Université Bretagne Sud

Master 1 Ingénierie de Systèmes Complexes

Spécialité Cybersécurité des Systèmes Embarqués

PoC déverrouillage de serrure connectée via HackRF

Stage Master 1

Gidon Rémi

Promotion 2019-2020

Contents

List of Tables

List of Figures

Introduction

Definition serrure connectee

Mecanisme ouverture/fermeture electronique embarquant un ordinateur permettant de le controler a distance. La plupart de ces mecanismes sont adaptables sur des serrures dites normales, prenant le controle du verrou.

Une serrure est dites connectee lorsqu'elle communique avec un autre systeme informatique. Via le smartphone d'un utilisateur pour echanger des ordres mais aussi avec un serveur du constructeur.

Il existe differente architecture utilisant des topologies reseau distinctes. La plus simple et courante est une architecture dite TODO: la serrure ne communique qu'avec le smartphone en BLE via une app. Cette meme app permet a la serrure de comm avec le serveur par l'intermediaire du smartphone (BLE -> app -> wifi -> server). Une autre approche est d'integrer les capacites wifi a la serrure, qui sera autonome et directement connectee au serveur ainsi qu'a l'utilisateur via BLE. Ainsi la serrure transmet et recois ces ordres de facon autonome. Avec une politique de regles sur les actions pouvant etres effectuees localement, une indisponibilite du serveur ne bloquerait pas totalement l'utilisation de la serrure car pouvant communiquer directement avec le smartphone en BLE sans le serveur.

Meme si d'autres protocoles peuvent etres utilises, toutes les serrures connectees du marche utilisent ajd le BLE car compatible avec tout les smartphones. Le NFC est envisageable (notamment comme canal pour la mise en place du BLE) mais son champ d'application est trop reduit avec ces 10cm. Le BLE emet jusqu'a 10m, permettant de faciliter l'ouverture/fermeture de la porte sans action utilisateur.

Fonctionnement, unlock automatique lorsque dans le range via BLE, unlock distance via WiFi.

Si le service ne fonctionne plus, le smartphone decharge ou indisponible ou tout autre disfonctionnement ,toutes les serrures embarques un ou plusieurs mecanismes tierces pour ouvrir. On peut citer la clef traditionnelle qui peut continuer d'etre utilisee, mais aussi un pad avec pin 6 chiffres, une telecommande comme pour les voitures. Aucune serrure connectee ne propose de moyen biometriques ou badge RFID car ceux-ci font partis d'une autre gamme s'addressant plutot au domaine professionnel pour securiser des entrees ou entrepots.

Architecture

diff buts ?

les diff technologies utilisees comme clef

technologies recover

Protocoles

BLE / NFC / WiFi

Topologie

topologies et implications

Attaques

Replay

HackRF

Poc