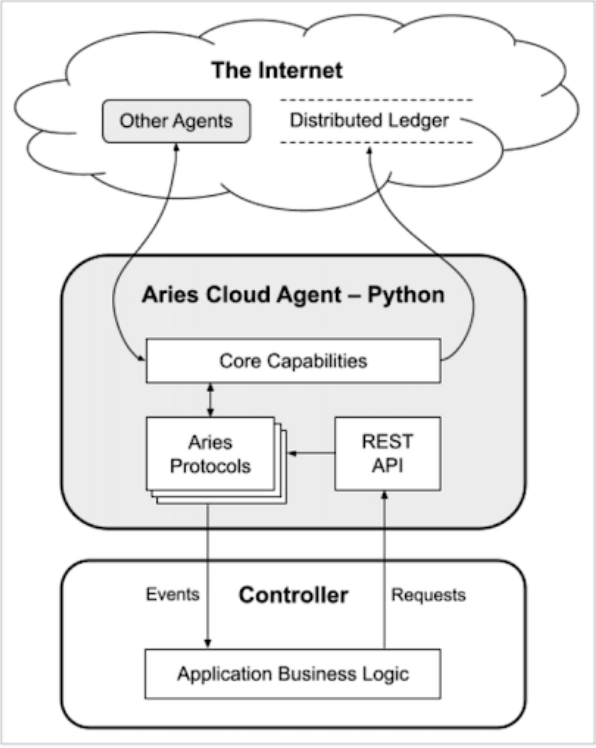
université de BORDEAUX

MASTER 2 INFORMATIQUE RCI

2021-2022

Rapport de PFE : Déploiement d'un VPN sur des équipements mobiles ou IoT



Alexis Henquinet Mohamed Diallo Sara Real Santos

Sommaire

1 Introduction

L'apparition de l'Internet of Things permet de rendre nos vies quotidiennes plus accessibles. La quantité d'objets IoT augmente et continuera à le faire, avec des prédictions quantifiant le nombre de dispositifs IoT en 2025 à 25 millions, face à 4900 en 2015. Cependant, l'augmentation de l'utilisation d'objets IoT pose aussi des problèmes concernant la sécurité de ces dispositifs. En effet, beaucoup d'objets IoT sont vulnérables à des attaques, et de plus en plus, il y a des attaques visant spécialement les dispositifs IoT.

La plupart des dispositifs IoT ne sont pas protégés par manque d'espace dans la mémoire, ou alors nécessitent des mises à jour régulières pour pouvoir être protégés. Une façon de pouvoir sécuriser les échanges entre les composants d'un réseau IoT est d'utiliser un VPN afin d'encrypter les différents messages. Une autre mesure complémentaire concernant la sécurité des connexions est l'utilisation de certificats. Les certificats sont utilisés pour s'authentifier auprès de différentes entités. Les certificats permettent de sécuriser les connexions en vérifiant que le certificat soit signé par une autorité qui 'a notre confiance', et donc qui permet de démontrer que l'agent avec lequel nous communiquons est de 'confiance' et vice-versa. Cependant, ce système dépend des autorités de certification et peut présenter différents problèmes. D'une part la possible censure ou contrôle de la part de cette autorité, mais aussi le fait que si jamais cette autorité est attaquée, alors tout les certificats délivrés par celle-ci sont compromis. Pour pouvoir contrer ces difficultés, nous pouvons utiliser des systèmes décentralisés qui remplacent l'autorité de certification

Dans ce projet nous avons utilisé ces deux méthodes pour sécuriser les échanges IoT. Notre réseau IoT est composé d'une machine Android et une machine Debian. Nous avons aussi un serveur qui communique avec la Blockchain Indy qui authentifie les différentes parties, client et serveur. Dans les deux machines nous avons installé et configuré un VPN avec le software Wireguard. L'utilisation de certificats a été remplacée par l'utilisation de Verified Credentials et l'authentification auprès de noeuds Blockchain.

2 Étude de l'existant

2.1 Wireguard

Wireguard est un VPN qui a été initialement déployé pour les systèmes Linux, mais qui maintenant peut être utilisé par des dispositifs Android, Windows, macOS et autres. Du côté utilisateur, Wireguard est simple à configurer. Il suffit juste d'échanger des clés publiques et Wireguard configure le VPN. La clé publique est une clé de 32 bytes construite avec Curve25519. Wireguard utilise cette clé pour créer une interface réseau associé à la clé publique. Ces interfaces font partie de la 'cryptokey routing table', qui peut être configuré et à laquelle on peut ajouter des règles de routage supplémentaires. Quand des paquets sont envoyés vers une machine par un tunnel Wireguard (donc, par l'interface dans la cryptokey routing table), ils sont encryptés avec la clé publique de la machine qui reçoit le paquet. Quand un

2.2 Verified Credentials

2.3 Aries

3 Besoins

TODO

3.1 Besoins fonctionnels

TODO

3.2 Besoins utilisateurs non fonctionnels

TODO

4 Scénarios fonctionnels

TODO

5 Architecture et implémentation

TODO

6 Analyse du fonctionnement & Tests

TODO

7 Conclusion

TODO

7.1 Limitations

TODO

7.2 Extensions

TODO

8 Bibliographie

TODO

9 Annexe

TODO