Speaker:
Dr. Daniele Iorio
daniele.iorio2@unina.it

Security, Analysis, and Implementation of a Distributed Mobility as a Service (MaaS) Application

Valentina Casola, Daniele Iorio
University of Naples Federico II

UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II
Scuola Politecnica e delle Scienze di Base
Corso di Laurea Magistrale in Ingegneria Informatica

Overview

Environment and Problem Introduction

Related Works

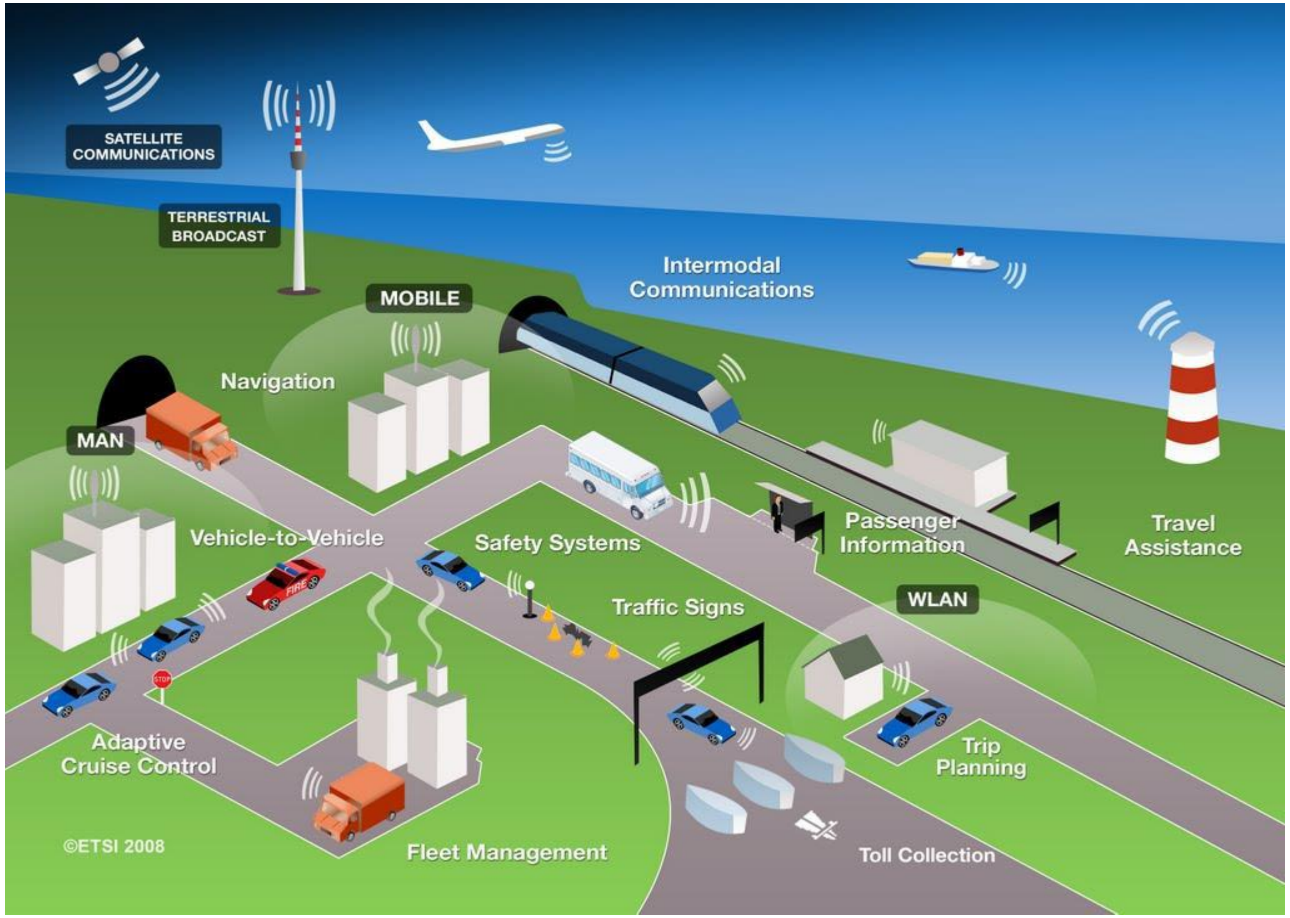
Open Research Challenges

Work Motivation and Proposal

Case Study Description

Environment Introduction

- In the era of **Smart Cities**, **Intelligent Public Transportation System (IPTS)** is devoted to better managing public transport by managing *(near-)real-time* data gathered.
- The **goal** is to:
  - reduce traffic jams and CO_2 emissions,
  - build an integrated, federated and user-friendly system enhancing city ecosystems.
- To achieve the goals, the **Mobility as a Service (MaaS)** paradigm offers integrated solutions to enhance urban mobility providing a **centralized digital hub**.



Related Works

- To understand the progress in this field and the state-of-the-art, we analyzed both literature and existing European projects.

- From the **literature** we identified two promising reference architectures:
  1. One provided by Hitachi Rail [2] suitable since it is a **modular data-oriented architecture**
  2. One proposed by University of Bologna [6] called SMAll (Smart Mobility for All) introducing **multimodal travelling** via a **microservice oriented application**.

- Furthermore, the following European **projects** were considered:
  - MaaS4EU (2017-2020) to understand privacy issues
  - MaaS4Italy (2023-2026) and Borgo 4.0 [8] to understand applied technologies and their security issues
  - MOST (this work contributed to its Spoke 8) to understand the evolution of the research topic.

Open Research Challenges

- At the state-of-the-art there is still a **lack of guidelines** for
  - users and architecture identification
  - definition of standards for data formatting, storing, manipulation, and sharing.

- There is no standard **Reference Architecture** i.e., a blueprint for the system architecture description with crucial features such as cooperation, modularity and law compliance.

- The MaaS environment is used to manage **sensitive data** such as users', traffic, vehicle location, public means of transport occupation, etc.

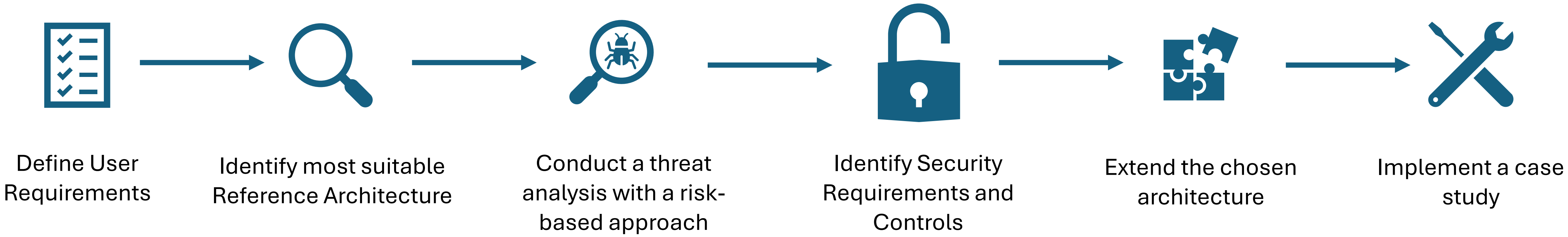
- **Security** and **privacy** of data and infrastructure, are still open issues that may limit full adoption of these applications.

Work Motivation

- Due to the open challenges, the **goal of this work** is to:
  - Identify the main **users and security requirements** of a MaaS application.
  - Identify the most suitable **reference architecture** (general enough to cope with the needs).
  - Perform a **risk-based security analysis** to identify possible threats and related risk.
  - Extend the chosen architecture with **security controls**.

- The **outcome** is to propose a **security-by-design approach** applied to the MaaS environment to mitigate security and privacy related issue following the Software Security Development Lifecycle (SSDL).

Methodology: Security-by-Design



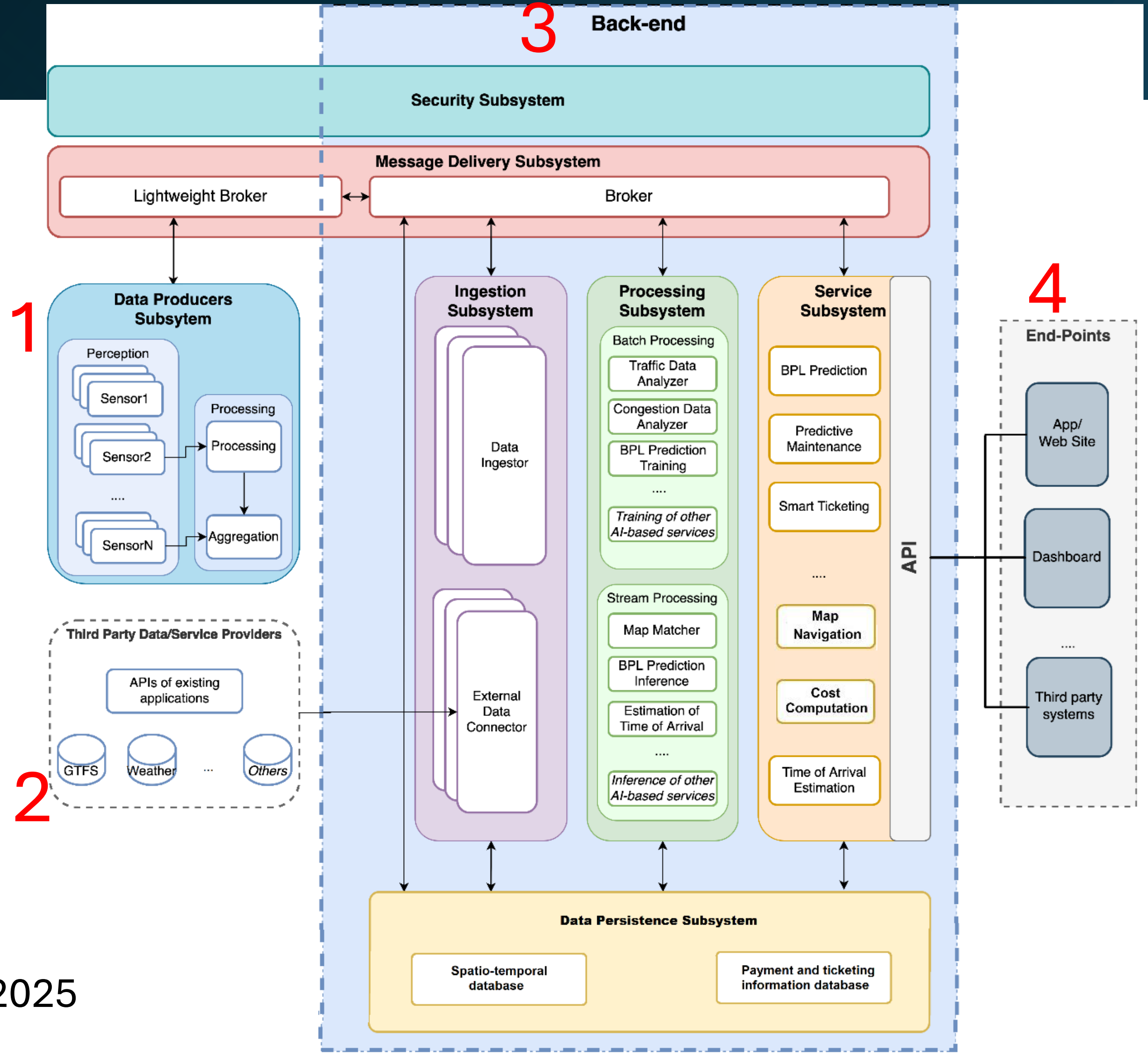
User Requirements and Reference Architecture Identification

➢ To identify the **requirements**, we used:
- SINTEF report [3] → users' definition and context formalization,
- Di Martino et al. [2] and Callegati et al. [6] → existing requirements,
- Cottril et al. [7] and MaaS4EU [4] → privacy concerns and Data Sovereignty Constraints
- Mobility Data Space, and Gaia-X [5] → data sharing in compliance with GDPR

➢ The result is a collection of **32 non overlapping requirements** divided between functional (F), non-functional (NF), security (S), or privacy (P) related.

➢ For the **Reference Architecture** we choose Hitachi Rail IPTS [2] i.e., a modular data-oriented architecture allowing interaction of multiple data sources due to its structure, modularity (thanks to the operating environment), and its public employment.

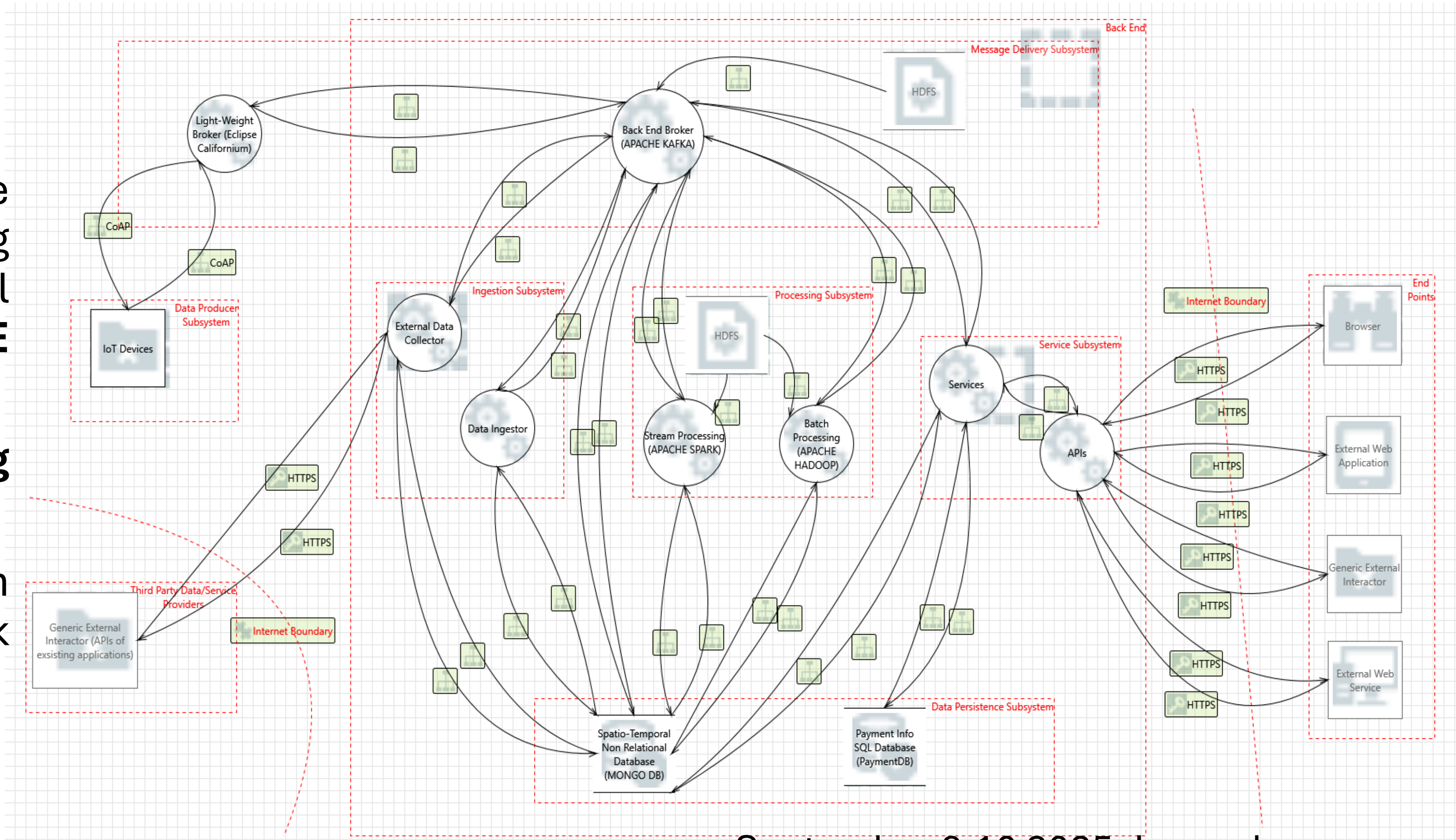
Reference Architecture Details



- The analyzed Reference Architecture is the **Hitachi Rail IPTS** composed by 4 different layers:
  1. Data Producers
  2. Third Party Data or Service Providers
  3. Back End (communication, data, and service management)
  4. End Points

Security Requirements: Reference Architecture Threat Modeling

- A **threat model** of the architecture was realized using the Microsoft Threat Modeling Tool (MTMT) based on **STRIDE** paradigm.
- The analysis allowed a **mapping** between the asset and the threat
- A **risk analysis** was then performed following OWASP Risk Rating Methodology



Threat Modeling Details

Threat family name	*Stride category*	*Identified threat number*
Source & Destination Spoofing	S	21
Authenticated Dataflow Compromised	T	28
Collision Attack & Replay Attack	T	15
SQL Injection	T	8
Potential Data Repudiation	R	38
Weak Authentication Scheme & Access Control,	I	11
Weak Credential Storage	I	20
Denial of Service & Potential Process Crash	D	87
Elevation Using Remote Code Execution	E	25
Elevation Using impersonation	E	59

- MTM Tool returns a threat report categorizing them into:
    1. Spoofing
    2. Tampering
    3. Repudiation
    4. Information Disclosure
    5. Denial of Service
    6. Elevation of Privilege

Security Requirements: Threat Modeling Results

- The total of 308 threats are divided into:
  - 126 marked as “Not Applicable” since they are out of scope
  - 53 already mitigated due to architecture nature
- Leaving 129 active threats resulting in a Medium-High overall risk

Threat Model Summary:

Total	308
Total Migrated	53
Not Applicable	126

Threat	Risk Value
Spoofing	Medium
Authentication dataflow compromised	Medium
Collision and Replay	Medium
SQL Injection	High
Data Repudiation	Medium
Weak Access Control	High
Weak Credential Storage	Medium
Denial of Service	High
Elevation of privilege	Medium

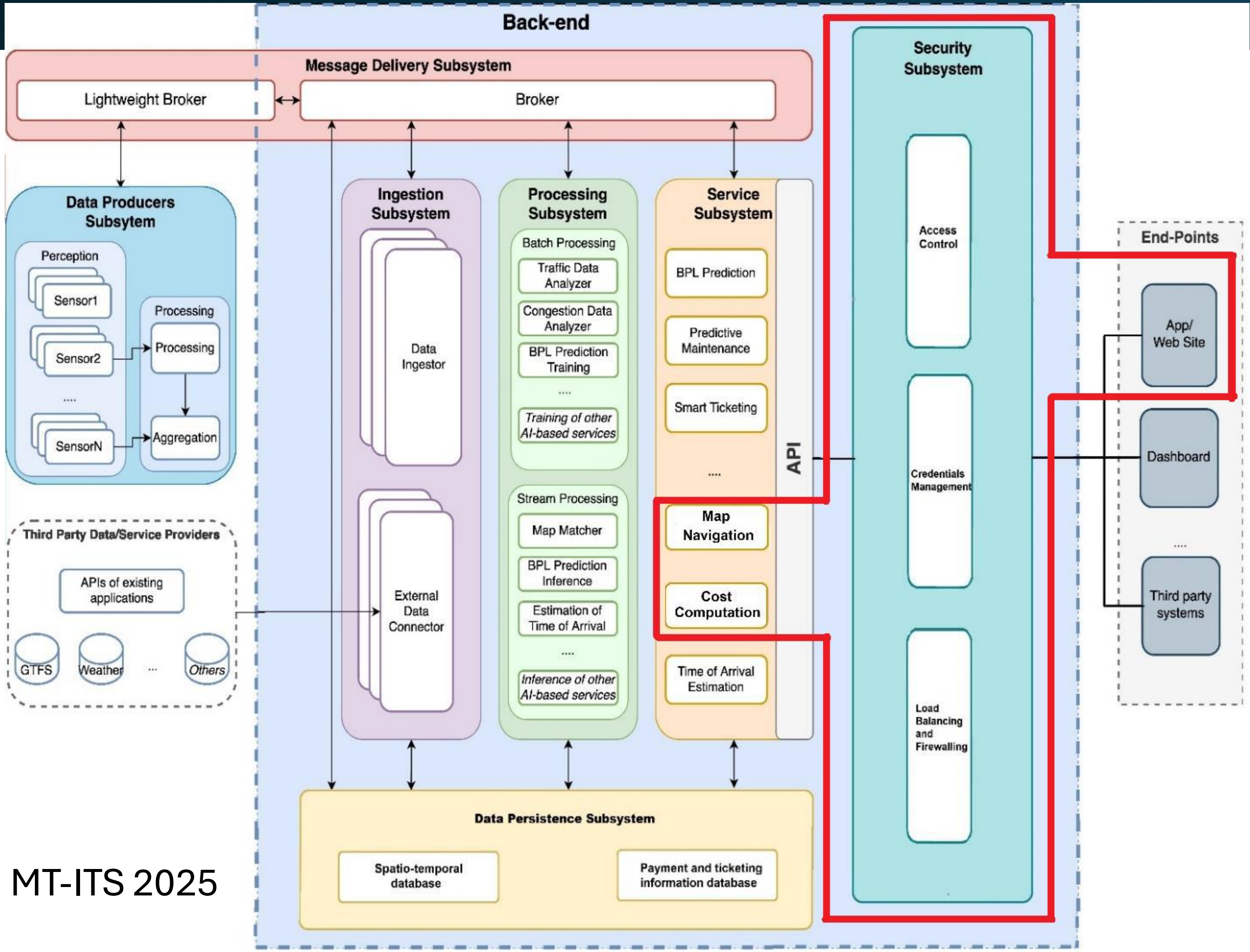
Security Controls Identification

- We relied on **NIST Security Control Framework rev. 5** to identify the needed controls (and their enhancements) to mitigate the threats.

- Families involved in the analysis are:
  1. **Access Control (AC)**
  2. **Audit and Accountability (AU)**
  3. **Identification and Authentication (IA)**
  4. **System and Communications Protection (SC)**
  5. **System and Information Integrity (SI)**

Family ID	*Applicable controls*	*Required level*	*Responsibilities*
AC	10/25	High	Account management Access Enforcement Separation of Duties
AU	12/16	Mid/High	Event Logging Report and Alert Generation Non-repudiation
IA	6/12	High	User identification Authentication Feedback
SC	17/51	High	Separation of System User functionalities DoS, Boundary, and Cryptographic protection
SI	9/23	Mid/High	Malicious Code and Spam protection System Monitoring Error Handling Memory Protection

Extended Reference Architecture

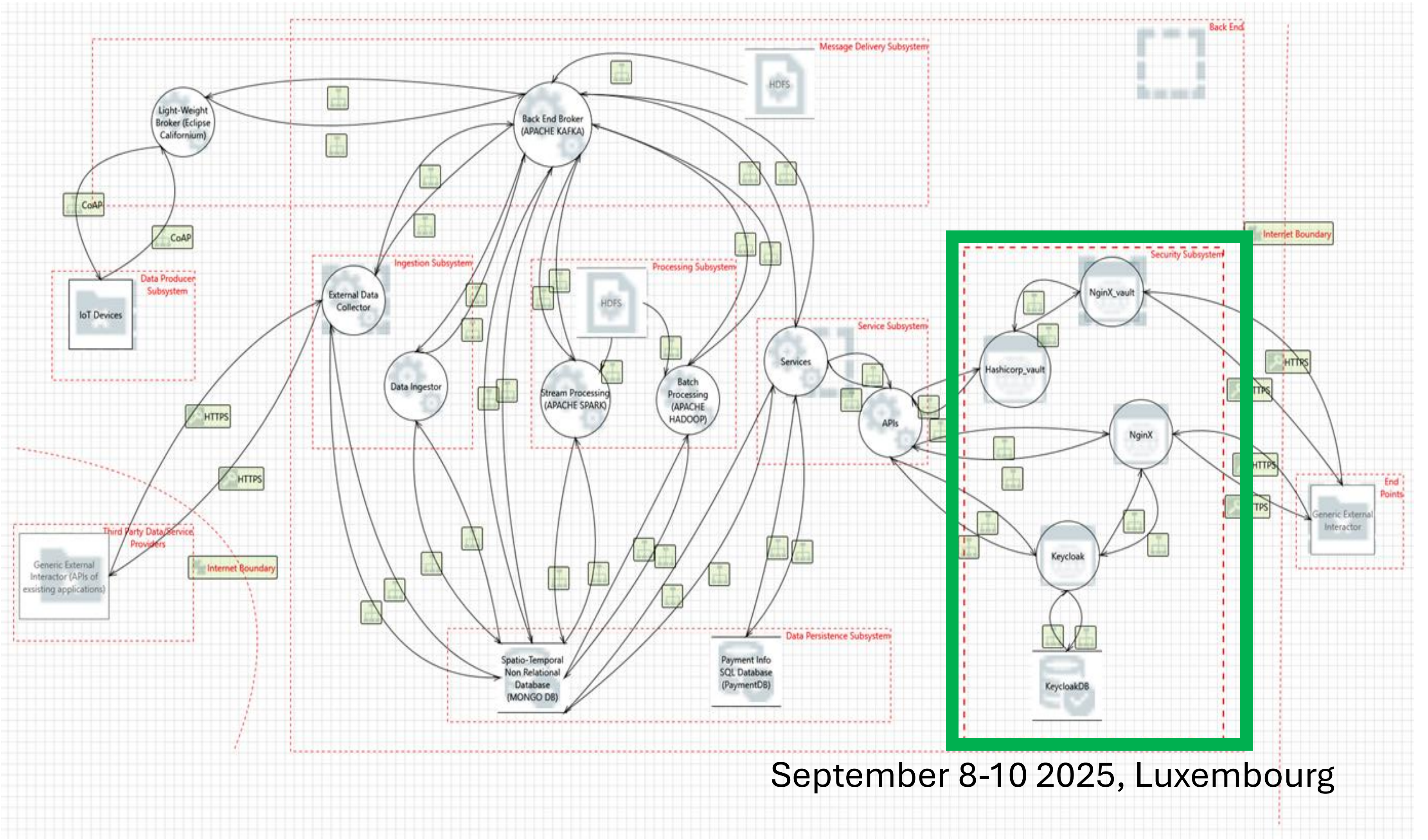


- To implemet the identified controls, the following prototype is proposed
- It provides **two mockup services**:
  - Map Navigation
  - Automatic Cost Computation
- The **Security Subsystem** is built allowing:
  - Access Control
  - Credential Management
  - Load Balancing and Firewalling

Secure Reference Architecture Assessment

- A threat model of the modified architecture is defined to:
  - identify the new set of threats
  - Perform a new risk analysis

- The results will be then compared with the previous ones to validate the controls.



Assessment Results

- The results of the new analysis shows a total of 369 threats of which:
  - 153 were marked as "Not Applicable" since they are out of scope
  - 106 were already mitigated due to the security subsystem implementation and containerization of the architecture
- Leaving 110 active threats resulting in a Medium-Low overall risk due to the change of Likelihood factor

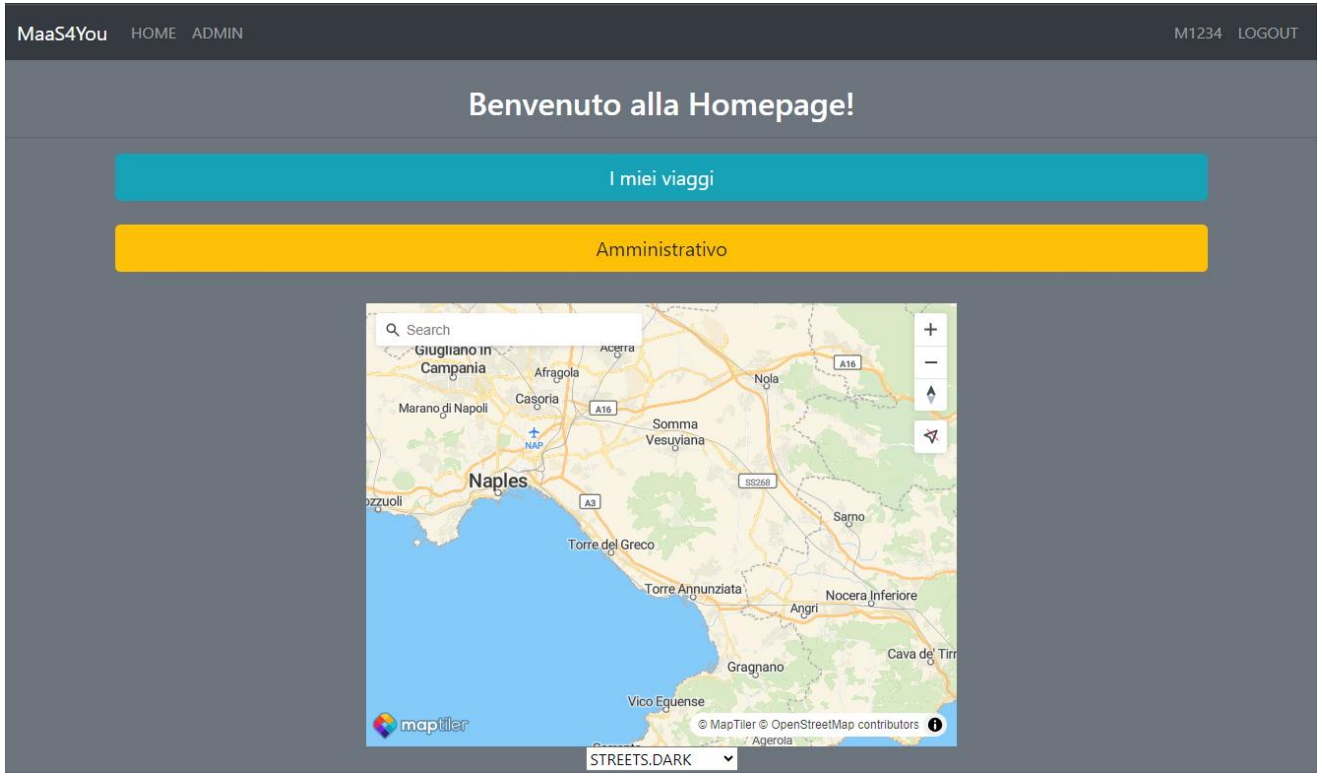
Threat Model Summary:

Total	369
Total Migrated	106
Not Applicable	153

Threat	Risk Value
Spoofing	Low
Authentication dataflow compromised	Low
Collision and Replay	Medium
SQL Injection	Medium
Data Repudiation	Low
Weak Access Control	Low
Weak Credential Storage	Low
Denial of Service	Low
Elevation of privilege	Medium

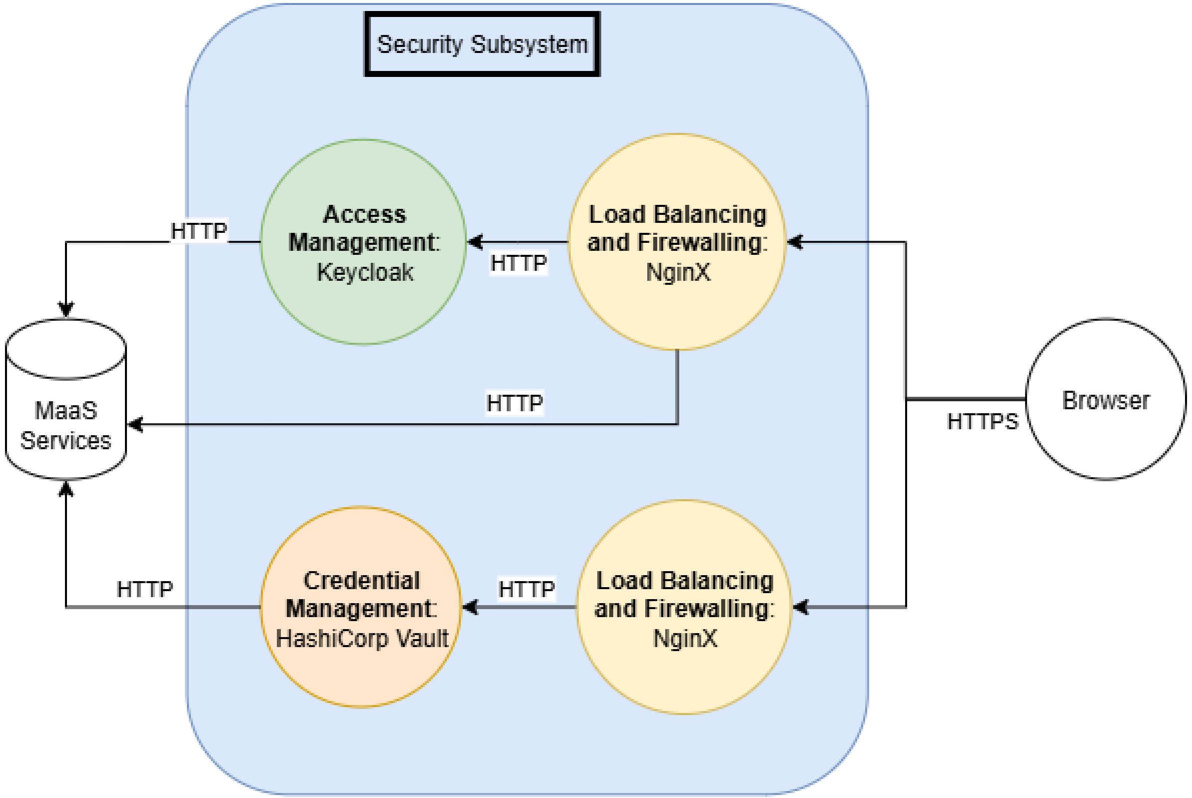
A Case Study: “MaaS4You” application

- As a proof ow work, we propose an **application prototype** developed in JAVA using the *Client-Server* paradigm and the Model View Controller (MVC) architecture.
- Implemented basic functionalities are:
  - Map navigation
  - Trip management lifecycle
  - Automatic cost computation based on the mean of transport



Security Subsystem Details

- The **Security Subsystem** is built using:
  - **Keycloak:** an open-source software for IAM allowing the introduction of a Single Sign-On (SSO) access mechanism
  - **HashiCorp Vault:** an identity-based secrets and encryption management system to safely store usernames, passwords, API keys, certificates, etc.
  - **NginX:** an open-source web server that allows implementations of proxy, reverse proxy, and load balancer.



Technology Details

Technology	Description
Keycloak	Implementation of : • Secure Access via Role and Authentication Based AC • Password lifecycle management • Session Management • Logging and Auditing for accountability purposes • DoS protection
HashiCorp Vault	Implementation of: • Secure Secret management (passwords, certificates, user credentials) via Shamir's Secret Sharing encryption Algorithm (SSSA).
NginX	Implementation of: • System Boundary protection • Secure Communication Protocol using HTTPS certificates and AES encryption

Control Coverage Detail

- For each NIST family identified, the following tables show the security level implemented using the technologies described

Control ID	Level
AC-2	Medium
AC-3	High
AC-4	High
AC-5	High
AC-6	High
AC-7	High
AC-8	High
AC-12	High
AC-18	Medium

Control ID	Level
AU-2	Medium
AU-3	Medium
AU-6	Low
AU-8	Medium
AU-10	Medium

Control ID	Level
IA-2	Medium
IA-3	Medium
IA-4	High
IA-5	Medium
IA-6	High

Control ID	Level
SC-2	High
SC-3	High
SC-4	High
SC-5	Medium
SC-7	Medium
SC-8	High
SC-10	High
SC-12	High
SC-13	High
SC-17	Medium
SC-18	High
SC-23	High
SC-28	High
SC-32	High
SC-39	Medium

Control ID	Level
SI-8	Medium
SI-10	Medium
SI-11	Medium
SI-16	Medium

Conclusions

- This work identified **32 requirements** used to formalize the main needs of users and security for a reference architecture.

- Given the **Reference Architecture**, a security enhancement was proposed and submitted to Hitachi security experts, showing how risk-based security analysis can be applied in MaaS ecosystem following a **security-by-design approach**.

- Furthermore, **security controls extension** is possible thanks to integration with new technologies to deploy additional security and privacy aspects.

Speaker:
Dr. Daniele Iorio
daniele.iorio2@unina.it

Thank you for your attention

Questions?

References

[1] Callegati, F., Gabbrielli, M., Giallorenzo, S., Melis, A., Prandini, M.: Smart mobility for all: A global federated market for mobility-as-a-service operators. In: 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC). pp. 1–8 (2017). https://doi.org/10.1109/ITSC.2017.8317701

[2] Rocco Di Torrepadula, F., Di Martino, S., Mazzocca, N., Sannino, P.: A reference architecture for data-driven intelligent public transportation systems. IEEE Open Journal of Intelligent Transportation Systems 5, 469–482 (2024). https://doi.org/10.1109/OJITS.2024.3441048

[3] Natvig, M.K., Vennesland, A., Stav, E.: Reference architecture for mobility as a service (maas)-stakeholder roles, motivations and use cases. a report from the project Reisenavet (2022)

[4] CORDIS EU research results: End-to-end approach for mobility-as-a-service tools, business models, enabling framework and evidence for European seamless mobility, https://cordis.europa.eu/project/id/723176

[5] Autolitano, S., Pawlowska, A.: Europe's quest for digital sovereignty: GAIA-X as a case study. JSTOR (2022)

[6] Callegati, F., Giallorenzo, S., Melis, A., Prandini, M.: Data security issues in maas-enabling platforms. In: 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI). pp. 1–5 (2016). https://doi.org/10.1109/RTSI.2016.7740624

[7] Cottrill, C.D.: MaaS surveillance: Privacy considerations in mobility as a service. Transportation Research Part A: Policy and Practice 131, 50–57 (2020). https://doi.org/https://doi.org/10.1016/j.tra.2019.09.026

[8] https://www.borgo40.eu/en/