Partenaires

Pôles de compétitivité

Soutiens

PACLIDO

Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets

Démonstrateur Domotique

Sécurisation des données applicatives d'une communication Bluetooth Low Energy : cas d'une clé dynamométrique connectée

PACLIDO - Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets

Objectifs et critères de validation

Le but de la démonstration et de mettre en avant la valeur ajoutée de l'algorithme de chiffrement **LILLIPUT-AE** dans le cas d'une **attaque Man-in-the-Middle** sur la clé dynamométrique.

Critères de validation :

- Sécurité et robustesse
- Taille RAM/ROM.
- Latence et absence d'impact sur l'expérience utilisateur

Bluetooth Low Energy

Un des protocole de communication sans-fil courte portée le plus utilisé dans l'IoT
La norme propose un chiffrement AES-128 et plusieurs méthodes d'appairage (mais pas toujours mis en œuvre par les fabricants)

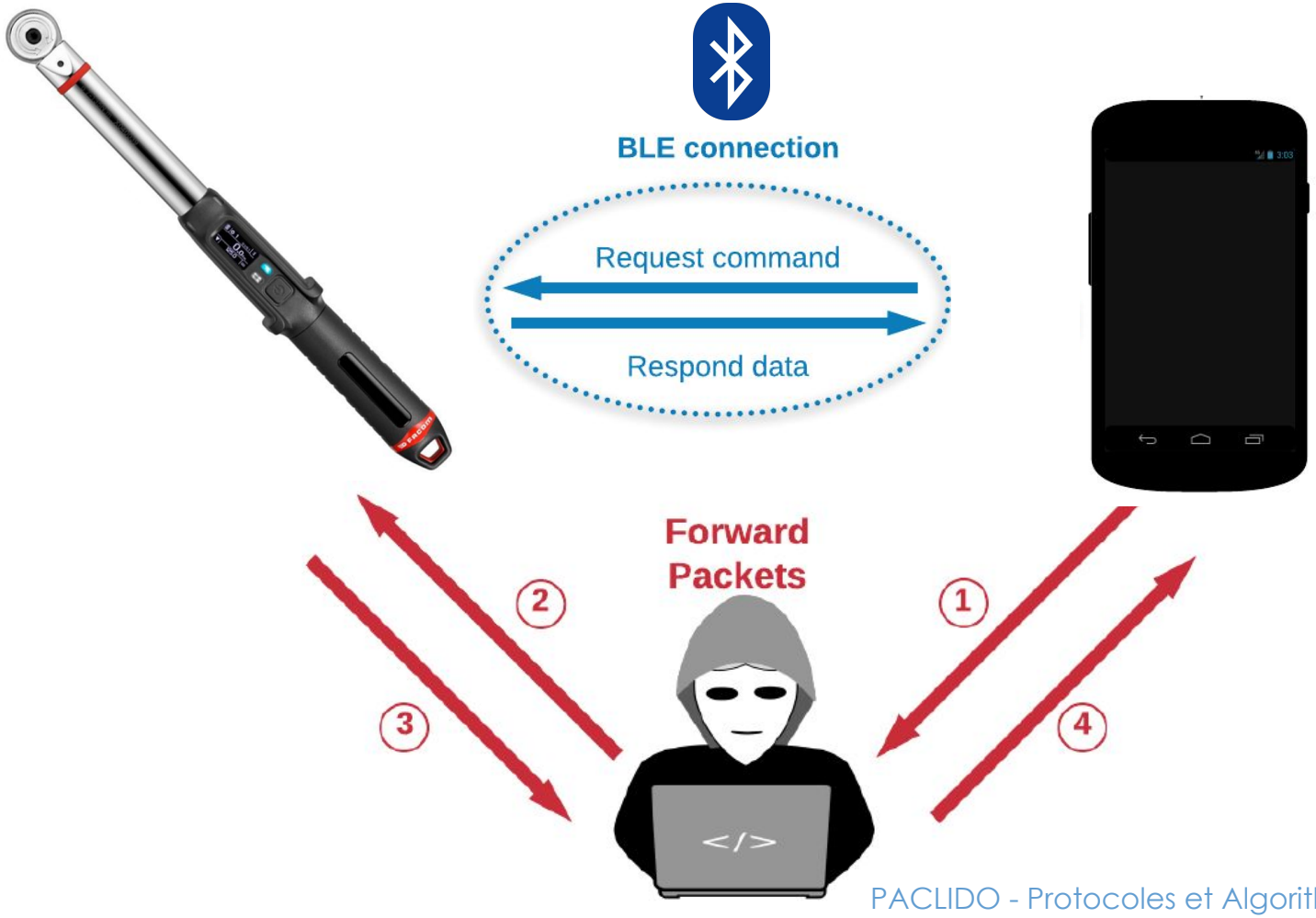
Des vulnérabilité du protocoles sont trouvées régulièrement

- 2013 : BLE encryption cracker
- 2018 : BlueBorn
- 2020 : BLESA (Bluetooth Low Energy Spoofing Attack)
- 2020 : BIAS (Bluetooth Impersonation Attacks)
- 2020 : BLURTooth
- …


BLE connection
Request command
Respond data

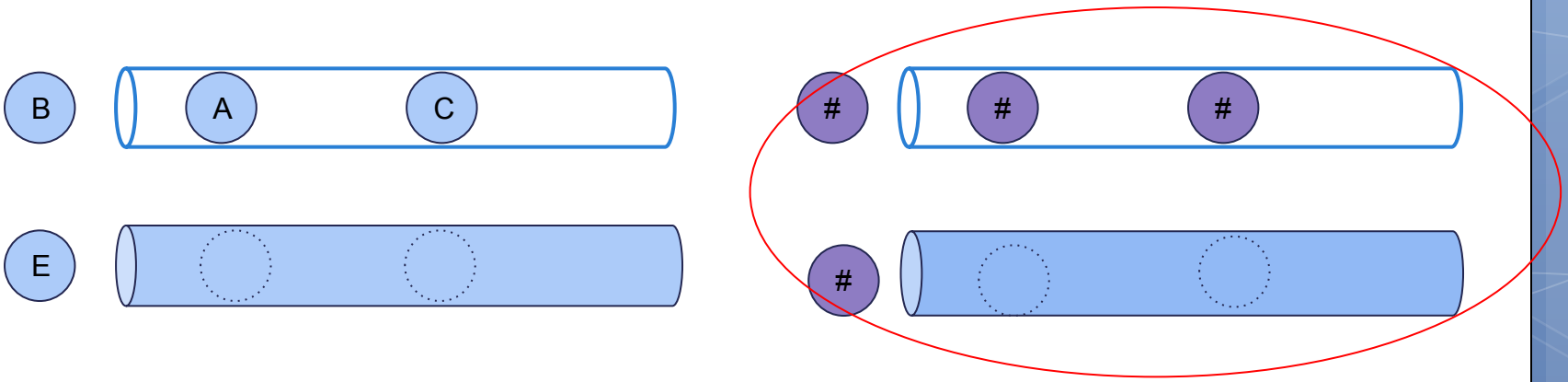
Scénario d'attaque

1. l'attaquant "**clone**" le profile BLE de la clé dynamométrique et se connecte à la vraie clé
2. l'**application mobile se connecte à la clé virtuelle de l'attaquant**
3. toutes les valeurs entrées et envoyées par l'application mobile sont **interceptées et altérées** par l'attaquant, puis **relayées** à la vraie clé.
4. la valeur du couple de serrage envoyée n'est donc pas la même valeur affichée sur l'écran de la clé dynamométrique.


BLE connection
Request command
Respond data
Forward
Packets
1
2
3
4
</>

Bluetooth LE + LILLIPUT-AE

- L'algorithme LILLIPUT-AE est utilisé pour chiffrer les **données applicatives** échangés.
- Indépendamment du chiffrement du protocole Bluetooth LE



Résultat et Performances

- L'attaque MiTM est bloquée : l'attaque ne peut pas lire et altérer les données
- Même si le chiffrement du protocole est absent ou cassé
- Le fonctionnement de la clé dynamométrique n'est pas altéré par l'ajout de LILLIPUT-AE
- Aucun impact sur l'expérience utilisateur
- Latence introduite de quelques dizaines de millisecondes

Merci de votre attention.

QUESTIONS ?