Chair of Computer Engineering

A Systematic Categorization of IoT Security Patterns

Exposé by

Eva Gründinger

Advisor
Prof. Dr. Stefan Katzenbeisser

April 12, 2022

Contents

1 Problem

Designing a computer system is a complex project that gets easier by utilizing the right tools. Specific patterns and architectures allow a developer to simplify problems in an abstract way and analyse the given structure of a system. By not only applying different patterns for design but also security or even privacy the developed system ensures a secure and privacy-aware operation by design. But the development and usage of said security and privacy patterns is hindered by the needed expert knowledge in these areas. For this reason extensive documentation and testing in practice is needed to ensure usable patterns that can be easily applied by any developer to a given system.
While design patterns for development and implementation are common for most computer systems these days, domain-specific patterns like for Internet of Things are rare to find. Because of different requirements that an IoT system has compared to a general computer system, existing design patterns are often not suitable for this specific use case. When IoT-specific patterns are already hard to find, it is only reasonable to assume that IoT patterns that are security or privacy specific are even rarer. Even though they exist, a structured and organized catalogue of all kinds of IoT security patterns is basically non-existent at this point in time.
Therefore, this master's thesis proposes a systematic collection and categorization of IoT security (and privacy) patterns and analyses the gaps of the recent research work regarding IoT security. As a catalogue that combines all IoT security patterns in one place and is organized in a top to bottom approach that follows the IoT World Forum Reference Model of the IoT architecture, this collection will play an important part in future development of secure IoT solutions.

2 State of the art

2.1 IoT Patterns and Architectures

Patterns are a common way to describe abstract solutions to design problems and can be used to analyse and understand computer systems in an easier way. Reinfurt et al. [Rei+17] describe in their paper IoT-specific patterns that help to design Internet of Things systems and can be applied to the domain of Smart Factory Systems.

Other than design patterns, different architecture styles can be utilized when creating IoT systems. Muccini et al. [MM18] provide a number of abstract IoT reference architectures in their paper. Their study helps to classify existing and future approaches for IoT styles at the architectural level.

In order to get a better idea of the landscape of patterns and architectures that have accumulated over the years in research, Washizaki et al. [Was+19; Was+20] analysed the successes and failures of the used patterns for IoT systems. But because of limited documentation there is a lot of room for improvement in the development of IoT-specific patterns and architectures.

2.2 IoT Security Patterns and Architectures

Fysarakis et al. [Fys+19] sketch the SEMIoTICS approach in their paper. Aiming to develop a pattern-driven framework, the SEMIoTICS project wants to guarantee semi-autonomic behaviour in IoT/Industrial IoT applications.

Organized in an hierarchical taxonomy, Papoutsakis et al. [Pap+21] collect and categorize a set of security and privacy patterns. This usable pattern collection should guide developers to design IoT solutions that are secure and privacy-aware by design.

Over the last 3 years, Rajmohan et al. [RNF20a; RNF20b; RNF22] published different papers that review the research work regarding IoT patterns and architectures for IoT security and privacy. Although there is a rise in the number of publications, there is not yet an approach of applying architectures and patterns together that address security not only on the architectural but also on the network or IoT-devices level.

3 Research questions

The thesis aims to answer the following research questions:

- R1 Which layer in the IoT World Forum Reference Model of the IoT architecture is covered by the least security patterns?
- R2 Which security goal is addressed by security patterns the least?
- R3 How many of the OWASP Top Ten most common vulnerabilities within IoT are solved by utilizing these security patterns?

4 Evaluation

Before any of the research questions can be answered, we have to search for security patterns that are specific for IoT that already exist in literature and specify them in a systematic way: *pattern name, intent, problem & solution, applicability, UML representation, implementation, known uses.*
Then we categorize each pattern according to the IoT World Forum Reference Model (WFRM) of the IoT architecture by assigning it to its corresponding layer and list them in a top to bottom approach.

R1 Compare the number of security patterns of each layer in the IoT WFRM.

R2 List the important security goals for an IoT system and check for each pattern which goals it protects. Compare the coverage of the different security goals.

R3 List the OWASP Top Ten most common security (and privacy) vulnerabilities within IoT and check if each vulnerability is solved by at least one pattern.

5 Outline

1. Introduction
    a) The role of IoT in daily life
    b) Security Risks of IoT
2. Background
    a) What is Internet of Things?
        i. Definition of IoT
        ii. Application Areas
    b) Security Goals
        i. Confidentiality
        ii. Integrity
        iii. Availability
        iv. Authentication
        v. Authorization
        vi. Accountability
        vii. Privacy
    c) Open Web Application Security Project (OWASP)
        i. Top Ten Common IoT Vulnerabilities
        ii. Top Ten Privacy Risks

6 Future Work

1. Application of IoT security patterns to use cases to test their usability in practice.
2. Cooperation of industry with academia to develop new IoT security patterns.
3. Expanding the IoT pattern catalogue with more security and privacy patterns as well as other design patterns.
4. Designing IoT security architectures that take advantage of these IoT security patterns.

Bibliography

[Fys+19] Konstantinos Fysarakis et al. "Architectural Patterns for Secure IoT Orchestrations." In: *2019 Global IoT Summit (GIoTS)*. 2019, pp. 1–6. DOI: 10.1109/GIOTS.2019.8766425 (cit. on p. 2).

[MM18] Henry Muccini and Mahyar Tourchi Moghaddam. "IoT Architectural Styles." In: *Software Architecture*. Ed. by Carlos E. Cuesta, David Garlan, and Jennifer Pérez. Cham: Springer International Publishing, 2018, pp. 68–85. ISBN: 978-3-030-00761-4 (cit. on p. 2).

[Pap+21] Manos Papoutsakis et al. "Towards a Collection of Security and Privacy Patterns." In: *Applied Sciences* 11.4 (2021). ISSN: 2076-3417. DOI: 10.3390/app11041396. URL: https://www.mdpi.com/2076-3417/11/4/1396 (cit. on p. 2).

[RNF20a] Tanusan Rajmohan, Phu H. Nguyen, and Nicolas Ferry. "Research Landscape of Patterns and Architectures for IoT Security: A Systematic Review." In: *2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. 2020, pp. 463–470. DOI: 10.1109/SEAA51224.2020.00079 (cit. on p. 3).

[RNF22] Tanusan Rajmohan, Phu Hong Nguyen, and Nicolas Ferry. "A decade of research on patterns and architectures for IoT security." In: *Cybersecurity* 5 (2022), pp. 1–29 (cit. on p. 3).

[RNF20b] Tanusan Rajmohan., Phu Nguyen., and Nicolas Ferry. "A Systematic Mapping of Patterns and Architectures for IoT Security." In: *Proceedings of the 5th International Conference on Internet of Things, Big Data and Security - IoTBDS,* INSTICC. SciTePress, 2020, pp. 138–149. ISBN: 978-989-758-426-8. DOI: 10.5220/0009583001380149 (cit. on p. 3).

[Rei+17] Lukas Reinfurt et al. "Applying IoT Patterns to Smart Factory Systems." In: *Proceedings of the 11th Advanced Summer School on Service Oriented Computing*. IBM Research Division, 2017, pp. 1–10 (cit. on p. 2).

[Was+19] Hironori Washizaki et al. "Landscape of IoT Patterns." In: *2019 IEEE/ACM 1st International Workshop on Software Engineering Research Practices for the Internet of Things (SERP4IoT)*. 2019, pp. 57–60. DOI: 10.1109/SERP4IoT.2019.00017 (cit. on p. 2).

[Was+20] Hironori Washizaki et al. "Landscape of Architecture and Design Patterns for IoT Systems." In: *IEEE Internet of Things Journal* 7.10 (2020), pp. 10091–10101. DOI: 10.1109/JIOT.2020.3003528 (cit. on p. 2).