Partenaires

Pôles de compétitivité

Soutiens

Avec la participation de :

10/11/2020

PACLIDO

Présentation

Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets

Agenda

	Sujets	Présentateurs
09h30 – 10h15	Présentation du projet PACLIDO	Nicolas Darnet (Airbus CyberSecurity) Guillaume Séraphine (Saint-Quentin en Yvelines) Paul-Emmanuel Brun (Airbus CyberSecurity)
10h15 – 10h40	Présentation du démonstrateur Domotique	Alexis Duque (Rtone)
10h40 – 11h05	Accélération matérielle de l'algorithme LILLIPUT-AE sur cœur RISC-V	Mikaël Le Coadou (CEA)
11h05 – 11h30	Présentation du démonstrateur Industrie	Paul-Emmanuel Brun (Airbus CyberSecurity)
11h30 – 12h10	Présentation du démonstrateur Smart City	Jawad Didouh (Sophia Engineering)
12h10 – 12h30	Questions / Réponses	

Objectif du projet

- **PACLIDO** -> **P**rotocoles et **A**lgorithmes de **C**ryptographie **L**égers pour l'**I**nternet **D**es **O**bjets

- Intégration dans des objets connectés d'algorithmes et de protocoles de cryptographie **légers** garantissant :
  - la confidentialité
  - l'intégrité
  - l'authentification

- des données échangées entre un objet connecté et un serveur.

Objectifs

- Développer des algorithmes efficaces sur les **3 plateformes majoritairement utilisées dans l'IoT** : MSP430, ATMEGA, ARM Cortex
- Développer des algorithmes significativement **plus performants** que les standards actuels du marché (tous américains) : gain en vitesse, gain en énergie…
- S'engager dans un processus de **standardisation** des différents algorithmes et protocoles développés dans le cadre du projet
- Assurer et valider la sécurité physique des ces implémentations cryptographiques
- Supervision d'un réseau IoT
- **3 use cases**

Cadre du projet

bpifrance SERVIR L'AVENIR

Cadre de financement : FUI 23 (Fonds Unique Interministériel) **BPI, DGE**

Durée des travaux : 3 ans

Date de début : 1er Décembre 2017

Pôle de compétitivité : Systematic (Ile-de-France), SCS (PACA), Minalogic (Auvergne-Rhône-Alpes), ALPHA-RLH (Limoges)

Systematic Paris Region Deep Tech Ecosystem Cyber & Security

POLE SCS

MINALOGIC

ALPHA RLH

Consortium

- Compétences clé des partenaires :
  - **Cryptographie et sécurité** (Airbus CyberSecurity, LORIA-CNRS, Univ. Limoges, CEA)
  - **IoT Ecosystem** (Rtone, Sophia Engineering, Trusted Objects)
  - **Utilisateurs finaux** orientant et supportant le projet (SQY, Lacroix, CCE)

Soutiens :

Avec l'aide de :

SAINT QUENTIN EN YVELINES
Terre d'innovations

Smart City
L'enjeu de la cybersécurité

- Rôle de tiers de confiance des collectivités
- Efficience des services par la digitalisation
- Augmentation importante des surfaces d'attaque (Iot/Télétravail)
- Recrudescence de la menace pour les collectivités
- Complexité de déploiement de solutions « Secure by design »

3 cas d'usage

- Smart City : sécurisation de deux parcs de lampadaires communiquant au travers d'un réseau LORAWAN
- Domotique : sécurisation d'une clef dynamométrique au travers du protocole BLE
- Industrie 4.0 : sécurisation de bout en bout et déploiement sécurisé de capteurs communiquant via le protocole LORAWAN

Smart city

Domotique

Industrie 4.0

Principales réalisations

- Définition et implémentation du protocole de chiffrement léger appelé Lilliput-AE
- Validation sécuritaire matérielle et logicielle de ces implémentations
- Développement de différentes solutions intégrant ce protocole
- Intégration de ces solutions dans différents cas d'usages

Solutions PACLIDO

1. Gateway LoRaWAN totalement intégrée incluant l'algorithme de cryptographie Lilliput-AE
2. Secure Element qui implémente Lilliput-AE
3. Intelligence artificielle permettant la détection d'anomalies sur des réseaux IoT
4. Couche de sécurité logicielle permettant de sécuriser une liaison BLE
5. Surcouche de chiffrement de bout en bout entre des capteurs et une application finale

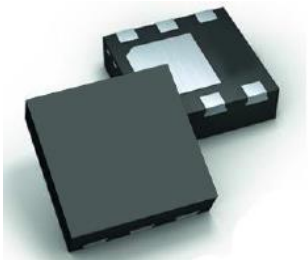
Solutions PACLIDO
1- Gateway LoRaWAN

- Passerelle réseau matérielle totalement intégrée incluant les composants suivants :
  - Packet forwarder
  - LoRaWAN Network Server
  - LoRaWAN Application Server
  - Accès distant sécurisé

- Protocole LoRaWAN optimisé par :
  - Intégration de l'algorithme Lilliput-AE à la place de l'AES

- Cas d'usage typique :
  - Déployer un réseau LoRaWAN local, facilement et rapidement, en optimisant la sécurité et les performances par rapport aux systèmes traditionnels à base d'AES

Solutions PACLIDO
2- Secure Element



- Composant matériel :
  - Permettant d'intégrer l'algorithme de chiffrement Lilliput-AE et de stocker les clefs de manière sécurisée,
  - Le tout protégé contre les attaques physiques

- Exemple de cas d'usage :
  - Mise en œuvre de Lilliput-AE de manière sécurisée. Intégration du SE dans un capteur pour s'assurer qu'il est protégé contre les attaques physiques.

Solutions PACLIDO
3- Logiciel d'IA pour la détection d'anomalies

- Composant logiciel permettant la détection d'anomalies sur des réseaux IoT grâce à des mécanismes d'IA utilisant à la fois des données envoyées par les objets mais aussi des métadonnées

- Composant pouvant être intégré dans une Gateway ou utilisé de manière centralisée (dans un SOC par exemple)

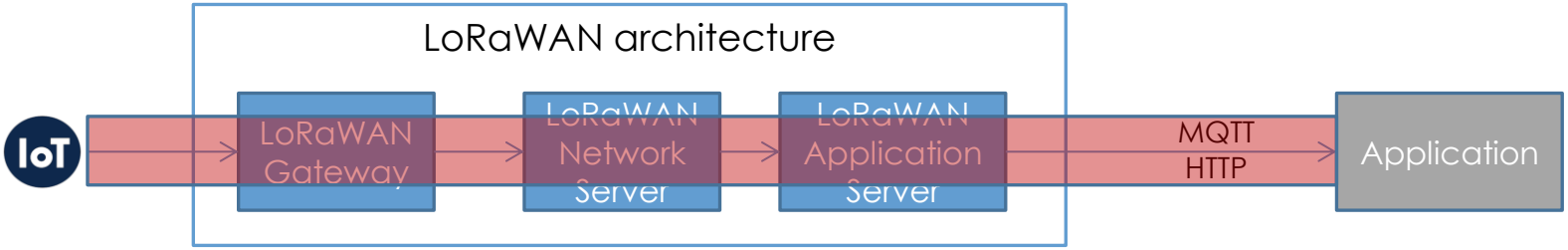
- Exemple de cas d'usage : détection de cyberattaques sur des réseaux IoT

Solutions PACLIDO
4- Couche de sécurité pour BLE

- Couche de sécurité logicielle permettant de sécuriser une liaison BLE intégrant :
  - Chiffrement et authentification (basés sur Lilliput-AE) par l'entité cliente
  - Déchiffrement par l'élément qui va recevoir la donnée
- Exemple de cas d'usage : sécuriser la couche applicative d'une liaison de type BLE

Solutions PACLIDO
5- Surcouche de sécurité de bout en bout

- Intégration de Lilliput-AE dans la solution CymID IoT d'Airbus CyberSecurity
- Composant logiciel permettant de sécuriser de bout en bout une communication entre un capteur et une application finale au travers de différents réseaux (différentes ruptures protocolaires)



- Exemple de cas d'usage : s'assurer de la sécurité d'une donnée envoyée par un objet connecté au travers de différents réseaux, le tout sur des infrastructures IoT compatibles avec les standards existants du marché.

Solutions PACLIDO

- Solution liée à la Détection :
  - **Détection d'anomalies** sur des réseaux IoT basée sur des **mécanismes d'IA**
- Solutions liées à la Protection :
  - Secure Element : pour l'intégration **matérielle** de Lilliput-AE
  - Gateway LoRaWAN intégrée : pour la mise en œuvre rapide de réseaux LoRaWAN **standalone optimisés**
  - Couche de sécurité BLE : pour protéger les liaisons de type **BLE**
  - Surcouche de sécurité de bout en bout : pour protéger les **systèmes IoT existants** avec peu d'effort d'intégration

Cas d'usage PACLIDO

3 cas d'usage pour démontrer la valeur ajoutée des solutions PACLIDO

	1- LoRaWAN Gateway	2- Secure Element	3- AI Based detection	4- Security over BLE	5- End-to-end security
Domotique		✓		✓	
Eclairage public	✓	✓	✓		
Industrie 4.0					✓

Merci de votre attention !

Nicolas Darnet
Project manager
AIRBUS CyberSecurity
nicolas.darnet@airbus.com

Paul-Emmanuel Brun
IoT system security expert
AIRBUS CyberSecurity
paul-emmanuel.brun@airbus.com