Resilient Security of Medical Cyber-Physical Systems

Aakarsh Rao[1], Nadir Carreón[1], Roman Lysecky[1], Jerzy Rozenblit[1], and Johannes Sametinger[2(✉)]

[1] University of Arizona, Tucson, AZ, USA
{aakarshrao7,nadir}@email.arizona.edu,
{rlysecky,jr}@ece.arizona.edu
[2] Johannes Kepler University Linz, Linz, Austria
johannes.sametinger@jku.at

Abstract. Incorporating network connectivity in cyber-physical systems (CPSs) leads to advances yielding better healthcare and quality of life for patients. However, such advances come with the risk of increased exposure to security vulnerabilities, threats, and attacks. Numerous vulnerabilities and potential attacks on these systems have been demonstrated. We posit that cyber-physical system software has to be designed and developed with security as a key consideration by enforcing fail-safe modes, ensuring critical functionality and risk management. In this paper, we propose operating modes, risk models, and runtime threat estimation for automatic switching to fail-safe modes when a security threat or vulnerability has been detected.

Keywords: Cyber-physical system · Medical device · Security

1 Introduction

Advancements in computational resources, sensors, and networking capabilities have led to the incorporation of Internet-connected devices in our lives [14]. These developments have also strongly influenced advances in healthcare and medical devices that have become part of digital health ecosystems [3]. Continual patient monitoring and services, interoperability, and real-time data access has become a normality. Life-critical devices, including implantable pacemakers and wearable insulin pumps, are essential for patients' health, well-being, and life. However, they pose additional security challenges in addition to those being considered for regular IT [17]. This is particularly exacerbated due to communication methods like Wi-Fi or Bluetooth that enable remote monitoring, real-time data analysis, and remote updates and configurations of device parameters [13].

2 Related Work

Considerable work has been done in the analysis of multi-modal CPSs with adaptive software for efficient resource utilization, incremental integration and

G. Anderst-Kotsis et al. (Eds.): DEXA 2019 Workshops, CCIS 1062, pp. 95–100, 2019.
https://doi.org/10.1007/978-3-030-27684-3_13

adaptability [8]. Mode change protocols are either event or time triggered [9]. Much work exists in real-time threat assessment and management particularly in intrusion detection systems, that however do not have the rigid timing and robust requirements found in medical CPSs [2,5]. Several works have been proposed for ensuring safety and security in medical devices, in broad areas of risk management, hardware devices, formal modeling and verification, and security schemes [4,15,19]. These proposed defenses require additional hardware to be worn by the patient or involve biological authentication schemes requiring further processing. However, security must be deeply integrated in the very design of medical devices and suitable mitigation schemes have to be incorporated in order to dynamically mitigate risks during deployment. Towards this direction we previously formally modeled a multi-modal software design framework with an adaptive risk assessment methodology and showcased preliminary findings with an integrated threat detector [11,12].

3 Resilient Security of Cyber-Physical Systems

Resilient context-aware medical device security has been proposed in [16]. The authors have shown the effect of sensitivity, impact, exposure, and authentication on context-awareness and resilience. We extend these mechanisms and propose to have resilience in CPSs by designing them in multiple modes, by modeling risk and by adaptive update of these risks, and eventually by automatic mitigation schemes.

3.1 Multi-modal Design

We propose to design application software for medical CPSs in a multi-modal fashion, cf. [8,12]. The system can operate in only one mode at a time. To ensure critical functionality of the medical device, the system has one essential mode that runs with a minimal attack surface. Each mode consists of a set of tasks to be performed by that mode, where a task would represent the implementation thread. In the essential mode, the tasks performed are the critical ones required for the essential functionality of the system. Different modes can have tasks in common based on the functionality.

3.2 Adaptive Risk Modeling

Risk modeling is a central activity in order to ensure security of systems [7]. A risk model is deeply integrated into the multi-modal software model by associating risk values at every hierarchical level of the mode to provide robust risk assessment and management, cf. [10]. During the deployment of the device, risks of the operations are assessed and updated based on the threats detected and estimated threat probabilities of the operations. Our threat detector is implemented in hardware and focuses on monitoring and analyzing the timing of the internal operations of the target system by utilizing a sliding window [6]. At

runtime, the timing samples inside each sliding window are analyzed, and the probability of the current execution being malicious (threat probability) is calculated. In addition to the proposed risk update in [11], we augment an additional risk update condition for impactful operations. Impactful operations are defined as operations whose base risk is beyond an impact threshold that would directly affect the critical functionality of the system. The risk update is exponential for these operations as compared to an additive increase as proposed in [11].

3.3 Threat Estimation

For runtime risk assessment, risk values need to be updated in a composite risk model. If we detect security threats with estimated threat probabilities, we can update risk values accordingly, depending on the estimated security threat probabilities. We assign initial composite risks to the modes based on their composition of tasks or task options that constitute the modes. For example, initial operation risks can be assigned based on security scores as proposed in [18].

3.4 Automatic Mitigation Schemes

In many domains, including health, risks have arisen through the addition of software and connectivity. Attack vectors that did not previously exist have suddenly become a priority [1]. To ensure risk management during deployment of the device, we propose an automatic mitigation scheme that changes operating modes of the system triggered by updates in risk values in order to reduce the effective risk of the system. The system risk is the risk of the current operating mode. A system level risk threshold is defined by an expert that represents the level beyond which the system cannot operate in the current operating mode. It is assumed that during initial deployment the system always operates in the highest mode, thus, having full funtionality and connectivity to the outside world.

3.5 Architectural Overview

Figure 1 gives an overview of the components of a secured cyber-physical system. We can see that various modes are available that are switched depending on risk assessment. Depending on the determination of risks, threat estimations will lead to mitigation activities that have an effect on the operation of the CPS by means of switching the modes. The modes have common functionalities, but the lower the mode number, the more restrictive are activities that may lead to security problems. We imagine that in the essential Mode 0, a CPS will only provide basic functionlity with any communication turned off that is not absolutely necessary for the basic functioning. Thus, Mode 0 will have the smallest attack surface possible, while Mode n will provide full functionality of the system with the biggest attack surface.

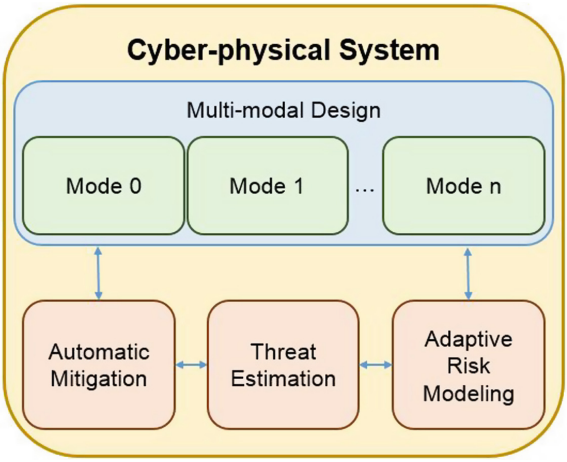

Fig. 1. Architectural overview.

4 Insulin Pump

We have started to evaluate our proposal with different insulin pump scenarios. The attacks we will use in these scenarios will be based on known malware that we will adapt to the insulin pump model. For example, the Fuzz malware is a common attack by malicious users, with the purpose of interfering with the predefined functionality of the target system by "fuzzing", or slightly altering the data. The Information Leakage malware is another well-known attack, with the goal of breaking confidentiality by extracting information from the patient and transmitting it to an unauthorized user. We plan to use the same configuration for all simulations. The starting point of the simulations will always be the highest functionality mode. Then we'll try to find out how well the system will adapt to different threat scenarios and whether these adaptations will effectively be able to mitigate the threats.

5 Conclusion

CPSs pose many security threats. We suggest that, in addition to considering security issues during development from the very beginning, we have to make sure that our systems are capable of reacting to threat scenarios not yet known during development. Software updates are a means of adapting systems in such scenarios. However, for CPSs, updates and patches are not always practicable. For such cases, our proposed resilience mechanisms with a multi-mode design, adaptive risk updating, and an automatic mitigation scheme seems a reasonable solution. We are now in the process of experimenting with an insulin pump to find out how our proposed solution reacts to various attack scenarios.

Acknowledgement. This work has partially been supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria.

References

1. Biro, M., Mashkoor, A., Sametinger, J., Seker, R. (eds.) Software safety and security risk mitigation in cyber-physical systems. IEEE Softw. **35**(1), 24–29 (2018)
2. Blyth, A., Thomas, P.: Performing real-time threat assessment of security incidents using data fusion of IDS logs. J. Comput. Secur. **14**(6), 513–534 (2006)
3. Krishnamurthy, R., Sastry, A., Balakrishnan, B.: How the internet of things is transforming medical devices. Cognizant 20–20 Insights, Cognizant (2016)
4. Li, C., Raghunathan, A., Jha, N.K.: Improving the trustworthiness of medical device software with formal verification methods. IEEE Embed. Syst. Lett. **5**, 50–53 (2013)
5. Lu, S., Seo, M., Lysecky, R.: Timing-based anomaly detection in embedded systems. In: Proceedings of the 20th Asia and South Pacific Design Automation Conference, pp. 809–814 (2015)
6. Lu, S., Lysecky, R.: Time and sequence integrated runtime anomaly detection for embedded systems. ACM Trans. Embed. Comput. Syst. **17**(2), 38:1–38:27 (2018)
7. National Institute of Standards and Technology: Guide for Conducting Risk Assessments. NIST Special Publication 800–30 Revision 1, September 2012
8. Phan, L.T.X., Lee, I.: Towards a compositional multi-modal framework for adaptive cyber-physical systems. In: IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, pp. 67–73 (2011)
9. Phan, L.T.X., Chakraborty, S., Lee, I.: Timing analysis of mixed time/event-triggered multi-mode systems. In: IEEE Real-Time Systems Symposium (RTSS), pp. 271–280 (2009)
10. Rao, A., Rozenblit, J., Lysecky, R., Sametinger, J.: Composite risk modeling for automated threat mitigation in medical devices. In: Proceedings of the Modeling and Simulation in Medicine Symposium, Virginia Beach, VA, USA, pp. 899–908 (2017)
11. Rao, A., Carreon Rascon, N., Lysecky, R., Rozenblit, J.W.: Probabilistic security threat detection for risk management in cyber-physical medical systems. IEEE Softw. **35**(1), 38–43 (2018)
12. Rao, A., Rozenblit, J., Lysecky, R., Sametinger, J.: Trustworthy multi-modal framework for life-critical systems security. In: Annual Simulation Symposium, article no. 17, pp. 1–9 (2018)
13. Roberts, P.: Intel: New Approach Needed to Secure Connected Health Devices (2015). https://www.securityledger.com/2015/03/intel-new-approach-needed-to-secure-connected-health-devices/
14. Rose, K., Eldridge, S., Chapin, L.: The Internet of Things (IoT): An Overview-Understanding the Issues and Challenges of a More Connected World. Internet Society (2015)
15. Rostami, M., Juels, A., Koushanfar, F.: Heart-to-Heart (H2H): authentication for implanted medical devices. In: ACM SIGSAC Conference on Computer & Communications Security, pp. 1099–1112 (2013)
16. Sametinger, J., Steinwender, C.: Resilient context-aware medical device security. In: International Conference on Computational Science and Computational Intelligence, Symposium on Health Informatics and Medical Systems (CSCI-ISHI), Las Vegas, NV, USA, pp. 1775–1778 (2017)

17. Sametinger, J., Rozenblit, J., Lysecky, R., Ott, P.: Security challenges for medical devices. Commun. ACM **58**(4), 74–82 (2015)
18. Sametinger, J., Rozenblit, J.W.: Security scores for medical devices. In: Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2016) - Volume 5: HEALTHINF, pp. 533–541 (2016)
19. Xu, F., Qin, Z., Tan, C.C., Wang, B., Li, Q.: IMDGuard: securing implantable medical devices with the external wearable guardian. In: IEEE INFOCOM (2011)