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

TrustGW

Programme : **CE39**

Édition : **2021**

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.

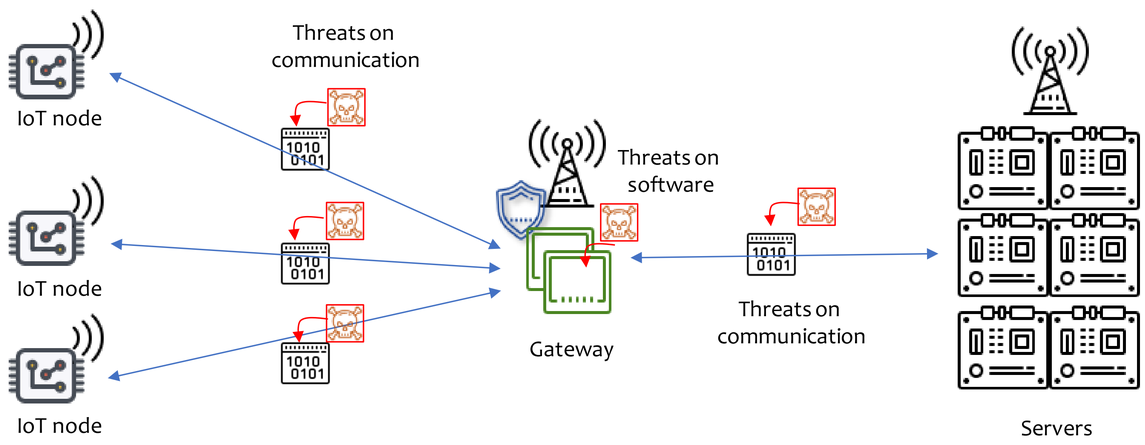
https:\\trustgw.projects.labsticc.fr

CONTEXTE ET OBJECTIFS

Les systèmes embarqués communicants se répandent massivement dans des infrastructures critiques.

Ils contribuent à un meilleur contrôle et une plus grande optimisation pour à la fois augmenter leur efficacité et leur usage et répondre à des défis sociétaux.

MAIS Ils participent à l'augmentation de la surface d'attaque globale des systèmes d'information ce qui représente une menace sans précédent.



Le système considéré est composé d'objets connectés à une gateway qui elle-même est connectée à un ou plusieurs serveurs de calculs

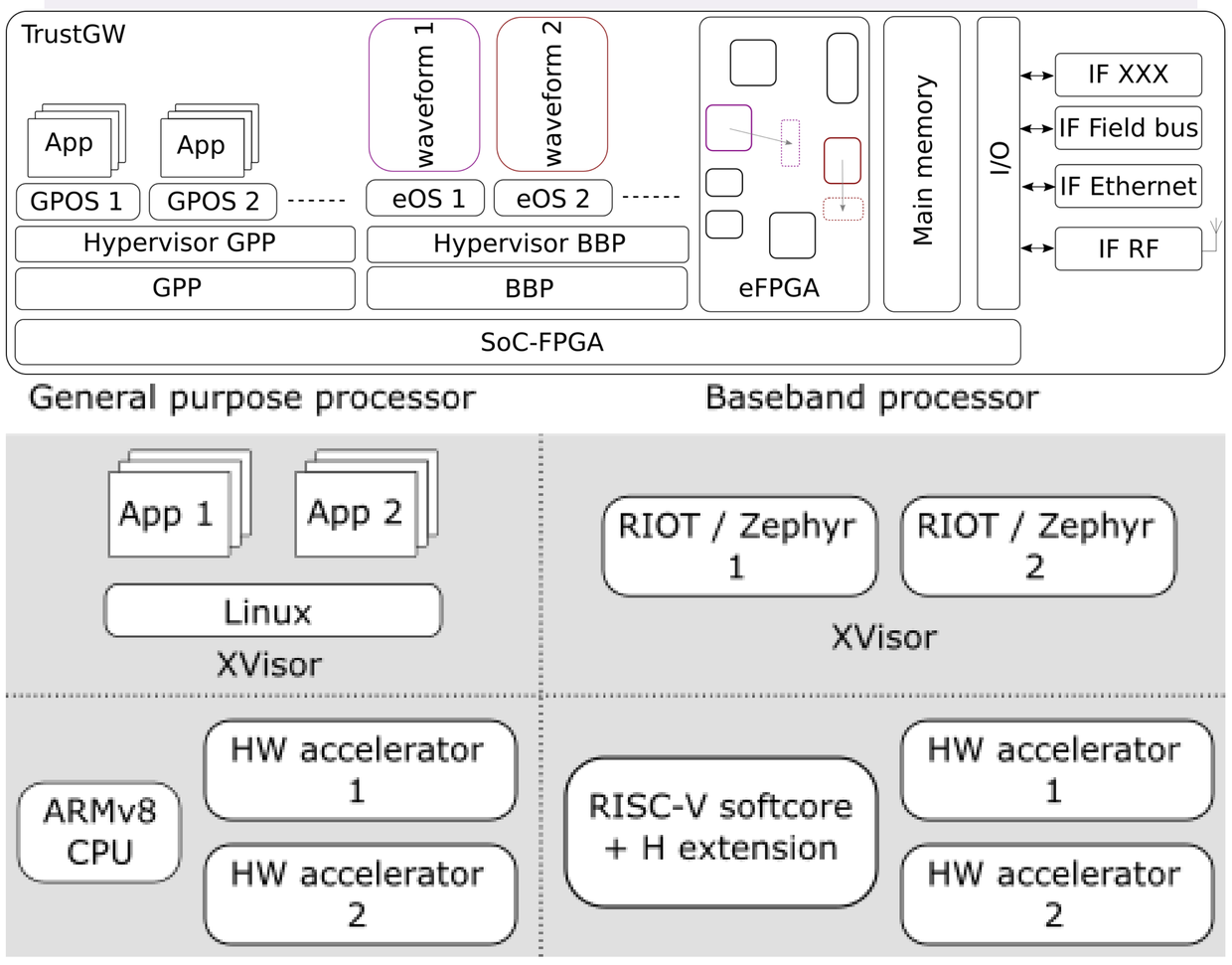
L'architecture de la gateway est hétérogène logiciel-matériel

- Plusieurs processeurs (processeur bande de base, processeur applicatif)
- Accélérateurs matériels implémentés sur FPGA (les ressources FPGA sont virtualisées afin d'avoir une vue uniforme du point de vue des applications)
- La gateway embarque plusieurs machines virtuelles afin de pouvoir déployer les services des différents opérateurs qu'elle héberge et cela de façon cloisonnée
- Architecture de gateway hétérogène garantissant des propriétés de confidentialité, d'intégrité, de disponibilité, et d'authentification

MÉTHODOLOGIE ET RÉSULTATS

Trois principaux défis scientifiques :

- Architecture de gateway hétérogène logiciel-matériel reconfigurable dynamiquement de confiance
- Hyperviseur de confiance permettant de déployer des machines virtuelles sur une architecture hétérogène logiciel-matériel avec une virtualisation des ressources
- Sécurité des applications au sein des machines virtuelles



VALORISATION ET PERSPECTIVES

Les développements réalisés seront open-source afin de garantir leur audit et faciliter le transfert vers les acteurs du domaine.

Mise en place d'un comité scientifique industriel Thales, Orange, AMD, Vosys, ANSSI et DGA MI.

Irriguer les formations afin de développer les expertises liées à ces problématiques et aux enjeux associés