Travail de Bachelor 2024

Externalisation des clefs privées WireGuard sur des périphériques sécurisés

Contexte

Actuellement, les VPNs sont largement utilisés pour protéger les communications sensibles contre des menaces telles que l'interception de données et les attaques de type man-in-the-middle. Parmi les nombreuses solutions VPN, WireGuard se distingue par sa modernité, sa performance, sa sécurité robuste, sa rapidité et sa simplicité d'utilisation.

Problématique

Le problème principal de ce travail réside dans la gestion de la clé privée de WireGuard, actuellement stockée sur le système de l'utilisateur au niveau de la mémoire, la rendant vulnérable en cas de compromission de la machine. Un attaquant pouvant extraire cette clé pourrait écouter les communications actuelles et usurper l'identité de l'utilisateur dans les sessions futures. Ce risque est un obstacle majeur à l'adoption de WireGuard dans des environnements hautement sécurisés.

Objectif

Pour répondre à cette problématique, l'objectif de ce travail de Bachelor a été d'intégrer WireGuard avec des périphériques externes sécurisés tels que des YubiKey ou NitroKey afin d'externaliser la clé privée du VPN.

En déplaçant cette clé à l'extérieur de la machine de l'utilisateur cela réduit la surface d'attaque à la session VPN courante. Celui-ci peut toujours récupérer la clé qui a été dérivée pour la session, mais pas la clé privée longue durée.

Méthodologie

Le projet a d'abord exploré différentes implémentations et périphériques, optant finalement pour BoringTun (implémentation WireGuard en Rust) ainsi qu'une NitroKey en utilisant le protocole OpenPGP pour sa compatibilité et sa simplicité d'intégration.

Dans un second temps, un programme de test a démontré que l'utilisation d'une smartcard pour les opérations cryptographiques est interchangeable avec l'utilisation de la librairie cryptographique de BoringTun, validant ainsi la faisabilité de l'externalisation de la clé privée.

Les résultats de ces tests ont ensuite été transférés directement sur l'implémentation de BoringTun afin d'avoir un VPN totalement fonctionnel avec une smartcard.

Conclusion

Les recherches, ainsi que les modifications apportées à BoringTun, ont permis d'améliorer significativement la sécurité de ce VPN en le rendant plus adapté aux environnements hautement sécurisés où la compromission de la clé privée serait une faute grave.

Auteur: **Alexis Martins Lemos Pinto**
Répondant externe: **Michael Da Silva**
Prof. responsable: **Maxime Augier**
Sujet proposé par: **Maxime Augier**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale