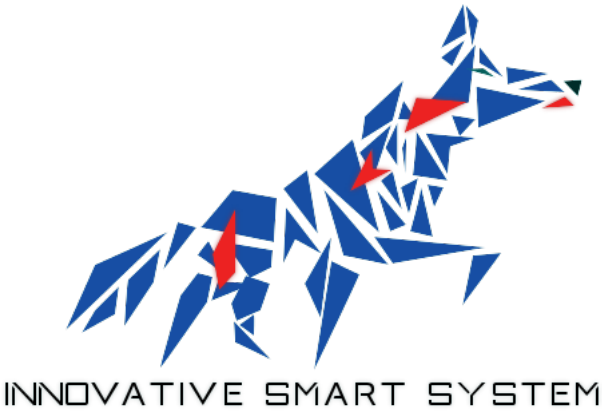
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

2023 - 2024

Security Measures for Water Leak Detection Porject



Abdelmajid Anka Soubaai

Département Génie Électrique et Informatique
135, Avenue de Rangueil
31077 Toulouse Cedex 4

Introduction

Although security was addressed in our English report, I chose to write this report to have a written record of each class we attended (PTP ISS).

To make sure our system stays secure, we followed the EBIOS Risk Manager approach for the security part of the water leak detection project. We did this to understand and deal with potential digital risks. Developed by the folks at ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), EBIOS Risk Manager is all about expressing our needs and figuring out our security goals. This give us a structured way to look at our information setup, helping us get a handle on what we need to do. It's versatile too, fitting into different types of organizations.

1 EBIOS Steps

Ebios follows the following steps

- **Context Establishment:**Understanding the organization's environment, objectives, and constraints.
- **Risk Identification:** Identifying vulnerabilities that could affect the digital assets.
- **Sizing Up the Risks:** Finding the impact of risks.
- **Risk Treatment:** Developing strategies to deal with risks.
- **Action Plan and Monitoring:** Implementing plan to deal with risks.

Now let's zomm a little bit in every steps :

2 Context Establishment

2.1 Project Overview

A device designed to detect water leaks in house implementing it at the water inlet.It collects water consumption data and communicates it to users via a website interface.

2.2 Traget users:

Homeowners or renters interested in monitoring water usage and preventing water damage.

2.3 Technical Environment:

The device connects to home water systems (water inlet) and communicates the data through the WiFi gateway to a server where data is stored and processed. Users access this data through a web interface.

3 Risk Identification :

- **Physical Risks:** Damage to the device from environmental factors, malfunction.
- **Cyber Risks:** Unauthorized access to the device or website, data interception during transmission, malware, and system vulnerabilities.
- **Data Risks:** Loss, corruption, or unauthorized access to water consumption data, which may include personal information about users.
- **Operational Risks:** Device failure leading to undetected leaks, website downtime, or inaccurate water usage reporting.
- **Compliance Risks:** Non-compliance with data protection laws like GDPR (General Data Protection Regulation).

4 Risk Analysis and Evaluation

- **Prioritize Risks:** Prioritize risks such as data breaches, device malfunction, or legal non-compliance (GDPR).
- **Impact Analysis:** Assess the potential impact of each risk on users, the company's reputation, and financial costs.

5 Risk Treatment

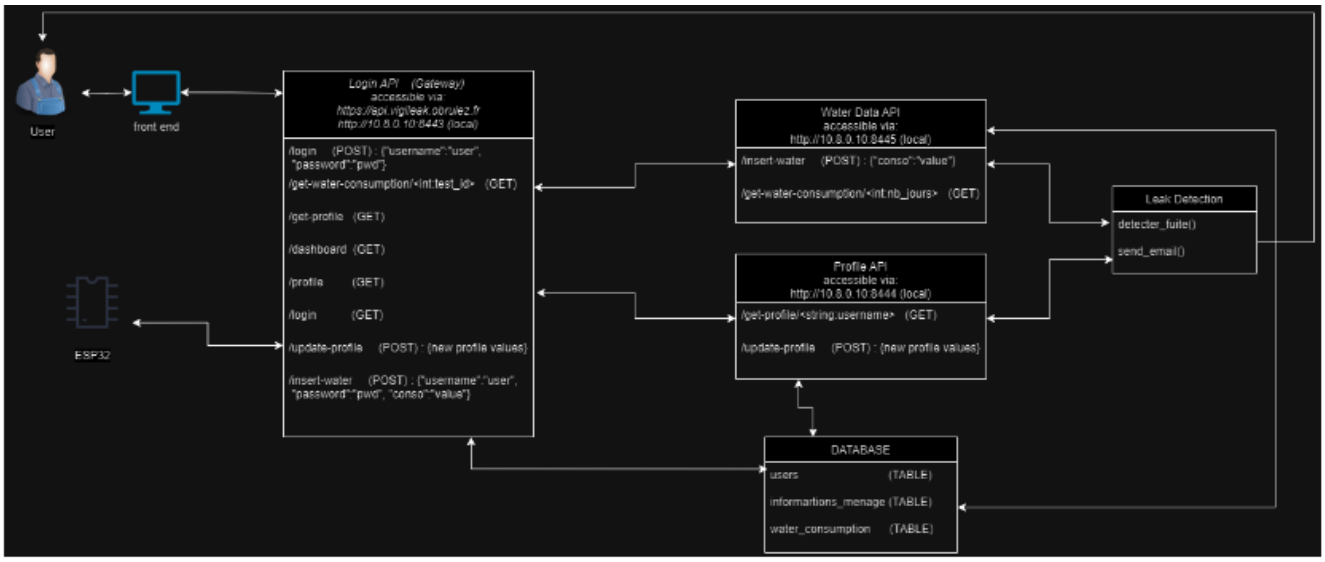
- **Mitigation:** Stay informed about relevant data protection laws (like GDPR) and ensure compliance through regular legal consultations and audits.
- **Avoidance:** Design the system with privacy by design principles, ensuring it meets legal standards from the beginning.

6 Action plan:

We did several actions to ensure the security for the water leak detection project.

First, an important thing to know is that there are principally 2 places where we can intercept data. Between the ESP32 and the server, and between the database and the user interface (website).

Here is the organisation of our micro service architecture :



We chose a protocol of communication for those 2 places, because we use an API, all the data passing through these ways are encrypted with the protocol HTTPS. Even if an attacker intercepts data, he cannot understand the payloads because of the encryption.The infrastructure is accessible by only one gateway that can do only some actions.

We can contact the gateway only with the correct username/password. The rest of the interface is not available, but it can only be made available by having previously given the correct information (username/password). To prevent the user from being able to retrieve information that they are not supposed to access, the server only gives them the rest of the user interface if the user has the connection cookie. To explain it more clearly, when you log correctly into the interface, you get a connection token, and in every communication you have with the server, it verifies if the token is correct, then gives you the interface.

All the ports of the servers are closed, the system respects the minimum security because it hasn't (for the moment) been pwned even if in 2 months, more than 10 000 attacks have been detected.

7 Conclusion

In conclusion, this report serves as a paper trail of the security part in our water leak detection project. We have used the EBIOS protocol and explain the main steps of it and integrate it into our application in order to avoid data leaks in this project.