Protection de gateway IoT contre des menaces logicielles et sur les communications **TrustGW**

Programme : **CE39**

Instrument : **PRC**

Contact : **Guy GOGNIAT**

COORDINATEUR : Lab-STICC (guy.gogniat@univ-ubs.fr)

PARTENAIRE : IRISA, IETR

Résumé :
Le projet TrustGW vise à développer une architecture hétérogène logiciel-matériel de gateway reconfigurable dynamiquement et de confiance : Architecture de gateway hétérogène garantissant des propriétés de confidentialité, d'intégrité, de disponibilité, et d'authentification.

https:\\trustgw.projects.labsticc.fr

CONTEXTE ET OBJECTIFS

Le système est composé d'objets connectés à une gateway reliée à des serveurs de calculs. L'architecture de la gateway est hétérogène logiciel-matériel :

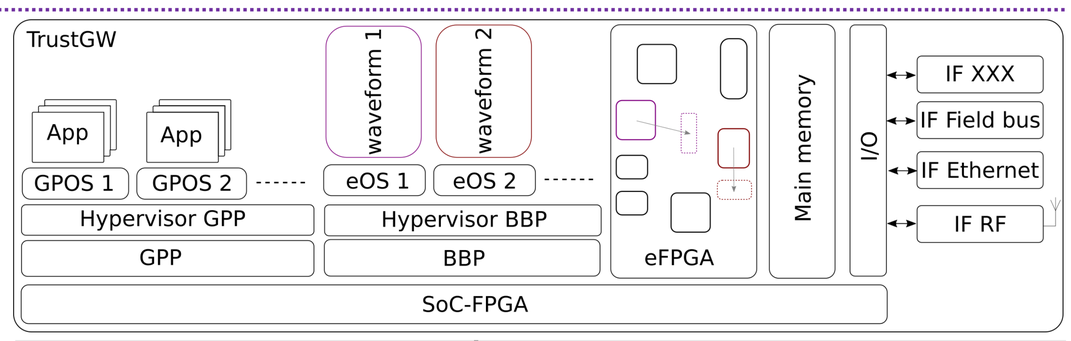
- Processeurs applicatifs et bande de base
- Accélérateurs matériels implémentés sur FPGA
- Machines virtuelles pour déployer les services des opérateurs de façon cloisonnée

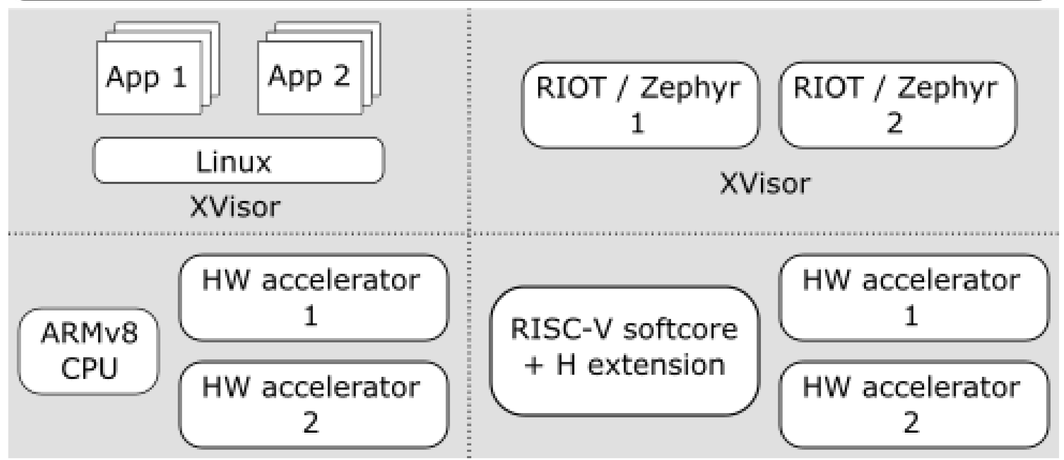
MÉTHODOLOGIE ET RÉSULTATS

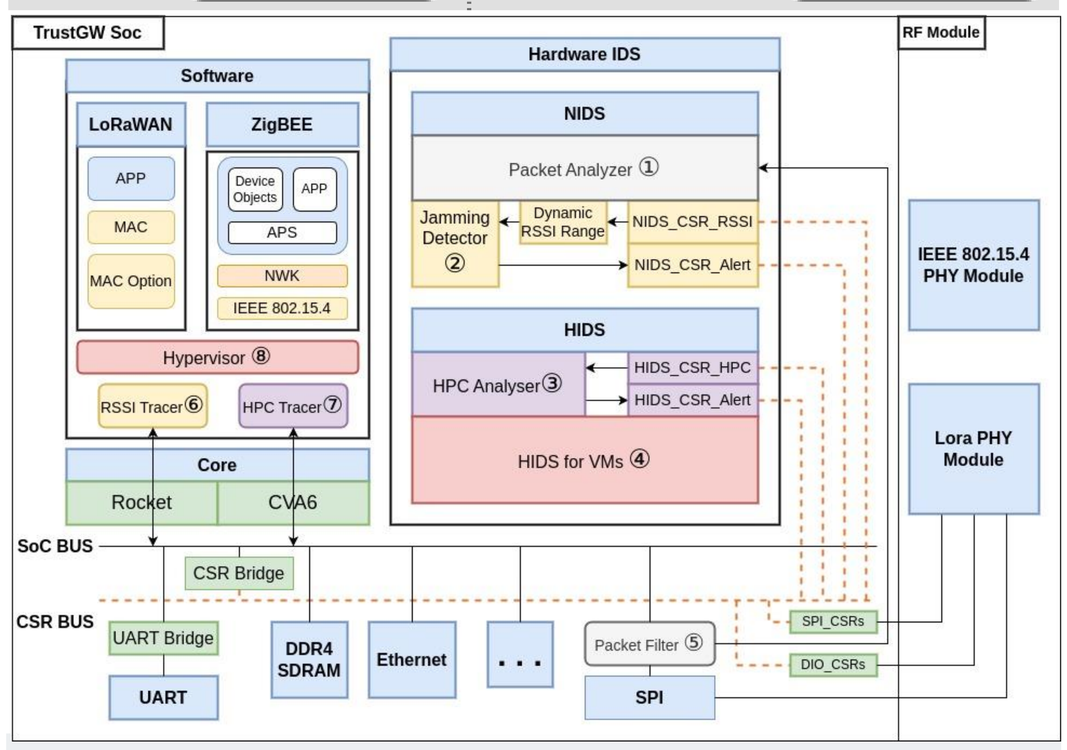
- WP1 : Sécurisation de l'architecture de communication de la gateway (thèse de Tianxu Li)
  - Développment d'un Hardware-assisted Intrusion Detection System (HIDS) prenant en compte les paramètres suivants : multi-metrics (HPC, RSSI, ...), multi-level (HW, SW, NW) et multi-protocols (LoRaWAN et ZigBee)

- WP2 : Sécurisation de l'hyperviseur et des ressources virtualisées -> Voir le poster de la thèse de Aya Jendoubi

- WP3 : Sécurisation des applications au sein des machines virtuelles - Introspection de machines virtuelles via un hyperviseur pour renforcer la sécurité du système d'exploitation (thèse de Lionel Hemmerlé).
  - Développement d'un DSL permettant à un système d'exploitation de décrire des invariants sur ses structures de données internes durant son exécution.
  - Développement d'un patch pour un hyperviseur (Xvisor) permettant de détecter dynamiquement les violations d'invariants.
  - Evaluation de la détection des attaques décrites précédemment sur un noyau Linux, et évaluation de l'impact de ce renforcement de la sécurité sur les performances des VM.
- WP3 : Sécurisation des applications au sein des machines virtuelles - Suivi de flux d'information pour des applications hybride fonctionnant sur CPU et FPGA (stages de M2 de Romain Ninot et Oumar Niang)







VALORISATION ET PERSPECTIVES

Plusieurs publications et présentations, voir le site : https:\\trustgw.projects.labsticc.fr

1ère rencontre, le 26 janvier 2023, avec le comité scientifique industriel : Thales, Orange, AMD (Xilinx), Vosys, ANSSI et DGA MI.

Briques technologiques en cours de développement. 1er éléments d'intégration visés pour l'automne 2024 (développements en open-source)

Lien avec les formations pour développer les expertises liées au projet : Master Erasmus Mundus CYBERUS, CMA CyberSkills4All…