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

Gogniat Guy[1], Tanguy Philippe[1], Cotret Pascal[2], **Hiet Guillaume**[3], Tronel Frédéric[3], Wilke Pierre[3], Prévotet Jean-Christophe[4], Nouvel Fabienne[4], and Dardaillon Mickaël[4]

[1]Lab-STICC (UBS) [2] (ENSTA Bretagne) / [3]IRISA (CentraleSupelec) / [4]IETR (INSA Rennes)

— **Porteur principal** : Guy Gogniat (Lab-STICC/UBS)
— **Consortium** : Lab-STICC (UBS), IRISA (CentraleSupelec), IETR (INSA Rennes)
— **Financement** : ANR PRC
— **Dates** : sélection en 2021, travaux scientifiques du 01/01/2022 au 31/12/2025
— **TRL** : 1-4

1 Contexte des travaux

Nous considérons un système composé d'objets connectés à une gateway qui, elle-même, est connectée à un ou plusieurs serveurs de calculs (déployés par exemple dans le cloud). Les objets connectés (nœuds IoT) transmettent et reçoivent des données de la gateway. Chaque nœud communique potentiellement avec une forme d'onde différente (p. ex. LoRaWAN et Bluetooth). En outre, la gateway permet de réaliser un traitement local sur les données issues des nœuds IoT (architecture de type *edge computing*). Nous faisons l'hypothèse que la gateway est mutualisée et exécute différentes applications pour le compte de différentes entités. Il est donc nécessaire de partager les ressources matérielles de la gateway entre les différentes applications et d'isoler/protéger ces différentes applications.

L'architecture de la gateway est hétérogène (logicielle-matérielle), composée d'un processeur bande de base (BBP), d'un processeur applicatif (GPP) et d'accélérateurs matériels implémentés sur un FPGA. Ces derniers sont déployés dynamiquement en fonction des besoins d'accélération des applications à un instant donné. Le GPP permet d'exécuter les applications de type edge computing et le BBP est dédié à la gestion des communications et des différentes formes d'ondes.

2 Verrous scientifiques et technologiques

Le projet **TrustGW** adresse trois principaux défis scientifiques et technologiques :

— C1 : Concevoir une architecture hétérogène logiciel-matériel, de confiance et reconfigurable dynamiquement ;
— C2 : Proposer un hyperviseur de confiance permettant de déployer des machines virtuelles sur une architecture hétérogène logiciel-matériel avec une virtualisation des ressources ;
— C3 : Garantir la sécurité des applications au sein des machines virtuelles.

3 Pistes de recherche

Pour relever ces défis, le projet explore trois pistes de recherche :

1. Développer un hyperviseur permettant d'offrir une gateway hétérogène logiciel-matériel sécurisée reconfigurable dynamiquement (thèse Aya Jendoubi)
   — Virtualisation des ressources CPU, mémoire et FPGA
   — Exécution de service de confiance (reconfiguration du FPGA)
2. Développer des mécanismes de sécurité directement au niveau du BBP (thèse Tianxu Li)
   — Développement d'un moniteur pour détecter des attaques visant les communications radio
   — Extensions du processeur pour accélérer/protéger les traitements radio
3. Protéger/isoler les applications s'exécutant sur le GPP
   — Développement de suivi d'information (DIFT) permettant de surveiller les applications hybrides, qui déportent une partie de leur calcul sur FPGA
   — Protection du noyau des différentes VM par introspection depuis l'hyperviseur, via un langage dédié (thèse Lionel Hemmerlé)

L'environnement de développement retenu est une carte Zynq UltraScale+ MPSoC ZCU104 avec un processeur ASIC ARM (GPP). Le BBP sera un softcore RISC-V sur FPGA (Rocket ou CVA6). Les travaux sur l'hyperviseur se baseront sur Xvisor.