Safety and security architecture analyses framework for the internet of things of medical devices

Julia Rauscher, Bernhard Bauer

Angaben zur Veröffentlichung / Publication details:

Rauscher, Julia, and Bernhard Bauer. 2018. "Safety and security architecture analyses framework for the internet of things of medical devices." In *Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 17-20 Sept. 2018, Ostrava, Czech Republic, Czech Republic*, edited by Martin Černý and Norbert Noury. Los Alamitos, Calif.: IEEE. https://doi.org/10.1109/healthcom.2018.8531121.

Safety and Security Architecture Analyses Framework for the Internet of Things of Medical Devices

Julia Rauscher, Bernhard Bauer
Software Methodologies for Distributed Systems
University of Augsburg, Germany
{Julia.Rauscher, Bernhard.Bauer}@informatik.uni-augsburg.de

Abstract— **Internet of Things (IoT) is spreading increasingly in different areas of application. Accordingly, IoT also gets deployed in health care including ambient assisted living, telemedicine or medical smart homes. However, IoT also involves risks. Next to increased security issues also safety concerns are occurring. Deploying health care sensors and utilizing medical data causes a high need for IoT architectures free of vulnerabilities in order to identify weak points as early as possible. To address this, we are developing a safety and security analysis approach including a standardized meta model and an IoT safety and security framework comprising a customizable analysis language.**

Keywords- internet of things, health care, safety and security, architecture analyses

I. Introduction

We are increasingly living in a connected world. In line with this trend more and more devices have to be connected and communicate automatically. Through these new requirements the Internet of Things (IoT) emerged. The usage in industry, smart cities and agriculture are only a few of the widely spread application fields. Next to these also the health care area is able to take advantage of this technology trend in form of the Internet of Things of Medical Devices (IoT-MD). Initially, IoT-MD is deployed in modern hospitals and medical smart homes with health care sensors organized by the occupants. The potential of IoT-MD is recognized by more and more stakeholders. Ambient assisted living, telemedicine including remote patient monitoring and personalized medicine approaches are only a couple of the possibilities for patients, elderly and health-conscious persons to make use of the IoT-MD and its potential. However, next to all the above named advantages IoT also involves the danger to include new risks regarding safety and security. Especially, IoT-MD has to deal with health-endangering vulnerabilities. Those range from simple theft of intimate data to life-imperiling endangerments of exactly those with a higher need of care, like infants or seniors. [1][2] Thus, a timely identification and elimination of safety and security vulnerabilities is essential, e.g., 50% of security flaws happen in the design phase [3]. Therefore, architecture analyses are needed. However, most of current research focuses on IoT analytics to gain knowledge about collected data. Hence, a lack of architecture analyses remains in the research field of IoT planning. A possible reason for this deficiency is the missing standardization of IoT modeling as a basis for architecture analyses.

To address the above mentioned issues, we are developing a meta model for standardizing IoT safety and security architectures. This will be used to identify architectural weak points with the aid of our analysis framework during design phase.

II. Safety and Security Analysis Approach

Our approach aims at identifying safety and security IoT-MD architecture vulnerabilities. Therefore, we defined two main steps.

First, for enabling IoT architecture analyses a standardized representation is needed. This will be achieved by developing a meta model for IoT architectures with the Eclipse Modeling Framework (EMF) [4]. Our meta model is based on the existing Microsoft Azure IoT reference architecture [5] and the IoT-A project [6]. Our meta model contains all parts of a holistic IoT environment with several members, devices and services represented in about 50 classes and their references. Among others we provide elements for modeling of physical connected devices including low power devices and typical IoT devices e.g. with an IP address and communication possibilities. Therefore, all needed communication elements are implemented like communication protocols and encoding types. Additionally, an opportunity for stakeholder modeling is embedded. To guarantee analytics, Azure elements [5] are considered. These examples are only a small excerpt of our holistic IoT meta model. To build a visual representation of a concrete IoT system a graphical editor is needed which is based on our meta model. Details will be offered on the end of this section.

The meta model can be used in three different analysis scenarios:

1) A new IoT system which is not implemented yet and shall be analyzed in advance to prevent safety and security vulnerabilities.

2) An IoT system extension which is modelled an analyzed beforehand to prohibit new issues.

3) An already existing IoT system is analyzed regarding its present vulnerabilities.

Scenario one and two represent the concept of safety/security by design and meet the aforementioned issues by eliminating vulnerabilities during design phase.

After building the basis for our analysis approach our IoT Safety and Security Architecture Analysis Framework (IoT-

S2A2F) is introduced as the second main step. Our framework is divided into three segments (A-C):

A. Architecture Analysis Configuration Language

We are developing an Architecture Analysis Configuration Language (AACL) which enables IoT system architects to apply safety and security architecture analyses depending on their domain-specific goals and needs as early as possible in IoT planning processes. The construction of our language is based on the Domain Specific Language of [7] and is implemented with Xtext [8]. Our language provides means of choosing the analysis type and method depending on functional and technical aims like failure effects or safety flaws. Subsequently, each analysis can be configured according to the needs of the respective flaw to be analyzed. Consequently, during the usage of the analysis language an IoT model is needed as input and proper metrics have to be chosen.

B. Definition and Execution of Analyses

Before describing implementation details, we explain the definitions of our analyses that shall be part of the aforementioned AACL. Other research areas already addressed the need of architecture analyses. Hence, we are conducting a concept transfer by using the experience and research results of already existing analysis as a first option to identify flaws. Those analyses are already feasible, evaluated and offer metrics. Examples are analyses of Enterprise Architecture Management (EAM) [7] or automotive software engineering with safety and security concerns [9]. Our analyses are based on several of these, like change impact, failure impact or security analyses [10]. The most suitable ones are adapted for our IoT safety and security analyses regarding special IoT-MD architecture needs and requirements. All of our analyses aim at identifying architectural safety and security flaws to prevent vulnerabilities. As a second option for flaw identification we are developing architecture patterns. These patterns are used for architecture pattern recognition which is conducted by our analyses. Through pattern recognition safety and security issues can be detected like missing authentication, false authorization or insufficient cryptography and design principles like the weakest link principle can be observed.

For implementing the analyses, provided by our AACL, we are using the Model Analysis Framework (MAF) which enables implementing dynamic model analyses [11] and is based on EMF. For executing analyses with MAF a meta model, an instance, a data flow initialization, an analysis configuration and an analysis strategy is needed. Our meta model can be inserted automatically as input for MAF. For our analyses the algorithms are traversing the model and visit every node and edge in order to evaluate the patterns to be observed.

C. Analyses Visualization

As a last step of our framework the conducted analyses can be visualized with our own visualization tool implemented with Eclipse Sirius [12]. Hereby, the results of our analyses can be processed graphically, e.g. to show safety and security vulnerabilities easily at a glance. The elements of the model are represented with suitable styles through a conditional style option. Therefore, the user can perceive differences or errors immediately. In addition, the visual representation is able to display the different layers of the elements through an implemented filter.

III. Evaluation

To evaluate our introduced approach of our IoT-S2A2F several evaluation parts are necessary. As already stated above, the used and adapted analyses are verified through former research, in which the chosen analyses are deployed successfully. However, to prove the accuracy and applicability of our remaining approach, i.e. IoT-S2A2F, we are using a medical IoT use case for evaluation. Our use case is based on a medical smart home which integrates connected home automation devices and medical or health care devices, like fall detectors, implanted glucose monitors or wearables. The medical smart home, which is focused on patients or elderly, monitors the occupants' health continuously and unobtrusively. To prove the extendibility of our approach the smart home is connected with multiple stakeholders like ambulance, hospitals, pharmacies and other tele medical members. For evaluation we first model the use case with the aid of our meta model. Accordingly, the meta model is evaluated whether all needed parts can be represented with all required details and relations. Afterwards the three steps of our framework have to be evaluated. The framework applies safety and security analyses to prove the correctness of our approach and to identify safety and security design flaws of the use case architecture exemplarily. Therefore, the use case model is loaded into IoT-S2A2F as an input model which is needed as mentioned before. Subsequently, the configurations have to be set up with AACL. We define the goals of our use case and choose the developed analyses to be executed e.g. proof of authentication before every device access. IoT-S2A2F conducts the analyses and represents flaws visually, like missing encoding processes. Our evaluation reviews our approach holistically by including all developed parts.

IV. Related Work

The potential of architecture analyses was recognized by many researchers before. However, the major part of architectural approaches is located in other research fields. An example are the already mentioned EAM analyses. [7] conducted a literature search to accomplish an overview of existing analyses. There are various approaches, from architecture dependencies with Bayesian networks [13] to the usage of extended influence diagrams for diverse analysis aims [14]. Since architecture analyses are already successfully used in EAM the analyses were recognized in other research fields. [15] represents one of the few approaches which combine EAM principles with IoT. They describe the similarities of both concepts and methods. However, they are not including the analyses approaches.

Further research was conducted concerning IoT architecture approaches like [16] to represent an IoT system on model level. Accordingly, diverse reference architectures were designed. Famous ones are the Azure project [5], IoT-A [6], RAMI [17] and IIoT [18]. As a next step, meta models and layer architecture models were invented. While [6] also proposes a few meta model excerpts, [19] and [20] present layer architectures of 3 to 5 layers. These approaches are only considered to model or structure IoT systems, but do not use the created models for architecture analyses.

However, IoT analyses are not uninvestigated. Especially security analyses are available, e.g. [21] and [22] consider this aspect. Though, these approaches are not conducted on architecture level and thus do not provide possibilities to evaluate the security in the design phase. Consequently, the principles of safety/security by design are not fulfilled.

[23] and [24] present analyses which are conducted on architecture level. [23] analyzes failure modes and effects by using SysML to evaluate medical devices and to prove the need of analysis in an early design process phase. [24] proposes the usage of Architecture Analysis and Design Language (AADL) to be able to model an IoT system with needed details for identifying security vulnerabilities.

This section showed that although there are related approaches taking IoT, architecture analysis and security/safety by design into account, the research field has not yet been sufficiently considered.

V. Conclusion

We elucidated the existence of safety and security issues in medical smart homes and suggested an approach for safety and security vulnerability prevention during design phase. On one side architecture analyses can be used to plan new IoT architectures security- and safety-aware. On the other side existing systems can be analyzed and optimized or existing systems can be extended without new arising vulnerabilities. For enabling IoT architecture analyses we claimed the necessity of a standardized meta model for a consistent architecture representation. Afterwards we presented our approach for the IoT-S2A2F for IoT-MD architecture security and safety optimization. The framework consists of the definition of an AACL including the configuration of analyses. The remaining framework conducts and visualizes these analyses to reveal vulnerabilities. Thus, safety and security critical architecture flaws of an IoT architecture are detected and can be fixed or prevented consequently. For evaluation we presented a use case to validate and verify our meta model and framework. Our holistic approach for IoT architecture modeling and analyzing for safety and security attack prevention ensures save usage of medical devices in IoT systems.

References

[1] FDA, “Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter”, https://bit.ly/2qqkgiA (accessed on 3/20/18), 2017

[2] RAPID7, “Hacking IoT:A Case Study on Baby Monitor Exposures and Vulnerabilities”, https://bit.ly/1JC9jfS (accessed on 3/20/18), 2015

[3] J. Viega and G.R. McGraw, “Building secure software: how to avoid security problems the right way”, 2001, Pearson Education

[4] Eclipse Modeling Framework, https://www.eclipse.org/modeling/emf/

[5] Microsoft Azure IoT, “Reference Architecture”, https://bit.ly/2bbcMsT (accessed on 5/28/18), 2016

[6] IoT-A, “Internet of Things – Architecture”, https://bit.ly/2GhCb0w (accessed on 3/27/18), 2013

[7] J. Rauscher, M. Langermeier and B. Bauer, “Classification and Definition of an Enterprise Architecture Analyses Language” Business Modeling and Software Design, 6th Int. Symposium 2016, Springer

[8] Eclipse Xtext, https://www.eclipse.org/Xtext/

[9] P. Lohmüller, A. Fendt and B. Bauer, “Multi-Concerns Engineering for Safety-Critical Systems”, MODELSWARD 2018

[10] T. Sommestad, M. Ekstedt and P. Johnson, “Combining defense graphs and enterprise architecture models for security analysis”, EDOC’08, 12th International IEEE , 2008, S. 349–355

[11] C. Saad and B.Bauer , “Data-flow based Model Analysis and its Applications”, MoDELS 2013, Springer

[12] Eclipse Sirius, https://www.eclipse.org/sirius/

[13] U. Franke, W.R. Flores and P. Johnson, "Enterprise architecture dependency analysis using fault trees and bayesian networks", Spring Simulation Multiconference. Society for Computer Simulation International, 2009

[14] P. Johnson et al., "Extended influence diagrams for enterprise architecture analysis", Enterprise Distributed Object Computing Conference, 2006 Oktober, pp. 3-12

[15] A. Zimmermann et al., “Enterprise architecture management for the internet of things”. Gesellschaft für Informatik eV, 2015

[16] D. Uckelmann, M. Harrison and F. Michahells, “An Architectural Approach Towards the Future Internet of Things” in Architecting the Internet of Things, 2011, pp. 1-24

[17] R. Heidel et al., “ Referenzarchitekturmodell und Industrie 4.0-Komponente Industrie 4.0 ”, Plattform Industrie 4.0, 2017

[18] S. Lin, “The Industrial Internet of Things Volume G1: Reference Architecture”, 2017

[19] M. Wu, “Research on the architecture of Internet of things”, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) Research, 2010

[20] R. Kahn et al., “Future Internet : The Internet of Things Architecture , Possible Applications and Key Challenges”, 10th International Conference on Frontiers of Information Technology (FIT), 2012

[21] G. Gan, Z. Lu and J. Jiang, “Internet of Things Security Analysis”, Internet Technology and Applications (iTAP), 2011

[22] C. Tian, “Analysis and Design of Security in Internet of Things”, Biomedical Engineering and Informatics (BMEI), 2015

[23] M. Hecht et al., “Automated generation of failure modes and effects analysis for a medical device." Software Reliability Engineering Workshops (ISSREW), 2015

[24] P. A. Wortman et al., "Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare domain." Biomedical & Health Informatics (BHI), 2017