TGbi - Enhancing Privacy – a Smart Home Use case

Date: 2021-05-01

Authors:

Name	Affiliations	Address	Phone	email
A. De la Oliva	InterDigital, UC3M	Avda. De la Universidad 30, Leganes, Madrid, Spain	+34 91 6248803	aoliva@it.uc3m.es
Joseph LEVY	InterDigital, Inc.	111 W 33rd Street New York, NY 10120	+1.631.622.139	jslevy@ieee.org
Amelia Andersdotter	Self			

Abstract

This document describes the Smart Home scenario, highlighting possible privacy risks due to the static nature of the smart home appliances and possible correlation by inspection.

Use case description

Smart homes are populated with different types of connected devices:

- **Infrastructure (control):**
  - Smart switches
  - Smart bulbs
  - HVAC controls (heating, cooling, ventilation)
- **Sensors:**
  - Presence sensors (security, house management, etc..)
  - General sensors (temperature, water, C02, fire, etc..)
- **Smart appliances (fridge, microwaves, washing machines..)**
- **Entertainment (TVs, Sound Systems, etc…)**
- **Robots (Lynx, Zenbo, Landroid, Nautilus, Roomba, etc..)**

A smart ecosystem of things is usually connected by a wireless network, these devices require varying levels of security

Characteristics of smart home devices (Infrastructure, Sensors, and Appliances)

- **Infrastructure, sensor, and appliance devices share the following characteristics**
  - Are mainly static, they are installed, they do not change their location unless they are reinstalled
  - Maintain association to a BSS for long periods of time, typically do not change BSS
  - Information exchanged can be easily recognized based on patterns
    - These patterns can be easily correlated with home occupant behavior (e.g., living rooms lights are turned off, bedroom lights turn on, bathroom light turn on and off, bedroom lights turn off – the occupant went to sleep).
    - Direct observation of this network traffic can provide the observer detailed private information on the people living in the smart home

Characteristics of smart home devices (Infrastructure, Sensors, and Appliances)

- **In addition**
  - These devices are authorized to use the network (they have associated using PSK)
  - If there is an ACL, their MAC address is there
  - These devices typically use higher layer security (Internet Application-level security)
  - These devices are not usually updated
  - Typically, device and manufacturer can be found by direct observation of MAC address

Example: Presence sensor

- **Presence sensor indicates when a person enters a room**
  - Fixed location: Correlation with physical space is possible
  - Fixed MAC Address: known manufacturer and type of sensor, i.e., presence
  - If transmission is tied to positive indication (i.e., someone is present)
    - Presence can be monitored outside the network by observation
    - If transmission is periodic, will generate unnecessary traffic, introduces latency and uses energy

Problem 1: statement

- **Current MAC Address randomization capabilities do not address the issues in this case**
  - Current MAC Address randomization only applies prior to association.
  - Typically, these devices only associate once (once per installation).
  - Some of these devices use fix MAC Address (disclosing manufacturer and model)
- **Mechanisms are needed to provide enhanced privacy.**
  - Enabling these devices to maintain network connectivity and not constantly broadcast a known MAC Address that is correlated to user information that should remain private