MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Analyse des propriétés de sécurité dans les implémentations du Bluetooth Low Energy

Nicolas Docq
Tristan Claverie
José Lopes-Esteves

02 juin 2021

Plan

Le fonctionnement et la sécurité du BLE
La problématique de cette étude
La propagation des propriétés de sécurité selon la norme
L'étude de l'implémentation de la norme par Linux et Android
Conclusion

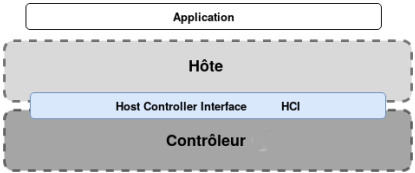
Le fonctionnement et la sécurité du BLE

Le fonctionnement du BLE

Généralités

- Bande de fréquence ISM 2,4 GHz
- Norme commune Bluetooth Classique / BLE
- Non compatible Bluetooth Classique

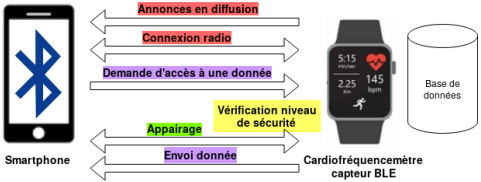
Une pile protocolaire avec 2 sous-ensembles



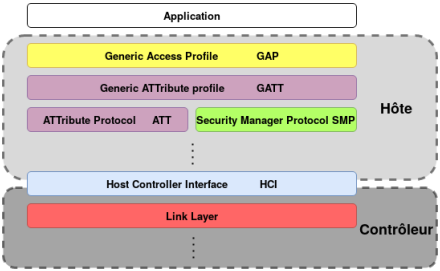
Le fonctionnement du BLE

Généralités

- Bande de fréquence ISM 2,4 GHz
- Norme commune Bluetooth Classique / BLE
- Non compatible Bluetooth Classique



Une pile protocolaire avec 2 sous-ensembles



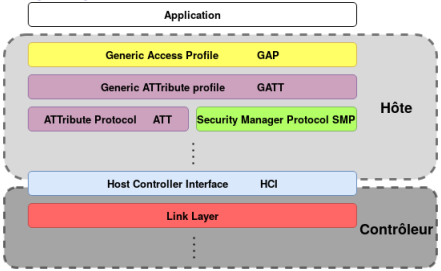
- Imbrication des couches et appellations changeantes

Les couches liées à la sécurité

Couche **Link layer**

- Gestion des rôles maître / esclave
- Chiffrement des données

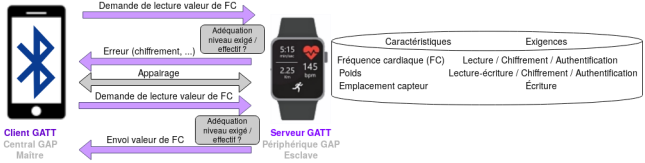
La pile protocolaire du BLE



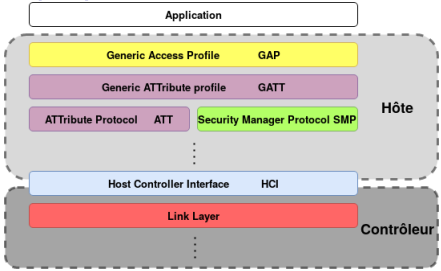
Les couches liées à la sécurité

Couches ATT et GATT

- Gestion des rôles de serveur et client GATT
- Couche ATT : définition du modèle client / serveur, stockage de caractéristiques et des propriétés d'accès
- Couche GATT : ordonnancement des données ATT en une base de données standardisée



La pile protocolaire du BLE

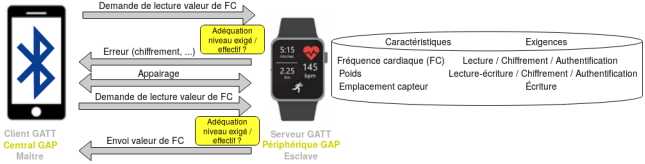


Les couches liées à la sécurité

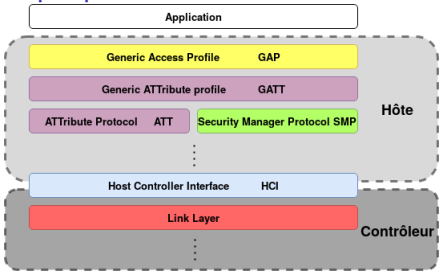
Couche GAP

- Gestion des rôles de *central* et *périphérique*
- Choix d'un mode et niveau de sécurité pour masquer la complexité

Mode	Niveau	Connexion
1 - chiffrement	1	Pas de sécurité
	2	Chiffrée, non authentifiée
	3	Chiffrée, authentifiée
	4	Chiffrée, authentifiée, Secure Connections et clés de 128 bits



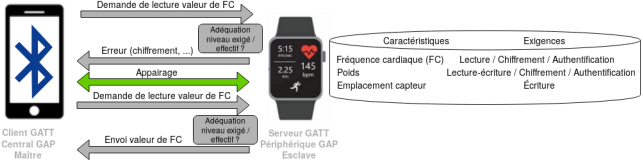
La pile protocolaire du BLE



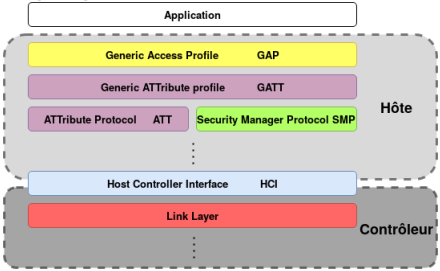
Les couches liées à la sécurité

Couche SMP

- Permet l'appairage :
  - Échange des fonctionnalités lors de l'appairage
  - Création et échange des clés de chiffrement
- Deux possibilités d'appairage :
  - Appairage *Legacy* : 3 méthodes
  - Appairage *Secure Connections* : 4 méthodes
- Association éventuelle

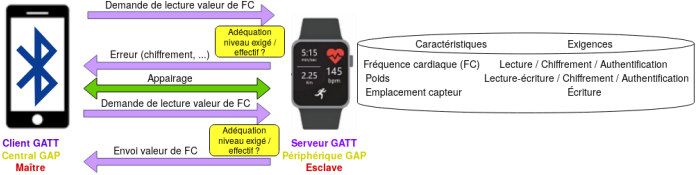


La pile protocolaire du BLE

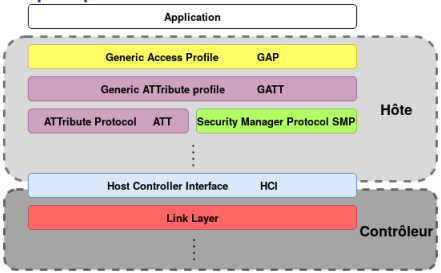


Les couches liées à la sécurité

L'imbrication des couches



La pile protocolaire du BLE



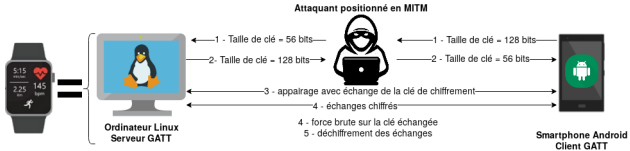
La problématique de cette étude

La problématique de l'étude par l'exemple

Norme Bluetooth :

- Version $\geq$ 4.0 (2010) : négociation de taille de clé [56 - 128] bits
- Version 4.2 (2014) introduit couche GAP mode 1 niveau 4 :
  - Appairage *Secure Connections*
  - Chiffrement et Authentification
- Version 5.0 (2016) ajoute au mode 1 niveau 4 l'exigence du chiffrement avec une clé de 128 bits

Attaque *Key Negotiation Of Bluetooth* (KNOB) (2019) :



Référence : Daniele Antonioli, Nils Ole Tippenhauer and Kasper Rasmussen. Low Entropy Key Negotiation Attacks on Bluetooth and Bluetooth Low Energy

Propagation par Linux entre couches BLE d'informations erronées

L'objet de la recherche

Objectifs :

- Analyser la propagation de la sécurité prévue par la norme
- Analyser si les implémentations :
  - Respectent la norme
  - N'ont pas de problème de sécurité
- Qualifier le niveau de sécurité d'une connexion BLE

Implémentations cibles :

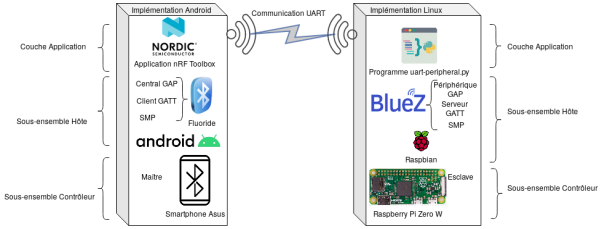
- Linux : pile BlueZ
- Android : pile Fluoride

Stratégie

Les moyens d'étude

- Analyse de la norme BLE version 5.2
- Analyse statique du code source BlueZ
- Analyse dynamique de la pile BlueZ
- Plateforme comportementale
  - Linux :
    - Changement des capacités annoncées
    - Choix de méthodes d'appairage *Legacy* ou *Secure Connections*
    - Changer exigence de sécurité en lecture/écriture d'une caractéristique d'un serveur GATT
  - Android : application client GATT

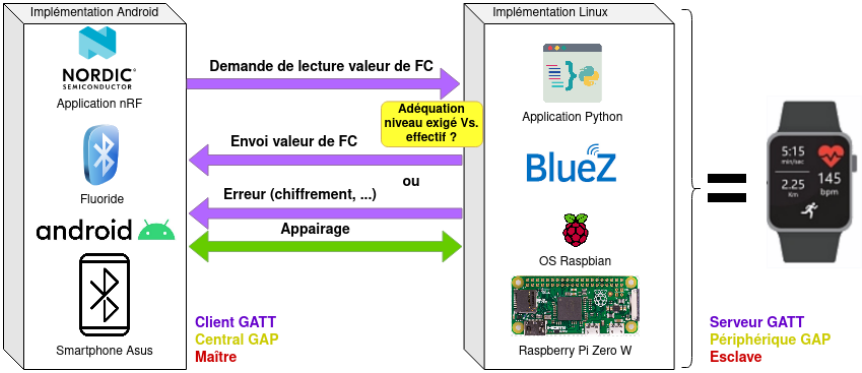
La plateforme comportementale



La propagation des propriétés de sécurité selon la norme

La propagation des propriétés de sécurité selon la norme

Lien entre couche GAP et ATT/GATT

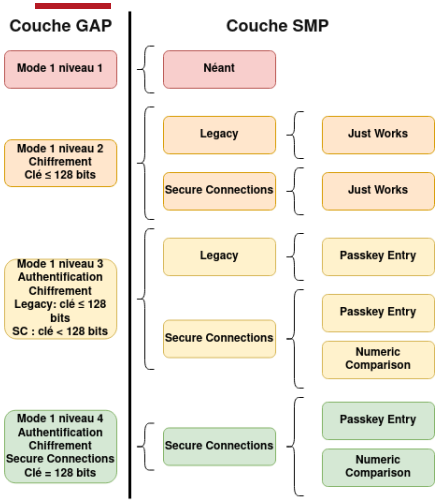


- Introduction d'exigences GAP qui n'ont pas d'équivalent au niveau ATT

La propagation des propriétés de sécurité selon la norme

Lien entre couches GAP et SMP

- *Passkey Entry* : quelle méthode d'appairage, quelle sécurité ?



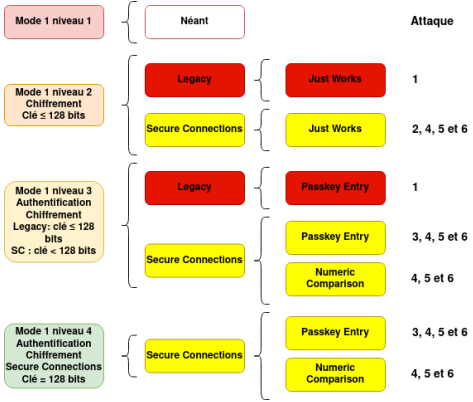
La sécurité des méthodes d'appairage après l'état de l'art

Impact des attaques

	Réf.	Impact	Attaquant
▶	1	Confidentialité et intégrité	Passif
▶	2	Confidentialité et intégrité	Actif
▶	3	Confidentialité, intégrité et authenticité	Actif
▶	4	Confidentialité et intégrité	Actif
▶	5	Confidentialité et intégrité	Actif
▶	6	Confidentialité et intégrité	Actif

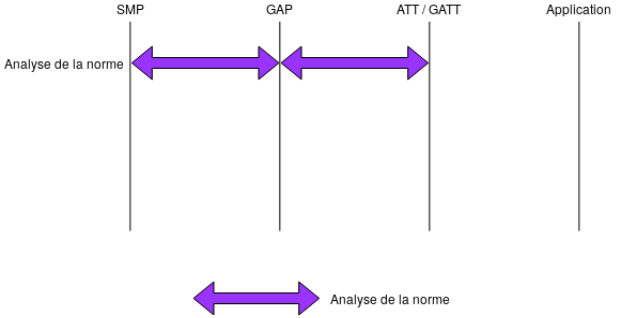
Les attaques référencées se trouvent en bibliographie en dernière diapositive.

Attaques sur les méthodes d'appairage



L’étude de l’implémentation de la norme par Linux et Android

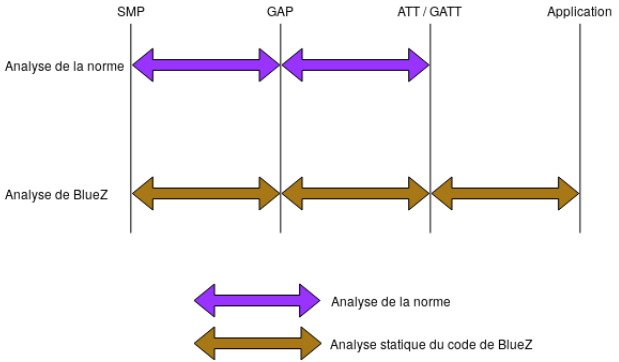
Processus d'analyse



Constats

- Couches de sécurité clairement décrites
- Pas de description du dialogue inter-couches
- Exigences GAP sans déclinaison au niveau ATT
- Morcellement dans toutes les couches des responsabilités de sécurité

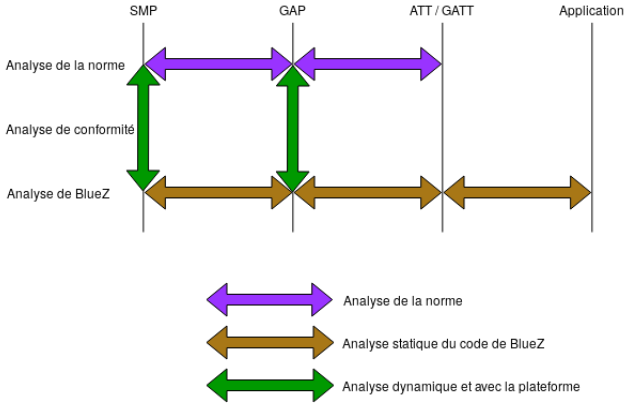
Processus d'analyse



Constats

- Pas de documentation / peu de commentaires dans le code
- Des fonctions liés à la sécurité pas forcément cohérente avec la norme
- L'ajout de permissions au niveau ATT pour répondre au manque de la norme
- La *KNOB attack* toujours non corrigée

Processus d'analyse

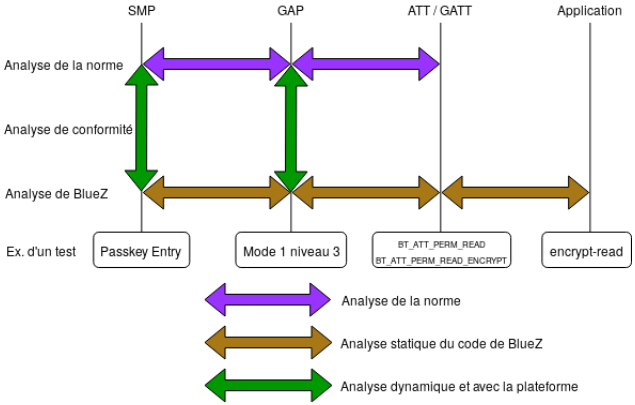


Corrélation norme / implémentation

Pour cela, utilisation de :

- l'analyse dynamique
- la plateforme comportementale

Méthodologie de test



Réalisation des tests

- Faire varier côté Linux :
  - les capacités annoncées
  - le choix de la méthode d'appairage : *Legacy* ou *Secure Connections*
  - le descripteur de sécurité de la couche Application BlueZ pour avoir un effet au niveau ATT et GAP
- Accéder depuis Android aux caractéristiques protégées

$\Rightarrow$ Matrice complète de tests

Les résultats obtenus

Des découvertes surprenantes, bien que la plupart des tests soient conformes aux attendus

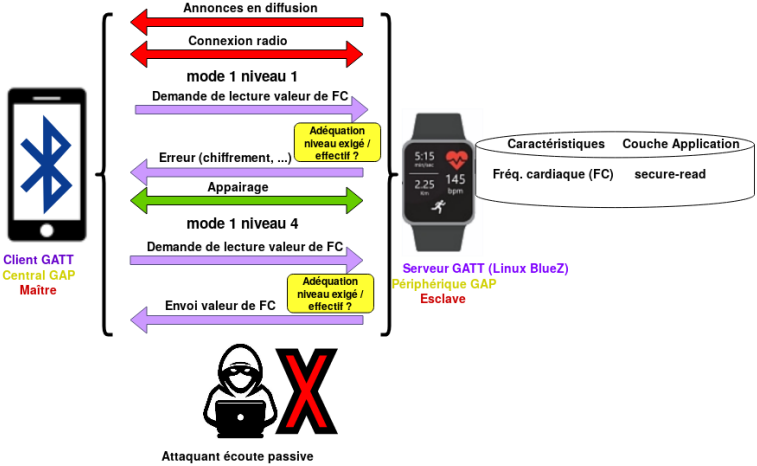
Sur Android

- Association silencieuse : découverte faite indépendamment par une autre équipe de chercheurs (CVE-2020-12856)

Sur Linux

- *Secure Connections only mode* non fonctionnel
- Toujours la possibilité de diminuer taille de clé alors que mode 1 niveau 4 GAP annoncé (*KNOB Attack*)
- Découverte de mauvaise vérification entre niveau de sécurité exigé et effectif du mode 1 niveau 4 GAP $\Rightarrow$ Proposition de correction $\Rightarrow$ commit de BlueZ par les développeurs $\Rightarrow$ CVE-2021-0129

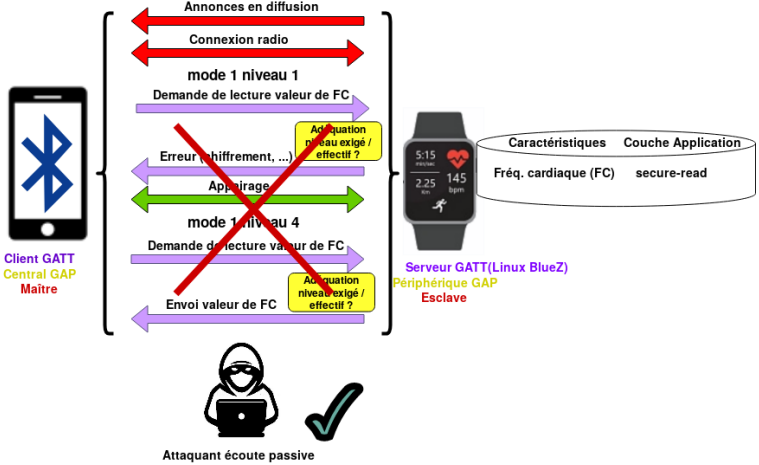
La CVE-2021-0129



Volonté du développeur

- Plus haut niveau de sécurité exigé :
  - authentification
  - confidentialité
  - appairage SC
  - clé de 128 bits
- Application : secure-read
  - GAP = mode 1 niveau 4
  - SMP = appairage obligatoire

La CVE-2021-0129



Volonté du développeur

- Application : secure-read
  - GAP = mode 1 niveau 4
  - SMP = appairage obligatoire
- Plus haut niveau de sécurité exigé

La réalité

- Mode 1 niveau 1 conservé
- Aucune sécurité!!

Conclusion

Conclusion

- La norme : analyse de la propagation de la sécurité ⇒ mise en relation norme / état de l'art
- Linux : la propagation des propriétés de sécurité ⇒ protocole de tests avec plateforme comportementale et analyse dynamique
- Qualification de la sécurité d'une liaison via l'analyse dynamique sous Linux
- Découverte de non conformité ⇒ Proposition de correctifs ⇒ Tests de conformité des correctifs
- Une implémentation défaillante par BlueZ du mode 1 niveau 4 GAP

Conclusion

- Une plateforme qui peut être améliorée
  - Rôles client / serveur GATT non interchangeables
  - Impossibilité de faire varier ce qui est annoncé par Android lors de l'appairage
  - Plus d'automatisation
- État des implémentations
  - BlueZ : respect insatisfaisant de la norme
  - Fluoride : étude à poursuivre
  - BlueZ et Fluoride : aucune information de sécurité accessible à l'utilisateur final

Questions

Bibliographie

Cette bibliographie concerne les six attaques décrites en diapositive 16.

1. Mike Ryan. Bluetooth : With low energy comes low security. 2013.
2. Keijo Haataja : "Practical man-in-the-middle attack against bluetooth secure simple pairing. 2008.
3. Andrew Y. Lindell : Attacks on the pairing protocol of bluetooth v2.1. 2008.
4. Eli Biham and Lior Neumann : Breaking the bluetooth pairing - fixed coordinate invalid curve attack. 2018.
5. Yue Zhang, Jian Weng, Rajib Dey, Yier Jin, Zhiqiang Lin, and Xinwen Fu. Breaking secure pairing of bluetooth low energy using downgrade attacks. 2020.
6. Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Key negotiation downgrade attacks on bluetooth and bluetooth low energy. 2020.