece.arizona.edu

Abstract. The *Internet of Medical Things* (IoMT) promises to improve patient care and the efficiency of *Medical Cyber-Physical Systems* (MCPSs). At the same time, the connectivity increases the security risk. We aim to model *Self-protective MCPSs* to reduce the attack surface during runtime. Even under attack, these systems require to provide clinical function for the patients. Monitoring vulnerabilities and suspicious behavior and sharing attacker information contributes to improved security and can be the foundation for automated actions for healthcare delivery organizations. Switching between context-aware security modes provides a flexible way to protect online and offline IoMT and increase patient safety. This paper presents our ongoing work to make healthcare systems more secure. We show current security and privacy challenges, discuss how self-protective systems can overcome them, and what role IoMT devices play in that context.

Keywords: Self-Protection · Medical Cyber-Physical Systems · Internet of Medical Things · Security · Mode Switching

1 Introduction

COVID-19 has pushed the development and usage of *Internet of Medical Things* (IoMT) devices. In critical times of lockdowns, such interconnected medical devices combined with medical sensors, actuators, applications, and services allow remote medical care delivery and reduce in-person visits. IoMT includes wearable medical devices to monitor blood pressure, heart rate, glucose, and other measures for chronic diseases, medicine pumps, fall detection sensors, remotely accessible medical implants, and connected clinic and hospital devices up to remote robotic surgical assistants. According to Statista [29], the global market value of IoMT will reach over 260 billion US dollars in 2027. However,

G. Kotsis et al. (Eds.): DEXA 2023 Workshops, CCIS 1872, pp. 57–66, 2023.
https://doi.org/10.1007/978-3-031-39689-2_6

these advantages in technology and connectivity are not restricted to lockdowns. IoMT supports the ideas of *telehealth* and *telemedicine*. Keeping track of vital signs 24/7 with remote monitoring provides more details than a brief office visit and improves personalized diagnosis. More data and information enhance patient-doctor communication. Compared to manual alerts from traditional personal emergency response systems, IoMT devices can automatically alert medical personnel if something happens, e.g., a specific value falls below or exceeds a pre-defined threshold.

Despite this positive outlook, *Medical Device Manufacturers* (MDMs), *Healthcare Delivery Organizations* (HDOs), and patients must consider the inherent risks associated with this technology. Remote monitoring and control can increase patients' quality of life but also pose potential threats. According to Claroty [7], IoT vulnerability disclosures increased by 57% in the first half year of 2022. The FBI [12] warns HDOs about unpatched and outdated medical devices. IoMT can directly or indirectly influence patients' conditions. According to Ajagbe et al. [1], security is one of the major challenges of IoMT. It is difficult to monitor and keep devices up to date for a lifetime of up to ten years. If a component breaks down or multiple connections cause a deadlock, the clinical function of the device should still be operational.

In our previous work [31,33], we implemented context-aware security modes for medical devices and switched them based on vulnerability scores. For example, *Mode 0* provided core functionality and *Mode 1-3* extended functionality like remote monitoring and control. We have focused on securing single devices such as pacemakers or insulin pumps. Switching modes provides a method to reduce the attack surface. However, in light of the increasing number of IoMT, protecting and securing them requires a broader focus than that of a single device, as we have shown for IoT devices in [32]. As the devices are networked, this can also be used for security purposes. Some anomalies and attacks can be detected only or easier with multiple IoMT devices and a central control component.

In this paper, we propose the design of a *Self-protective MCPS*. We extend our previous work with a client-server perspective, multiple IoMT devices, and an *Intrusion Detection and Prevention System* (IDPS). Our work aims to resiliently protect patients, MCPSs, IoMT devices, and the environment by monitoring and automatically adapting when anomalies occur or vulnerabilities become known. Security and reactions to attacks is necessary on multiple layers. Depending on IoMTs' context, e.g., the connection state (online/offline), the reaction can be less or more restrictive.

The paper is structured as follows. In Sect. 2, we discuss related work. We describe the security and privacy challenges of MCPS and how to deal with them in Sect. 3. We present our proposal for a *Self-protective MCPS* architecture in Sect. 4. In Sect. 5, we show a sample scenario and discuss the implications in Sect. 6. Finally, we draw our conclusions in Sect. 7.

2 Related Work

In their vision of autonomic computing, Kephart & Chess [22] consider the concept of self-protection. In contrast to manually detecting and recovering from

attacks by IT security professionals, self-protective systems can automatically defend against attacks, provide early warning, and attack mitigation methods. Likewise, self-healing capabilities [5] can enable systems to recover from attacks and reestablish functionalities. *Feedback* or *closed-loop systems* work similarly. Hellerstein et al. [19] consider feedback and sensor values to adapt systems to a goal without human intervention.

Our research builds up on the trustworthy multi-modal design for life-critical systems by Rao et al. [28]. They suggest decomposing systems into several modes facing different security risk values. Modes are switched based on events, system changes, or environmental changes related to risk values. While their focus during runtime is risk assessment for single devices, we consider sharing attacker information to prevent further attacks on other devices.

In the context of trustworthy secure systems, Ross et al. [34] suggest modes to encounter disruptions, hazards, and other threats. They describe modes for initialization, normal/operation/runtime, alternative, degraded, secure, standby, maintenance, training, simulation, test, recovery, shutdown/halted, and others. Each mode has its behavior, security configuration, and defined transitions to other modes. In addition, the German Federal Office for Information Security [4] differentiates among modes for medical operation, configuration, and technical maintenance in their cybersecurity requirements for network-connected medical devices.

3 Security and Privacy Challenges

Challenges in the medical domain have been addressed and discussed by several authors. The challenges include confidentiality, integrity, availability, reliability, safety, privacy, secure communication, software and hardware aspects, intrusion detection and reaction, formal methods, resource constraints, non-technical aspects, and organizational and regulatory issues [1,9,20,21,35,37,39].

The *NIST Cybersecurity Framework* [2] is a good starting point for these challenges. Based on existing standards, guidelines, and practices, it helps to manage and reduce cybersecurity risks with five core functions: *Identify, Protect, Detect, Respond, and Recover*. NIST also provides guidelines for foundational activities for IoT device manufacturers and a cybersecurity capability core baseline [10,11].

In the USA, the *Food and Drug Administration* (FDA) provides reports, white papers for threat modeling, incident response, off-the-shelf software, patient communication, and guidance for pre- and postmarket cybersecurity and quality system considerations in medical devices [14,17]. In the EU, the *Medical Device Coordination Group* provides guidance to fulfill the regulatory requirements [23]. The US Presidential Executive Order 14028, "Improving the Nation's Cybersecurity", pushed US agencies like the FDA to enhance cybersecurity and software supply chain security [38]. One result was the *Cybersecurity Modernization Action Plan* [18], which considers a zero trust approach, promotes best practices for secure development, and how to utilize *Artificial Intelligence/Machine Learning* (AI/ML) technologies for detection and response. In this paper, we

focus on the challenges of *Reliability and Availability*, *Safety*, and *Malware and Intrusion Detection* and *Reaction*.

4 Self-protective MCPS Architecture

MCPS and connected IoMT devices should be designed to detect and respond to anomalies and potential cyberattacks and recover from them. Therefore, MDMs and HDOs need a more comprehensive view than just monitoring single devices. Considering events of multiple IoMT devices provides a better overview and reduces false positives. Additionally, the reaction to attacks can be implemented on multiple layers of the *Self-Protective MCPS*.

Figure 1 shows our proposed architecture. We follow the principle of divide and conquer and want to utilize a distributed MAPE-K loop, as presented in [32]. Decisions are made as de-centralized as possible and centralized as necessary. A *Manager* application will use its *Inventory* to continuously monitor connected *IoMT devices* to provide enhanced visibility and situational awareness for the *Operator*. The *Operator*, like an IT security professional, can analyze the situation and plan and execute adaptations to reach the system goals. For efficiency, repetitive tasks and decisions can be partially or fully automated. Additionally, the *Manager* centrally monitors *Common Vulnerabilities and Exposures* (CVEs), medical advisories, safety communications, product alerts, warnings, recalls, and other events of public databases, as we presented in our previous work [31,33]. Based on that, the *Manager* can automatically send adaptation requests to IoMT devices to change their behavior, e.g., block IP addresses or switch their mode. Likewise, the *Operator* and the *Patient* can do that manually.

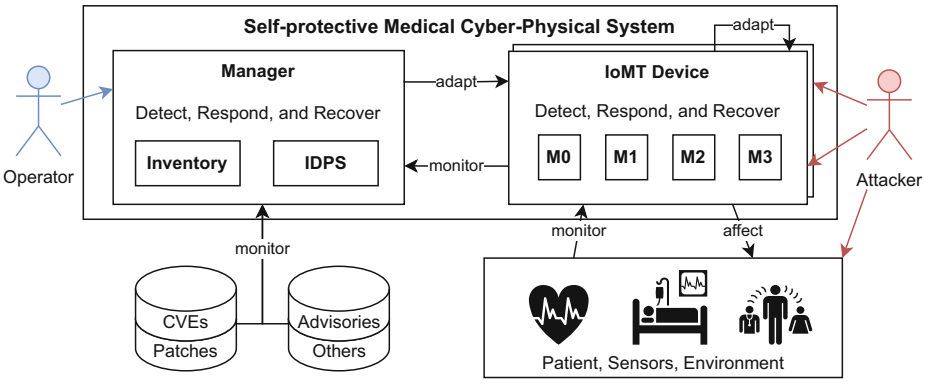

Fig. 1. Self-Protective Medical Cyber-Physical Systems Architecture.

Attackers can attack the *Self-Protective MCPS* on the hardware, software, and network layer. Therefore, anomaly and attack detection and reaction must be implemented on multiple levels. For example, trained deep autoencoder models

on typical non-malicious network packets/flows can help to detect anomalous traffic [30]. *IoMT devices* monitor and affect their environment: the patient, attached sensors, and actuators. If IoMT devices are online, they can send data to the connected *Manager* and forward information and decisions about further actions. Depending on the configuration, the *Manager* automatically decides, or an *Operator* (human-in-the-loop) decides on further steps. If an IoMT device is offline, it has to make decisions on its own and adapt itself if necessary. Predefined rules and actions on the IoMT device help to achieve that. Additionally, software and hardware window watchdog timers may help to reset the system or components if the software crashes or hangs from a denial of service attack [36]. The ultimate goal is to provide clinical function while reducing the attack surface. To reach this goal, we leverage the multi-modal architecture by [31] and extend it with an IDPS, a lightweight version on the *IoMT devices*, and a more extensive version on the *Manager*.

For example, attackers who try to crack passwords, login credentials, and encryption keys can be blocked after multiple wrong attempts with local firewall rules. However, if these attacks reach a specified amount, affect availability, or lead to battery depletion, the IoMT device may adapt itself and switch to a more restrictive mode. We suggest a low-power mode with limited functions to extend battery life and reduce the attack surface. An activity sensor or timer can trigger switching to a mode with more functionality. During the connection of the IoMT device with the *Manager*, switching to the high-security mode may provide an encrypted channel and make the device more resistant. In case of an attack, devices switch to degraded or failure mode, and self-healing capabilities [5] can enable systems to recover from attacks.

5 Sample Scenario

Self-protective MCPSs can be used in hospitals and at home for patients with chronic diseases like diabetes. Typically, such systems for *Automated insulin delivery* (AID) work partly or fully automated [25]. They consist of wearable devices to monitor vital signs, continuous glucose monitors, wireless connected medicine pumps, and handheld devices or smartphones for local control and connection to the HDO. Based on device settings, patient history, and the current condition, the handheld analyzes the data and may adapt the settings. For example, if the blood glucose level changes, the system decides to increase or decrease the dose of medication. Within a specific threshold, this process is automated as a closed loop. A closed-loop system automatically considers feedback and sensor values to adapt to the system goal without human intervention [3]. There exist several commercial and non-commercial AID systems. In 2016, Medtronic MiniMed 670G was the first FDA-approved commercial AID system [13]. Before 2016, some affected patients did not want to wait any longer and developed *Do-It-Yourself* closed-loop implementations and provided them open source, but, needless to say, without warranty. According to Dana Lewis and the OpenAPS Community [8], over 2700 people still use this solution.

In our context of IoMT, the closed-loop scenario is extended with information transfer to the HDO for remote monitoring and reconfiguration by a physician, as described in Rao et al. [27]. Using asymmetric cryptography protocols for command and control messages, e.g., signed with a unique public key of each IoMT device, can secure communication [40]. If a measured value is outside pre-defined thresholds or if certain sequences of commands are unusual and potentially cause physical damage, cf. Stuxnet [6], or potentially harm patients, the *Operator* (human-in-the-loop) will get a notification. Then the data can be reviewed and affected settings adapted, e.g., switching from mode M1 to M0.

We had a closer look at the Medtronic MiniMed 600 series and its vulnerabilities and analyzed how a *Self-protective MCPS* would be beneficial. In 2022, Medtronic [24] alerted patients about a vulnerability in the protection mechanism in their MiniMed 600 series: Exploitation could compromise communication, allow unauthorized users to change the insulin delivery, and could "potentially lead to seizure, coma or death". According to the FDA recalls [15,16], over 600 000 products in commerce were affected. The company recommended that patients should manually turn off the "Remote Bolus" feature on the pump, which was on by default. Using our *Self-protective MCPS*, we would have simplified this step for patients. The insulin pump would have a connected and disconnected mode. In the disconnected mode, the pump works offline and considers only pre-defined presets. Additionally, manual changes using the switches on the physical hardware are possible. The disconnected mode is also the fallback mechanism if the connection to other devices gets lost. In the connected mode, the pump would consider the information of connected sensors and automatically adapt the medication dose. The *Manager* would have recognized the vulnerability, notified the *Operator*, and may suggest actions to adapt the IoMT devices, like installing patches or updates or switching from the connected to the disconnected mode. Using the inventory would allow the *Operator* to notify patients directly at the device and obtain consent before executing the interventions. If no update is available and the patient safety risk is too high, we would switch devices to the disconnected mode. Additionally, security-concerned patients could manually switch from the connected to the disconnected mode in general or as needed, for example, when they are away from home. In the successor product MiniMed 770G, Medtronic [26] included the auto and the manual mode to provide similar functionality.

Another recommendation of the MDM [24] was to connect or link devices only in private places. Switching to a connected and protected mode would be beneficial after the system's initial setup. Only pre-defined connections to trusted devices are allowed in this mode, but no new ones to reduce the attack surface. Additionally, the lightweight IDPS on the IoMT device could analyze the traffic and data from connected devices, notify the *Patient* and the *Operator* about abnormal behavior, and automatically delete the suspicious device from the trusted list. Sharing information about potential attacks like wrong connection attempts or abnormal behavior will enrich the security visibility for the *Operator*. For example, if an attacker tries to attack multiple IoMT devices,

the *Manager* could recognize that, inform the *Operator*, and automatically warn other devices to increase the monitoring or to adapt security settings, e.g., by switching modes.

6 Discussion

Turning off the main features of healthcare systems is never an easy step and must only be considered as a last resort. *Self-protective MCPSs* can be a way to overcome this situation. Instead of just having the option to turn on and off devices, the availability of multiple modes provides more flexibility. A central *Manager* can allow HDOs to communicate with connected IoMT devices, analyze the security situation, notify patients (in specific cases), provide patches, and adapt IoMT device settings. Modes and mode switching, in turn, can pose new risks. We must take precautions so that malicious insiders cannot get control of the *Manager* and harm patients from this end. Thus, both technical and organizational security measures are essential.

The monitoring and control options are limited if the IoMT device has no connection to the *Manager*. A lightweight IDPS on IoMT devices can be beneficial by blocking suspicious traffic. However, in case of incorrect or faulty detection, this can lead to limited functionality. Another aspect results from the autonomy of *Self-protective MCPSs* itself. In highly automated scenarios, some serious events may remain undetected in the abundance of data and blind trust in the system.

7 Conclusion

Healthcare systems with connected IoMT devices pose many security threats and have to address several security and privacy challenges. We suggest taking advantage of their interconnected topology. Analyzing and correlating issues from multiple IoMT devices reveal anomalies and attacks that one device would not have recognized. In our *Self-protective MCPS* architecture, a central manager with an intrusion detection and prevention component can take over work from IoMT devices, analyze issues, and automatically take actions to adapt devices and prevent further attacks. Additionally, lightweight components on the IoMT devices can mitigate attacks if the device is offline. Our sample scenario has provided a first impression. We are now in the process of implementing our proposed architecture to experiment and simulate how it reacts to different attacks.

Acknowledgement. This work has partially been supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria, the Austrian Marshall Plan Foundation, and the National Science Foundation under Grant Number 1622589 "Time-Centric Modeling of Correct Behaviors for Efficient Non-intrusive Runtime Detection of Unauthorized System Actions." Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the supporting organizations.

References

1. Ajagbe, S.A., Awotunde, J.B., Adesina, A.O., Achimugu, P., Kumar, T.A.: Internet of Medical Things (IoMT): applications, challenges, and prospects in a data-driven technology. In: Chakraborty, C., Khosravi, M.R. (eds.) Intelligent Healthcare. Springer, Singapore (2022). https://doi.org/10.1007/978-981-16-8150-9_14
2. Barrett, M.: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. No. NIST CSWP 04162018, U.S. National Institute of Standards and Technology (NIST), Gaithersburg, MD (2018). https://doi.org/10.6028/NIST.CSWP.04162018
3. Boughton, C.K., Hovorka, R.: New closed-loop insulin systems. Diabetologia **64**(5), 1007–1015 (2021). https://doi.org/10.1007/s00125-021-05391-w
4. BSI: Cyber Security Requirements for Network-Connected Medical Devices. German Federal Office for Information Security (BSI) (2018). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/Medical_Devices_CS-E_132.html. Accessed 28 Dec 2022
5. Carreon-Rascon, A.S., Rozenblit, J.W.: Towards requirements for self-healing as a means of mitigating cyber-intrusions in medical devices. In: 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1500–1505 (2022). https://doi.org/10.1109/SMC53654.2022.9945507
6. Chen, T.M., Abu-Nimeh, S.: Lessons from Stuxnet. Computer **44**(4), 91–93 (2011). https://doi.org/10.1109/MC.2011.115
7. Claroty: State of XIoT Security Report (2022). https://claroty.com/press-releases/iot-vulnerability-disclosures-grew-57-percent-from-2h21-to-1h22. Accessed 28 Dec 2022
8. Lewis, D., The OpenAPS Community: OpenAPS Outcomes (2022). https://openaps.org/outcomes/. Accessed 10 Jan 2023
9. Elhoseny, M., et al.: Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. Sustainability **13**(2121), 11645 (2021). https://doi.org/10.3390/su132111645
10. Fagan, M., Megas, K.N., Scarfone, K., Smith, M.: Foundational cybersecurity activities for IoT device manufacturers. No. NIST IR 8259, U.S. National Institute of Standards and Technology (NIST), Gaithersburg, MD (2020). https://doi.org/10.6028/NIST.IR.8259
11. Fagan, M., Megas, K.N., Scarfone, K., Smith, M.: IoT device cybersecurity capability core baseline. No. NIST IR 8259A, U.S. National Institute of Standards and Technology (NIST), Gaithersburg, MD (2020). https://doi.org/10.6028/NIST.IR.8259a
12. FBI: Industry Alert: Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities. U.S. Federal Bureau of Investigation (FBI) (2022). https://www.ic3.gov/Media/News/2022/220912.pdf. Accessed 28 Dec 2022
13. FDA: FDA approves first automated insulin delivery device for type 1 diabetes. U.S. Food and Drug Administration (FDA) (2016). https://www.fda.gov/news-events/press-announcements/fda-approves-first-automated-insulin-delivery-device-type-1-diabetes. Accessed 10 Jan 2023
14. FDA: Postmarket Management of Cybersecurity in Medical Devices. U.S. Food and Drug Administration (FDA) (2016). https://www.fda.gov/media/95862/download. Accessed 28 Dec 2022
15. FDA: Class 2 Device Recall Medtronic MiniMed 600 Series Insulin Pump Systems. U.S. Food and Drug Administration (FDA) (2022). https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=196205. Accessed 10 Jan 2023

16. FDA: Class 2 Device Recall Medtronic MiniMed 600 Series Insulin Pump Systems. U.S. Food and Drug Administration (FDA) (2022). https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=196183. Accessed 10 Jan 2023
17. FDA: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance. U.S. Food and Drug Administration (FDA) (2022). https://www.fda.gov/media/119933/download. Accessed 28 Dec 2022
18. FDA: Cybersecurity Modernization Action Plan. U.S. Food and Drug Administration (FDA) (2022). https://www.fda.gov/media/163086/download. Accessed 28 Dec 2022
19. Hellerstein, J., Diao, Y., Parekh, S., Tilbury, D.: Feedback Control of Computing Systems. Wiley (2004). https://doi.org/10.1002/047166880X
20. IMDRF: Principles and Practices for Medical Device Cybersecurity. International Medical Device Regulators Forum (IMDRF) (2020). http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf. Accessed 28 Dec 2022
21. Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R.: A review on security and privacy of internet of medical things. In: Ghosh, U., Chakraborty, C., Garg, L., Srivastava, G. (eds.) Intelligent Internet of Things for Healthcare and Industry. Internet of Things. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-81473-1_8
22. Kephart, J., Chess, D.: The vision of autonomic computing. Computer **36**(1), 41–50 (2003). https://doi.org/10.1109/MC.2003.1160055
23. MDCG: Guidance on Cybersecurity for medical devices. Medical Device Coordination Group (MDCG) (2019). https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native. Accessed 28 Dec 2022
24. Medtronic: Urgent Medical Device Correction: MiniMed^{TM} 600 Series Pump System Communication Issue (2022). https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice19-letter. Accessed 10 Jan 2023
25. Medtronic: MiniMed 670G System Discontinuation of New Sales (2023). https://www.medtronicdiabetes.com/products/minimed-670g-insulin-pump-system. Accessed 10 Jan 2023
26. Medtronic: The MiniMed 630G and 770G Insulin Pumps (2023). https://www.medtronic.com/us-en/healthcare-professionals/therapies-procedures/diabetes/education/diabetes-digest/minimed-insulin-pumps.html. Accessed 10 Jan 2023
27. Rao, A., Carreón, N.A., Lysecky, R., Rozenblit, J.: FIRE: a finely integrated risk evaluation methodology for life-critical embedded systems. Information **13**(1010), 487 (2022). https://doi.org/10.3390/info13100487
28. Rao, A., Rozenblit, J., Lysecky, R., Sametinger, J.: Trustworthy multi-modal framework for life-critical systems security. In: Proceedings of the Annual Simulation Symposium, ANSS 2018, San Diego, CA, USA, pp. 1–9. Society for Computer Simulation International (2018). https://doi.org/10.5555/3213032.3213049
29. Reports And Data: Market value of the internet of medical things worldwide in 2019 and 2027 (in billion U.S. dollars). Statista (2021). https://www.statista.com/statistics/1264333/global-iot-in-healthcare-market-size/. Accessed 28 Dec 2022
30. Rezvy, S., Petridis, M., Lasebae, A., Zebin, T.: Intrusion detection and classification with autoencoded deep neural network. In: Lanet, J.-L., Toma, C. (eds.) SECITC 2018. LNCS, vol. 11359, pp. 142–156. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12942-2_12
31. Riegler, M., Sametinger, J., Rozenblit, J.W.: Context-aware security modes for medical devices. In: 2022 Annual Modeling and Simulation Conference (ANNSIM), pp. 372–382 (2022). https://doi.org/10.23919/ANNSIM55834.2022.9859283

32. Riegler, M., Sametinger, J., Vierhauser, M.: A distributed MAPE-K framework for self-protective IoT devices. In: 2023 IEEE/ACM 18th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (2023). https://doi.org/10.1109/SEAMS59076.2023.00034
33. Riegler, M., Sametinger, J., Vierhauser, M., Wimmer, M.: A model-based mode-switching framework based on security vulnerability scores. J. Syst. Softw. **200**, 111633 (2023). https://doi.org/10.1016/j.jss.2023.111633
34. Ross, R., McEvilley, M., Carrier Oren, J.: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. No. NIST SP 800-160, U.S. National Institute of Standards and Technology (NIST) (2016). https://doi.org/10.6028/NIST.SP.800-160
35. Sametinger, J., Rozenblit, J., Lysecky, R., Ott, P.: Security challenges for medical devices. Commun. ACM **58**(4), 74–82 (2015). https://doi.org/10.1145/2667218
36. Stajano, F., Anderson, R.: The grenade timer: fortifying the watchdog timer against malicious mobile code. In: Proceedings of 7th International Workshop on Mobile Multimedia Communications, MoMuC 2000, Waseda, Tokyo, Japan (2000). https://www.cl.cam.ac.uk/~fms27/papers/2000-StajanoAnd-grenade.pdf. Accessed 28 Dec 2022
37. Sun, Y., Lo, F.P.W., Lo, B.: Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access **7**, 183339–183355 (2019). https://doi.org/10.1109/ACCESS.2019.2960617
38. The White House: Executive Order 14028: Improving the Nation's Cybersecurity (2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Accessed 27 Dec 2022
39. Thomasian, N.M., Adashi, E.Y.: Cybersecurity in the Internet of Medical Things. Health Policy Technol. **10**(3), 100549 (2021). https://doi.org/10.1016/j.hlpt.2021.100549
40. Zeadally, S., Das, A.K., Sklavos, N.: Cryptographic technologies and protocol standards for Internet of Things. IoT **14**, 100075 (2021). https://doi.org/10.1016/j.iot.2019.100075