Designing Automotive Case Studies for Architectural Security Analyses

Nicolas Boltz, Maximilian Walter, Christopher Gerking
{nicolas.boltz, maximilian.walter, christopher.gerking}@kit.edu
Karlsruhe Institute of Technology (KIT)

Abstract

Digitalization is one of the biggest drivers of advancements in the modern automotive domain. The resulting increase in communication is leading to a more intensive exchange of data and the opening up of formerly closed systems. This raises questions about security and data protection. Software architecture analyses can help identify potential issues, thereby making systems more secure and compliant with data protection laws. Such analyses require representative case studies for development and evaluation. In this paper, we showcase the results of applying requirements and processes for case-study research during three bachelor theses with students. The resulting three case studies center around the automotive and mobility domain and focus on different security and privacy properties. We discuss our insights and experiences regarding the creation of case studies.

1 Motivation

The digital transformation reaches more and more aspects of our daily lives, enabling us to build smart interconnected devices and thereby efficiently solve various societal problems. One enabler of this transformation is the data exchange between different systems. This also affects the mobility domain, where cars are evolving into an increasingly digitized platform through advancements in terms of driving safety and convenience features. Modern connected cars [4] already have a large number of sensors and offer diverse interfaces for networking and communication, which are used to connect with the infrastructure or other service providers to exchange data. For instance, cars could exchange current traffic data for intelligent traffic management, the current number of passengers for ridepooling scenarios, or their location for car sharing. These concepts can help reduce congestion [6] and save costs.

However, with the opening of formerly closed systems such as cars and the increased data exchange, security and privacy issues arise [4]. According to *Upstream's* most recent *Automotive Cybersecurity Report* [13], remote attacks represent 84,5% of the attacks compared to physical attacks on vehicles. The report also states that, with 40.1%, the most common attack vector of connected vehicles is the servers and not the vehicle itself. This means that server architecture and communication are amongst the most security-critical aspects. Furthermore, the high degree of interconnection makes it hard to comprehend a complete system, as system boundaries blend together, making it increasingly difficult to check for security and privacy issues.

Using a system architecture representation provides a better overview of the system, in which e.g. complete vehicles are abstracted to only a few components containing parts where the vehicle interacts with the infrastructure. By taking this more abstract point of view of the system, we might neglect some more fine-grained internal issues, but in turn gain several abstractions, which can be used for the analyses of the overall system. Based on the system architecture, we could use existing architectural analyses, such as [7, 12, 14], to find security or privacy issues. While case studies represent the most common evaluation approach for such software architecture research [10], the majority of recent research articles still lack guideline-based evaluations.

For execution, most software architecture analyses require an architecture expressed in an architecture description language (ADL). In our case, we utilize the Palladio Component Model (PCM) [5]. Currently, we can only identify a very limited number of case studies meeting this requirement in the mobility or automotive domain. In addition, more informal architectural descriptions, e.g., purely natural language texts, only rarely contain the necessary properties.

In this paper, we showcase our experience and results of applying the requirements and processes defined in well-known case study research papers, like from Verner et al. [1] and Runeson et al. [3], during the supervision of three bachelor theses. During their theses, each student focused on different security or privacy properties and analyzed the created software architecture models with a corresponding architectural analysis. Further, we discuss our insights and experiences.

2 Foundations For Case Study Design

Different approaches try to tackle the usage, design, and conduction of case studies in the software engineering domain. Verner et al. [1] describe a case study as "a single case or a small number of cases", which are used in software engineering "for evaluating research but also to observe, explain and explore phenomena in real-life settings" [1]. They define guidelines and structure case study research in several phases. In their work, Runeson et al. [3] describe guidelines for case study research. They define a case study as an empirical means to evaluate software engineering in a real-life context [3]. During the study, the case is "the main subject of study" [2]. While conducting a case study, knowledge about previously not considered data is gained. To improve the case study design, the case study should be designed and conducted iteratively, including the previously gained knowledge in the case study design [3]. In our case, we first aim for exploration and evaluation. However, after the successful application of different architectural analyses, the case studies can also be used to explain or describe architectural analyses in the mobility section.

3 Case Studies

Each case study was created by a different student and investigated different security properties such as privacy or attacker propagation. In each thesis, we acted as an advisor to the students. In the interest of brevity, we only provide short descriptions of the systems that have been modeled and analyzed. More detailed descriptions and architectural models can be found in the respective bachelor theses or data sets.

Case Study Dataflow Analysis The protection of personal data has become an increasingly important issue. Analyzing the architecture of software systems with regard to data protection issues helps to create legally compliant systems at an early stage, thereby supporting data protection by design.

As part of his bachelor thesis, Palitza [17] designed a case study using the dataflow analysis of Seifermann et al. [12]. Instead of defining properties concerning confidentiality, like roles for access control, he focused on data protection-relevant properties, such as the categorization of data according to Art. 9 GDPR. To derive these properties, he mainly focused on the definitions and principles of the GDPR. His case study is centered around the system of a provider of a ridepooling service. Users interact with the system using a web interface and can request rides by providing their desired start and end location. Cars, which can be autonomous or be driven by a human driver, report whether they are available to the provider system backend. Both users and cars use the web interface to communicate with the provider system backend. Users which have registered with the provider system can not only request rides but are also able to take the role of a car and provide ridepooling services to other users. The user storage database, within the system backend, is used to consolidate all user and car information in the system. To process payments for completed trips, a payment system is used, which is officially operated by the municipality as part of its public transport concept.

Case Study Uncertainty Impact During development and operation, uncertainty about the system and its environment exists [16]. This is especially true for cyber-physical systems and systems of systems. Uncertainty exists due to open design decisions [15] or because of environmental properties like sensor inputs [8]. The impact of uncertainty should be considered in confidentiality analysis to prevent imprecise conclusions.

Priss [11] designed a case study considering the uncertainty impact in his Bachelor's thesis. To satisfy the real-world context requirement, the *Restricted Area Rides* and *Top Speed Calculation* use cases from Open Mobility Foundation (OMF)'s use case gallery [1] for Mobility Data Specification (MDS) were selected. The use cases describe that the city agencies are interested in whether riders drive through restricted areas and whether the speed limits are upheld by them. This is realized by processing the user data and the vehicles' telemetry data at the mobility service provider. Afterward, the agency can pull the required data for its analysis through the *provider* Application Programming Interface (API). Here, only non-sensitive data shall be transmitted. For the architectural analysis, an uncertainty impact analysis was used [15]. This analysis returns whether modeled uncertainty can affect the system's confidentiality.

Case Study Attack Propagation Estimating potential attack paths or attack graphs is one way to harden a system against attackers. There exist various approaches using different graphs for attacks [14]. These graphs help to identify possible attack paths and indicate how an attacker could propagate through a system. Therefore, it is beneficial to consider this security property in a mobility case study.

In his thesis, Evli [9] proposed a mobility case study based on MDS. His investigated case focused on the communication between the agency and mobility providers. For the architectural analysis, he used our architectural attack propagation approach [14]. It considers vulnerabilities and access control properties to estimate potentially affected architectural elements.

4 Lessons Learned

During our work, we identified several insights. The first insight pertains to the evaluation of the requirements. Deciding when a requirement is fulfilled is

[1] airtable.com/shrPf4QvORkjZmHIs/tblzFfU6fxQm5Sdhm

complicated. For instance, deciding whether a system is embedded in a real-world context is not easy and often depends on the interpretation of the individual. Based only on the description, it is unclear whether our case studies based on MDS are already embedded in the real world or not. On the one hand, the MDS API is used in real systems throughout different cities. On the other hand, our modeled systems are based only on the API description and other available information. Therefore, the studies are not based on a real system, which might entail different or additional security properties. In our cases, we have found that it would be beneficial to subdivide the requirements into different degrees of fulfillment. A possible degree is that the case is inspired by a real-world system. In our eyes, our case studies fulfill this degree.

During the design of one case study, we used a dedicated case study protocol. This documents the steps during the design of the case study and helps researchers make concrete preliminary considerations about the case study, its objectives, required data collection, and analysis methods. Furthermore, the protocol guides the researchers through the case study iterations, ensuring that all necessary points are addressed. All of our observations are consistent with the highlighted benefits of Runeson et al. [3]. These insights could be particularly interesting for educational purposes, as students often need more support with case study research.

5 Conclusion

In this paper, we presented three different architectural case studies, which have been created as part of bachelor theses. Each case study is based in the mobility domain and focuses on a different security or property. As lessons learned, we discuss several insights, like the difficulty of establishing a real-world context or determining whether it exists to a sufficient degree. The three proposed case studies can be seen as the first step for case studies in the automotive domain, with a focus on software architecture. We believe they can serve as a basis for extensions of others and help researchers or security analysis developers to evaluate their approaches.

Acknowledgment

This publication is partially based on the research project SofDCar (19S21002), which is funded by the German Federal Ministry for Economic Affairs and Climate Action. This work was also supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs and the BMBF (German Federal Ministry of Education and Research) grant number 16KISA086 (ANYMOS).

We like to thank Denis Priss, Yakup Evli and Fabian Palitza, for their Bachelor theses.

References

[1] J. Verner et al. “Guidelines for industrially-based multiple case studies in software engineering”. In: *RCIS*. 2009, pp. 313–324.

[2] R. K. Yin. *Case study research: Design and methods*. Vol. 5. sage, 2009.

[3] P. Runeson et al. *Case Study Research in Software Engineering: Guidelines and examples*. John Wiley & Sons, 2012, p. 237.

[4] R. Coppola and M. Morisio. “Connected Car: Technologies, Issues, Future Trends”. In: *ACM Computing Surveys* 49.3 (Oct. 2016).

[5] R. Reussner et al. *Modeling and Simulating Software Architectures – The Palladio Approach*. Cambridge, MA: MIT Press, Oct. 2016. 408 pp.

[6] J. Ke, H. Yang, and Z. Zheng. “On ride-pooling and traffic congestion”. In: *Transportation Research Part B: Methodological* 142 (2020), pp. 213–231.

[7] N. Boltz et al. “A Model-Based Framework for Simplified Collaboration of Legal and Software Experts in Data Protection Assessments”. In: LNI. 2022, pp. 521–532.

[8] N. Boltz et al. “Handling Environmental Uncertainty in Design Time Access Control Analysis”. In: *SEAA*. IEEE, 2022.

[9] Y. E. Evli. “A Mobility Case Study for Validating Attack Propagation Analyses”. Bachelor thesis. KIT, 2022.

[10] M. Konersmann et al. “Evaluation Methods and Replicability of Software Architecture Research Objects”. In: *ICSA*. 2022, pp. 157–168.

[11] D. Priss. “A Mobility Case Study Framework for Validating Uncertainty Impact Analyses regarding Confidentiality”. Bachelor th. KIT, 2022.

[12] S. Seifermann et al. “Detecting violations of access control and information flow policies in data flow diagrams”. In: *JSS* 184 (2022), p. 111138.

[13] UpStream. *2022 Global Automotive Cybersecurity Report*. 2022.

[14] M. Walter, R. Heinrich, and R. Reussner. “Architectural Attack Propagation Analysis for Identifying Confidentiality Issues”. In: *ICSA*. IEEE. 2022, pp. 1–12.

[15] S. Hahner, R. Heinrich, and R. Reussner. “Architecture-based Uncertainty Impact Analysis to ensure Confidentiality”. In: *SEAMS*. IEEE/ACM, 2023.

[16] S. Hahner et al. “A Classification of Software-Architectural Uncertainty regarding Confidentiality”. In: *ICETE*. Springer, 2023.

[17] F. Palitza. “Fallstudie zur Privatsphäre in Connected-Car Systemen”. Bachelor thesis. KIT, 2023.