Université Bretagne Sud

Master 1 Ingénierie de Systèmes Complexes

Spécialité Cybersécurité des Systèmes Embarqués

Promotion 2019-2020

Étude de système domotique: serrure connectée

Stage Master 1

Gidon Rémi

Avril/Juin 2020

Contents

List of Tables

List of Figures

Le but est d'étudier l'architecture des systèmes domotiques sous l'angle de la sécurité pour chercher des possibles fuites d'informations ou compromossions possible.
L'état de l'art révèle différentes architecture suivant le besoin et l'intégration voulue ainsi qu'une variété de canaux de communications plus ou moins adaptés.
Je me focaliserait sur les architecture contenant un *hub* domotique reliant tout les appareils ainsi que le protocole de communication `Bluetooth` en mode `Low Energy` (`BLE`).
Après étude de l'historique des attaques perpétuées sur le `BLE` et les objets domotique (connectés), je me consacrerait à la réalisation d'une preuve de concept sur des appareils `BLE`.

Domotique

Avec l'explosion de l'internet de objets (TODO chiffres) la domotique est devenue accessible et s'est popularisée à travers les objets connectés. Ceux-ci étendent leur équivalent mecanique en integrant des composants electroniques, permettant le controle a distance par exemple.
Ces ameliorations engendrent une augmentation de la surface d'attaque car leur modèle de menace doit intégrer non seulement leur fontion primaire (serrure, lampe, ...) mais également les systèmes informatiques utilisé.

Comme dans beaucoup de secteurs industriels, la sécurité n'est pas la priorité des fabriquants d'objets connectés. Ces appareils gerent des donnees utilisateur (personnelles) et leur utilisation pe critique (serrure, voiture). Devices peu cher generalement, bcp market/hype (voir ces), securite sous cote (mm si mtn c gage qualite) car fct avant tout.

Les

Ces ameliorations engendrent une augmentation de la surface d'attaque car ces *objets intelligents* (ou connectés) doivent résoudre les mêmes challenge que ceux des systèmes informatiques traditionnels en plus de leur fonction primaire.
Ces ameliorations engendrent une augmentation de la surface d'attaque de par l'integration et la communication entre systemes informatiques. explosion IoT, democratisation domotique, connexion de differents appareils (alexa, smartphone ,sensor, smart things). Securite souvent sous estimee, protocoles non adaptes et solution mal implementee / configuree

Architecture

Qu'est ce qu'un objet connecte en domotique ? Sensor (termometre)

Architecture reseau domotique

- simple: appareil non relie au reseau, dependant gateway utilisateur, remplissant une fonction d'augmentation seul (smart lock)
- avancee: appareil s'appuyant sur un reseau domotique pour realiser ses fonctions, relie a une gateway "sure" hub

Protocoles

Protocoles generaux supportes par tout appareil (smartphone notamment) et peu cher WiFi BLE NFC

Protocoles specifiques concus pour ces reseaux Zigbee Zwave

BLE

Attaques

Types d'attaques et appareils concernes (voir sources) Evolution du BLE (appairages) et attaques (replay, eavesdropping, mitm)

Types

- Eavesdropping
- MITM

Ressources

Materiel

Logiciels

Poc

ecoute passive

Identification

Localisation

Obtention secrets

Attaque matos

Logiciels

Etude des communications bluetooth: Wireshark Scappy etc Possible avec n'importe quel chip Bt deja sur la machine ou dongle USB pour une etude du traffic interne et des appareils emettants des adv.

Interceptions des communications

- BTLE (C)
- BTLEJack (lib python + firmware C)
- Mirage (framework python)

Proprietaires:

- nRF sniffer
- nRF Connect
- smartRF (TI)

Attaques

- GATTacker (NodeJS) MiTM
- BTLEJuice (NodeJS) MiTM
- BTLEJack (Jamming/ Hijacking)
- Mirage (MiTM / jam / hijack / crack)

Materiels

We can BLE dedicated devices to sniff or modify it. Internal Bt chips can only adv or connect to peripherals but never scan or modify it. They only see internal traffic (locked firmware).

Full featured HackRF PandwaRF Ubertooth

BLE HCI Dongle nRF52840 (https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52840)

- https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF52840-Dongle Some using CSR8510 (https://www.qualcomm.com/products/csr8510)
- Adafruit Bluetooth 4.0 USB Module (https://www.adafruit.com/product/1327)
- https://www.amazon.co.uk/CSR8510-Bluetooth-Adapter-Classic-Headset/dp/B01G92CNY8

Qualcomm, Broadcom, Realtek, NordicSemiconductor ... Featured in documentation is Qualcomm one

Sniffer

- Ubertooth One ($$)
- BTLEJack BBC Micro:Bit, Bluefruit, Waveshare BLE400, nRF51822 Eval kit (tweak) (https://github.com/virtualabs/btlejack)
- Bluefruit https://www.adafruit.com/product/2269 (limited)
- nRF51 https://www.nordicsemi.com/Software-and-tools/Development-Kits/nRF51-Dongle (close)
- TI CC2540 USB Dongle BLE sniffer (http://www.ti.com/tool/CC2540EMK-USB)
- Crazy Radio PA 2.4GHz (https://store.bitcraze.io/collections/kits/products/crazyradio-pa)

Board

- HackRF
- PandwaRF

Integration avec Mirage

Si je me concentre sur Mirage, cela restreint pas mal les outils possible:

- dongle BLE HCI standard
- sniffer BLE adaptable avec BTLEJack (micro:bit, bluefruit, ble400, nRF51) Les appareils dépendent des besoin, dans mon cas il me faudrait:
- inventaire: Sniffer (BTLEJack)
- obtention d'informations (crack, mit): dongle HCI x2 (un slave et un master, a voir si un BTLEJack peut remplacer un HCI)

- localisation / tracking (rssi + autres méthodes): Mirage ne permet pas cela nativement mais les informations demandées doivent être récupérables dans le framework pour l'implementer manuellement (RSSI, angle antenne ?). Cela demande au minima un dongle HCI, meme si les travaux trouvés sur le sujet utilisent un sniffer Bluefruit. Dans les travaux étudiés, la localisation demande 3+ appareils BLE pour permettre la trilatération

Il me manque donc a voir si un BTLEJack peut remplacer un HCI dans l'attaque MITM, ainsi que trouver des informations pour implementer la localisation IPS avec Mirage. Mirage supporte également d'autres appareils (comme Ubertooth) mais leurs fonctionnalités ne nous sont pas nécessaires, un sniffer flashé avec BTLEJack suffit (et coute moins cher). Pour les sniffers BTLEJack eligibles:

- Bluefruit et nRF51 (~20e) demandent reprogrammation via un "external SWD" (assez cher + 100e)
- la carte BBC Micro:bit (20e, non vendue en France directement) permet une reprogrammation sans appareil supplémentaire, et semble donc la plus simple

Pour résumer:

- dongle BLE (https://www.adafruit.com/product/1327 / https://www.amazon.co.uk/CSR8510-Bluetooth-Adapter-Classic-Headset/dp/B01G92CNY8)
- carte Micro:Bit (https://microbit.org/buy/)

Utilisation Mirage

Sniffing

Localization

Fingerprinting

A partir d'une liste de beacons et leurs position, calcul la position se rapprochant le plus d'un des beacons (a partir du RSSI).

Demande de pouvoir etablir la liste des beacons et les identifies de facon sure. Si le systeme est mit en place pour cet effet on s'assurera qu'ils soient identifiables (MAC unique par exemple) mais dans notre cas de recuperation d'information, les appareils peuvent mettre en place des mesures contre le tracage comme la generation d'adresse mac aleatoire. Il est possible d'utiliser le profile GATT pour identifier un appareil, combiner avec le RSSI dans le temps et les deplacements (capteurs) on peut esperer distinguer deux profils GATT identiques.

~ beacons coverage

Le beacon le plus proche

RSSI / TOA

~ m

Trilateration determines the position of an object by understanding its distance from three known reference points. In the case of Bluetooth, locators estimate their distance to any given asset tag based on the received signal strength from the tag

AOA / AOD

~ cm

Basee sur le nouveau systeme d'angle du BLE 5.1 Demande du materiel en plus (Multiple antennes directionnelles pour former une matrice) Differentes facon de calculee (angle arrivee, angle depart ...)

https://www.bluetooth.com/blog/bluetooth-positioning-systems/ https://www.bluetooth.com/bluetooth-resources/enhancing-bluetooth-location-services-with-direction-finding/?utm_campaign=location-services&utm_source=internal&utm_medium=blog&utm_content=bluetooth-positioning-systems

Ajouter de la precision

Fusionner les resultats avec un filtre kalmann:

- dead reckoning
- trilateration / triangulation

Ou RSS (range) + AOA (direction)

RSS

1. Scan devices BTLEJack sniffer
2. find settings (rssi, txPower / measured power ...) Tx Power service 0x1804 and Tx Power Level Characteristic 0x2A07
3. calculate distance (in a circle around you) 10 ^ ((txPower – RSSI)/(10 * N)) N = loss factor (between 2 and 4), 0 for optimal conditions
4. cross multiple references to determine a position (trilateration) repeat 3 times to 3 devices get OUR position

AOA

MITM