Configuration sécurisée d'infrastructure de communication IoT « by design »

Projet CyberExcellence

https://cyberwal.be/cyberexcellence/

Jeudi 06/04/2023

Défi 07 : Configuration sécurisée d'infrastructure de communication IoT « by design »

- Personne de contact : Nicolas Point (MULTITEL)
- Problème industriel
  - Sécurisation des infrastructures de communication (principalement mobiles)
  - Communication des équipements de type IoT dont l'utilisation ne fait que croître :
    - Communications dans la zone OT d'une entreprise
    - Communications en espace "public" : Smartcities, Intelligent Transport Systems...
  - En conjonction avec d'autres défis (réseaux énergétiques, CPS...)

Défi 07 : Configuration sécurisée d'infrastructure de communication IoT « by design »

- Challenges de recherche possibles
  - Développement de composants cryptographiques, d'infrastructures et/ou de protocoles adaptés ou développés spécifiquement pour un type d'application
  - Étude et implémentation de tous les éléments assurant un niveau de sécurité très élevé de la transmission des données, du capteur au serveur final de stockage (éventuellement dans le cloud, privé ou public)
- Impact industriel
  - Amélioration de la cybersécurité des infrastructures IoT (dès l'installation)
  - Développement de produits concurrentiels (de plus en plus de demandes des clients)
  - Alignement (ou anticipation) avec les référentiels industriels (NIS...)

Défi 07 : Configuration sécurisée d'infrastructure de communication IoT « by design »

- Equipes universitaires/CRA impliqués :

  - Prof. B Quoitin, Prof. P. Megret (Umons) : IoT devices & physical layer
  - Prof. Axel Legay (UCL) : Résilence aux cyberattaques
  - Prof. Benoit Donnet (ULiège) : Voir Défi « Réseau énergétique »
  - Christophe Ponsard, Sébastien Dupont (CETIC) : Systèmes Cyberphysiques
  - …

  Entreprises intéressées :

  - Thales, Icare, VocSens, ACIC…