SmartRecon: Spy on Smart-Home Devices Hidden Behind the Hub using Encrypted Network Traffic

Karthika Subramani, Omid Setayeshfar, Xingzi Yuan, Raunak Dey, Muhammed Abuodeh

Abstract

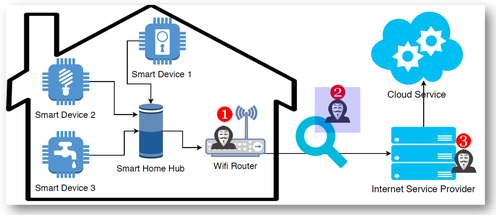
Smart-Home devices are becoming an integral part of people's lives making it more convenient for users to perform day-to-day activities. As a result, they gain knowledge of the user's personal and private information and behavior. We have developed SmartRecon, a novel approach that can accurately identify activities of smart-home devices only by monitoring encrypted traffic of the target home network.

- Our approach is minimally intrusive requiring no direct access to the hub or smart devices
- Our evaluation results show that the attacker can successfully disclose behaviors of smart-home devices with over **70% accuracy** on average
- We also demonstrate that the adversary can successfully recognize privacy-sensitive activities including open and close of a **smart door-lock**, and turn on and off of a **smart LED**

Adversary Model & Assumptions

We assume that an attacker only passively sniffs network encrypted packets.

1. First, the attacker can gain access to the traffic from a compromised router
2. Second, the attacker eavesdrops network traffic from the home router's up-link traffic .
3. Next, the attacker could gain access to the target's network traffic from the ISP



Goal of the attacker with access to the network traffic:

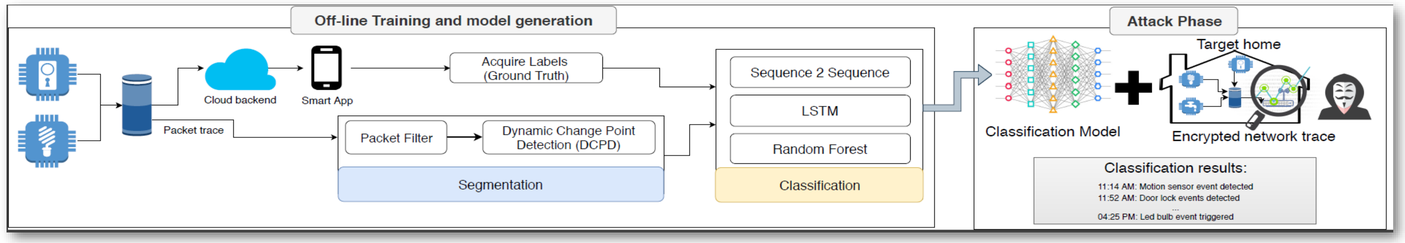
The attacker could implement an automated model that identifies patterns from the encrypted network traffic of smart home and map it to their respective devices. Using this pattern matching approach, the attacker could potentially perform following attacks

- **Large Scale Scout Attacks :** Similar to Mirai Botnet attacks
- **Targeted Scout Attack :** Recon for physical access to user's home
- **Privacy Violating Behavior Tracking :** Gain knowledge of user behavior

System Overview

Our entire approach has **2 major stages**, an Off-line training and model generation and an Attack phase. The first stage includes extensive data collection, data processing and model generation and training. At the attack phase, the trained model from first stage is used to identify smart home devices and events on the smart home devices.

- **Traffic Segmentation :** We need to further segment the captured traffic packets to determine the packets generated for a specific event. We use PELT segmentation method to dynamically segment the packets.

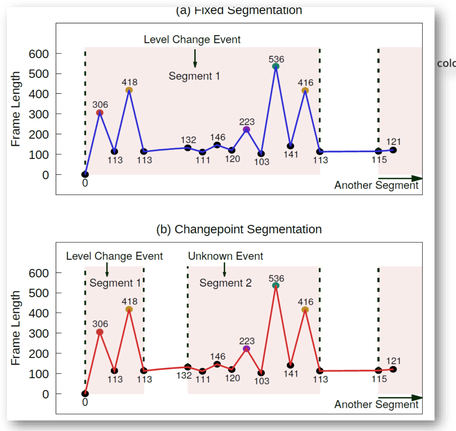


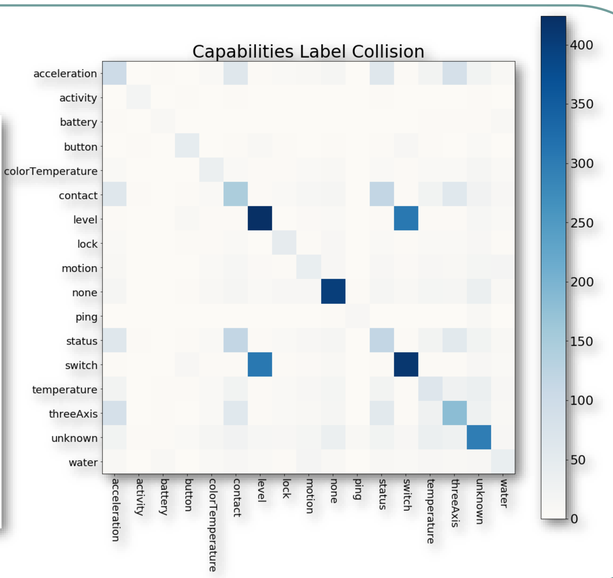
- **Data Collection :** We collect data from **Samsung Smartthings Hub and 16 smart home devices** that connect to the hub. The data is collected by monitoring the traffic to and from the router to which the hub is connected. **Ground truth** of the events from devices is obtained from the **logs** provided by **Samsung Smartthings** account
- **Model Generation:** The packets generated by the devices for a specific event were similar but followed various patterns to be detected by simple methods. Hence, we implemented three different machine learning models to classify the segmented packets into various devices and their events.

Evaluation Results

- Firstly, our results show that dynamic segmentation performs better then fixed segmentation
- Secondly, we were able to detect the capabilities of smart home devices with almost 70% accuracy
- Hence, we posit that measures need to be taken to secure smart home user's privacy

Classification Model	Average F1 Score
Random Forest	0.516
DeepTrafficNet	0.664
Seq2Seq	0.67





Detection Results

- We illustrate the extent of the new attack surface by inferring user behavior on three set-up home environments.
- We show that our model was able to detect the presence of smart lock in the user home and logged the lock activities performed by user at various point of time
- Our model was also able to identify smart switch events in the user home potentially revealing the user's presence in home.