Plateforme de tests d'attaques pour l'I-IoT

Auteurs : CHAPEL Antoine – CAVASSILA-BEUF Antoine – HOARAU Hugo

CONTEXTE ET OBJECTIF

Le programme PULSE de l'IRT Nanoelec vise à développer la cybersécurité, notamment dans le domaine de l'IoT et de l'I-IoT. Face à l'essor inédit de la cybercriminalité, il devient important pour les partenaires industriels de détecter dès que possible les menaces et de répondre aux cyberattaques.

Les objectifs de ce projet sont :

- Développer un banc de tests simulant une infrastructure industrielle
  - Le procédé physique simulé est un barrage hydroélectrique
  - Des automates émulés permettent de contrôler ce procédé physique
  - Un serveur permet la visualisation de son fonctionnement et son pilotage
- Implémenter différents scénarios de cyberattaques sur cette infrastructure afin de modifier son comportement.

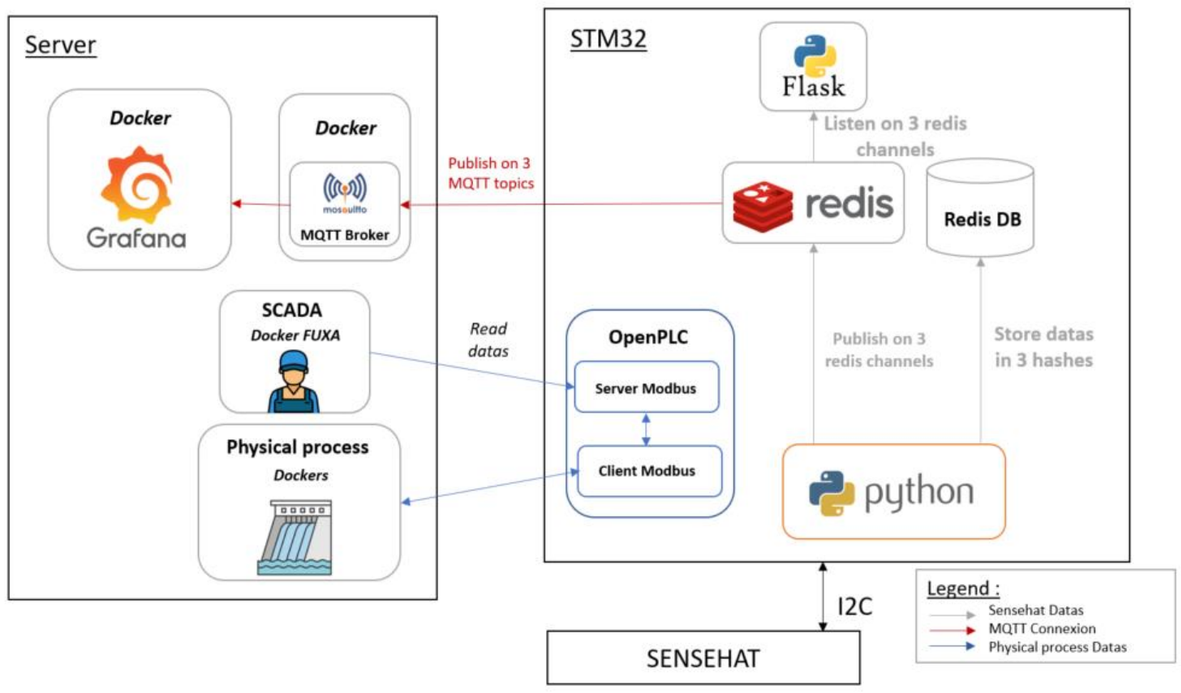
MÉTHODES ET DÉVELOPPEMENTS

L'organisation du projet s'est basée sur le méthode Agile SCRUM, avec une réunion hebdomadaire servant à présenter le travail effectué durant la semaine et à planifier la semaine suivante. Cela a rendu le projet plus modulable en donnant des retours rapides sur le développement du banc de test et des attaques.

Le banc de tests est composé de 3 éléments principaux :

- une carte multi-capteurs/actionneurs Raspberry Pi Sensehat
- Une carte électronique, basée sur processeur STMicroelectronics STM32MP1, émule un automate
- Un serveur simule un barrage hydroélectrique, intègre un logiciel SCADA et la remontée des données capteurs

Les principaux outils de développement utilisés sont Buildroot pour la création du Linux embarqué mais également Redis et Influxdb pour la gestion de base de données ou encore Docker, Grafana et Python.



RÉSULTATS ET CONCLUSION

Les équipes de l'IRT Nanoelec disposent d'un banc de tests fonctionnel permettant d'exécuter de nombreuses attaques. Cette exécution comprend également la restauration des cibles attaquées afin de pouvoir reproduire les tests rapidement.

Ce projet doit servir de base pour:

- Le développement d'une solution de détection de cyberattaques en permettant la génération de datasets pour entrainer et tester des modèles de machine learning
- Le développement de mécanismes de réponse et de restauration suite aux différentes attaques exécutées

L'ensemble de ce projet sera également mis en open source et fera l'objet d'une publication scientifique.

MOTS-CLÉS : I-IoT, Sécurité embarquée, Attaques, Système industriel