University of Zurich[UZH]

BACHELOR THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Inventorying and Secure Life-Cycles of IoT Devices

Armin Richard Veres
Zurich, Switzerland
Student ID: 20-700-118

Supervisor: Dr. Eryk Schiller
Date of Submission: December 1, 2023

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Bachelor Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Abstract

Das ist die Kurzfassung...

Acknowledgments

Optional

Contents

Chapter 1

Introduction

1.1 Motivation

1.2 Description of Work

1.3 Thesis Outline

Chapter 2

Background

2.1 Distributed Ledger Technology

Chapter 3

Related Work

3.1 CERTIFY

This thesis is carried out in conjunction with the CERTIFY project.

The National Institute for Standard and Technology has a few ongoing projects and white papers on security related mitigation methods for IoT devices.

3.2 DLT-based Asset-Tracking

Neisse et al. (2017) analyzed how blockchain-based approaches might be used for data accountability and provenance tracking under the then recently released GDPR legislation, highlighting challenges of scalability and considering sharding as a method to address it. [1] Further they also mentioned issues of clonability of the tracked assets, which we can also correlate to the physical assets that are tracked inside blockchain.

3.3 Device fingerprinting

In order to be able to track IoT nodes in a blockchain, they need to be uniquely identifiable, in our case even in a distributed manner, using Distributed Identifiers, DIDs. Methods of creating identifiers that are unique to devices exist, such as SRAM-Based PUF Readouts [2].

3.4 Cybersecurity of IoT Devices

In order to maintain participation rights for only valid users/clients, Manufacturer Usage Descriptions, MUDs, are getting more and more relevant, as also the National Institute for Standards and Technology, NIST, have been considering their use cases. [3]

Chapter 4

Use Case Definition - Connected Cabin System

4.1 Background

Our use case will take the CCS scenario from Figure 4.1 into consideration and build up on their use cases.

Nowadays more and more IoT devices are being deployed to aircraft cabins to improve passenger experience and airline operations. Benefits span from remote PHM to reduced maintenance time, while also supporting a continuous (re)certification process.

4.2 Actors

We will consider following actors for our use case.

- Airline: Owns the aircraft and oversees interactions and system operations.
- Airplane maintainer: They could be e.g., Airplane manufacturer. Oversees maintenance of the aircraft, including the integration of systems designed by different manufacturers and their configuration.
- Product Owner: Oversees design and maintenance of systems deployed in the aircraft on assignment of the airplane maintainer.
- Maintenance operator: They work for the airplane maintainer. Their responsibilities include e.g., the replacement of devices or on-site software upgrades of e.g., portable data loaders.
- Passenger, Attendant, Pilot: They interact with the aircraft through sensors, actuators or HMI.

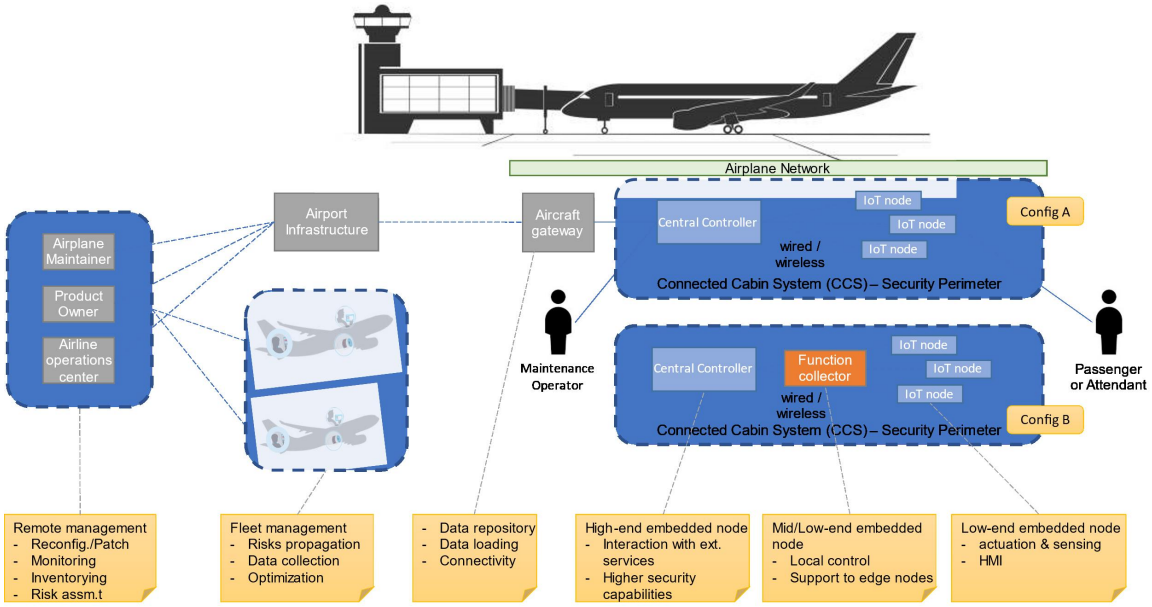

Figure 4.1: Collins CCS

4.3 System Components

We will consider an aircraft to have multiple networks, covering various aspects.

- In-flight entertainment system
- Aircraft System
- Flight Maintenance

For our use case we will assume config 'A' as the main configuration of the networks, where edge nodes are connected to a central controller that manages the edge nodes as a subnet.

- IoT / Edge Nodes: low-end devices, including actuation, sensing or HMI capabilities, with limited room for hardware and software based cybersecurity, that requires offloading to a more capable instance.
- Central Controller: High-end devices with ability to host full-fledged security functionalities.

External communication will take place through aircraft gateway offering services for data repository, data loading and connectivity with external environment. The airline operations center, product owner and airplane maintainer can interact through the airport infrastructure. A technician may directly access the aircraft if necessary.

Table 4.1: Actors involved

Airline	Airplane Maintainer	Product Owner	Maintenance Operator	Passenger, Attendant, Pilot
X	-	X	-	X

Table 4.2: Lifecycle stages involved

Bootstrapping	Operation	Update	Repurposing	Decommissioning
X	-	X	-	X

4.4 Scenarios

4.4.1 Installation of Connected Cabin Systems

4.4.1.1 Goals

The goals of this scenario include bootstrapping and customization of devices for specific deployment, updating and decommissioning of previous systems, guaranteeing a reset to a known and fresh, wiped data, state. Table 4.1 highlights the involved actors and Table 4.2 shows the stages involved in this scenario.

Chapter 5

Device Life-Cycle

Chapter 6

Evaluation

Chapter 7

Summary and Conclusions

Bibliography

[1] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proceedings of the 12th international conference on availability, reliability and security*, 2017, pp. 1–10.

[2] S. Vinagrero, H. Martin, A. de Bignicourt, E.-I. Vatajelu, and G. Di Natale, "Sram-based puf readouts," *Scientific Data*, vol. 10, no. 1, p. 333, 2023.

[3] D. Dodson, D. Montgomery, W. Polk, M. Ranganathan, M. Souppaya, S. Johnson, A. Kadam, C. Pratt, D. Thakore, M. Walker *et al.*, "Securing small-business and home internet of things (iot) devices: Mitigating network-based attacks using manufacturer usage description (mud)," National Institute of Standards and Technology, Tech. Rep., 2021.

Abbreviations

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
CCS	Connected Cabin System
CTIS	Cyber Threat Information Sharing
EVM	Ethereum Virtual Machine
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
IDS	Intrusion Detection System
IFE	In-flight Entertainment System
IPS	Intrusion Prevention System
IoT	Internet of Things
LRU	Line Replacable Unit
MUD	Manufacturer Usage Description
NIST	National Institute of Standards and Technology
PHM	Prognostics and Health Management
PUF	Physically Unclonable Function
SCADA	Supervisory control and data acquisition
SRAM	Static Random-Access Memory
TEE	Trusted Execution Environment
TOE	Target of Evaluation
VC	Verifiable Credential

Glossary

Trust Model In the trust model the issuer issues credential to a holder while the holder can prove identity by showing the credential to a verifier.

Manufacturer Usage Description A component-based architecture specified in Request for Comments (RFC) 8520 that is designed to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function.

Cloud Computing Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

Fog Computing As an extension of Cloud computing, Fog Computing brings the computation closer to IoT Edge devices.

Edge Computing Edge computing is the placement of storage and computing resources closer to source, where the data is generated.

Trusted Execution Zone

Line-Replaceable Unit modular component of airplane, designed to be replaced quickly

List of Figures

List of Tables

Appendix A

Installation Guidelines