
SAÉ 203 -



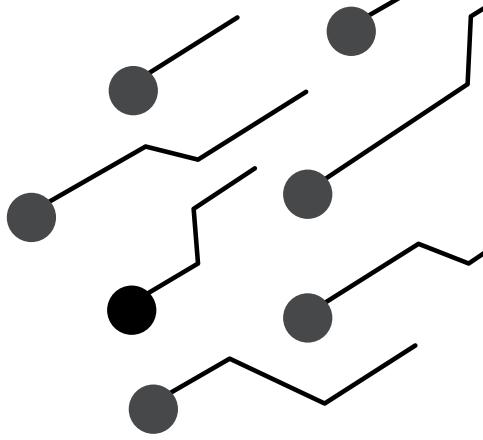
Plateforme de gestion des informations IoT & Cybersécurité



PEREZ Loris

KOKKINOPoulos Iloan

CYBERSÉCURITÉ



Introduction

La cybersécurité est un enjeu fondamental dans le cadre de notre plateforme IoT. Le système repose sur des capteurs connectés communiquant via le protocole MQTT, une base de données centralisée, et une interface web de visualisation. Une analyse a été menée pour identifier les vulnérabilités potentielles de cette architecture.

Identification des vulnérabilités

Vulnérabilité détectée	Catégorie	Détail
Communication non chiffrée sur le port 1883	Réseau	Les données peuvent être interceptées par un attaquant
Absence d'authentification MQTT	Réseau	Tout client peut publier ou s'abonner librement
Requêtes SQL	Injection SQL	Refactorisation du code
Données du capteur	Données aberrantes	Le capteur peut avoir un bug et envoie des données irréelles

Analyse du réseau via Wireshark

The screenshot shows a Wireshark capture of MQTT traffic. The packet list shows several TCP and MQTT frames. A red box highlights a MQTT Publish frame (packet 195) with the following payload:

```

{
    "api_time": "2025-05-28T12:30",
    "temperature": 23,
    "wind_speed": 12.0,
    "wind_direction": 291,
    "query_time": "2025-05-28T14:35:51"
}
  
```

The details pane shows the MQTT message structure, including the topic and payload.

→ Message de “Publish” visible en clair sur le réseau

→ La requête “Subscribe Request” a été accepté par le broker sans avoir besoin d’identifiant / mdp

Mesures correctives

• Communication non chiffrée sur le port 1883

Le protocole MQTT qui est utilisé sur le port 1883 ne chiffre pas les communications. Un attaquant placé sur le réseau peut intercepter les messages échangés entre les appareils connectés et le serveur.

Mesure de sécurité recommandée :

- Mettre en place MQTT TLS sur le port 8883 afin de chiffrer les données en transit.
- Générer et configurer des certificats SSL/TLS sur le broker MQTT.
- Forcer tous les clients à se connecter uniquement via une connexion sécurisée.

• Absence d'authentification

Aucune authentification n'est requise pour publier ou s'abonner à un topic MQTT. Tout utilisateur peut manipuler librement les données.

Mesure de sécurité recommandée :

- Éviter les brokers publics.
- Activer l'authentification par nom d'utilisateur et mot de passe sur le broker MQTT.
- Journaliser tous les messages pour pouvoir détecter les anomalies

• Données aberrantes issues des capteurs

Des capteurs défaillants (ou un bug) peuvent envoyer des données irréelles, comme des températures extrêmes ou incohérentes.

Mesure de sécurité recommandée :

- Mettre en place une vérification de la cohérence des données.
- Ajouter un système de filtrage ou de détection d'anomalie.
- Journaliser les valeurs rejetées pour analyse et maintenance.

Conclusion

La mise en place d'une plateforme de gestion d'informations IoT soulève de nombreux enjeux de cybersécurité.

Notre analyse a mis en évidence plusieurs vulnérabilités critiques : absence de chiffrement lors des échanges MQTT, manque d'authentification des clients, possibilité d'injection SQL dans l'interface web, ainsi que des risques liés à l'intégrité des données collectées (capteurs défectueux ou données irréelles).

Ces faiblesses peuvent avoir des impacts : interception de données sensibles, prise de contrôle du système par un attaquant, altération des tableaux de bord ou décisions fondées sur de fausses données.

Pour corriger ces menaces, plusieurs solutions doivent être mises en œuvre : activation du chiffrement TLS, mise en place d'une authentification côté MQTT, renforcement du code PHP contre les injections SQL.

Lorsque le broker MQTT est hébergé à l'extérieur, des mesures complémentaires comme le choix de fournisseurs sécurisés ou l'interposition d'un proxy local permettent de restaurer un certain contrôle.

Ce travail montre que la sécurité d'un projet IoT ne se limite pas au réseau, mais concerne l'ensemble de la chaîne d'information.

Une démarche rigoureuse, documentée, et continue est essentielle pour garantir la fiabilité et la résilience d'une solution.

SAÉ 203 –



**Plateforme de gestion
des informations IoT &
Cybersécurité**

PEREZ Loris

KOKKINOPoulos Iloan