Wireless Traffic Analysis Based Side-channel Attacks and Countermeasure in Smart Home

Yan Meng
yan_meng@sjtu.edu.cn
Shanghai Jiao Tong University
Shanghai, China

Haojin Zhu*
zhu-hj@sjtu.edu.cn
Shanghai Jiao Tong University
Shanghai, China

ABSTRACT

Smart home technology is a rapidly growing field that involves the intelligent integration of various sensors and devices to automate home functions such as appliances, lighting, heating and cooling systems, and security and safety systems. Our study centers around the issue of side-channel inference on the wireless traffic within smart home networks. We demonstrate that by exploiting side-channel information present in the wireless traffic, it is possible to deduce the device type and identify the smart apps deployed on the network using a state machine matching approach. To address this security concern, we propose a countermeasure scheme. This scheme involves injecting spoofing traffic, which effectively obfuscates the traffic patterns of smart home applications, thereby thwarting inference attacks.

KEYWORDS

Side-channel attack; Smart home; Traffic analysis; Obfuscation

ACM Reference Format:
Yan Meng and Haojin Zhu. 2023. Wireless Traffic Analysis Based Side-channel Attacks and Countermeasure in Smart Home. In *ACM Turing Award Celebration Conference 2023 (ACM TURC '23), July 28–30, 2023, Wuhan, China.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3603165.3607446

1 INTRODUCTION

Smart home, sometimes called home automation, is a concept of adopting a large variety of Internet of Things (IoT) to aid control and automation of home appliances (e.g., refrigerators, ovens, and washer/dryers), lighting, heating and cooling systems (air conditioning, heaters), and various home security (e.g., entry sensors, alarms) and safety (e.g., water, freeze, smoke detectors) systems. In recent years, the consumer market of smart homes has experienced rapid growth.

A typical example of smart home platforms is Samsung's SmartThings [2]. It enables devices (e.g., smart lights, smart switches, smart outlets) from different vendors to communicate through a local gateway (e.g., a hub or a base station) or cloud backend servers. Software applications can be developed by third-party developers to enable smart control of the devices. For example, an application (i.e., SmartApp) can monitor the status of one device (e.g., thermostats), and trigger some actions of another device (e.g., fire alarms) upon receiving certain event notifications (e.g., an extremely high the temperature detected).

Along with the popularity of SmartThings is the increasing concern about privacy breaches in smart homes. On the one hand, SmartThings is designed to facilitate peoples' control of smart devices. Thus, in many cases, the changes in smart apps' status are inherently correlated with the actions of human beings, which opens a back door for attackers to infer the actions of humans. On the other hand, human actions at home are most sensitive and thus should be kept private in any situation.

In this paper, we find that smart home platforms are particularly vulnerable to side-channel traffic analysis that to infer the encrypted content by observing the size and interval of encrypted wireless packets. The communication semantics in the smart home platforms do not carry sufficient entropy to prevent this type of analysis. To validate our findings, we developed a framework named HoMonit [3] which, by passively monitoring (*i.e.*, wireless sniffing) the size and inter-packet timing of the encrypted communication between the smart devices and the hub, in order to infer (1) the type of smart devices where the observed traffic is originated or sent, (2) the type of events triggered on/by the devices or commands sent from the SmartApp to the devices, and (3) the type of SmartApps which the smart devices communicate with.[1]

Evaluation results suggest our system (i.e., HoMonit) can effectively detect the smart devices, their associated events/commands, and also the SmartApps used by the user (if their behavior is separable). This side-channel attack allows an adversary who is able to place a sniffing device close to the home to monitor the interaction between SmartApps and the smart devices, which will lead to a severe breach of user privacy in some cases. We particularly show that (1) home occupation information (2) human activities and (3) elder care and health care information have the risk to be leaked through SmartApp inference. To resolve the dilemma, this poster proposes to thwart attacks by inserting some noisy traffic to obfuscate the communication patterns of a specific SmartApp and prevent the attacker's inference.

2 PRIVACY LEAKAGE VIA WIRELESS SIDE-CHANNEL ATTACK

In this section, we present several case studies to demonstrate that an eavesdropper is able to infer a wide range of sensitive information about the targeted residents and thus compromise the residents' privacy, including the residents' location privacy, activity privacy, age groups (e.g., elder) and health conditions, etc.

*Haojin Zhu is the corresponding author.

ACM TURC '23, July 28–30, 2023, Wuhan, China

ACM ISBN 979-8-4007-0233-4/23/07.
https://doi.org/10.1145/3603165.3607446

[1] Due to the page limit, the details of HoMonit can be found in [3].

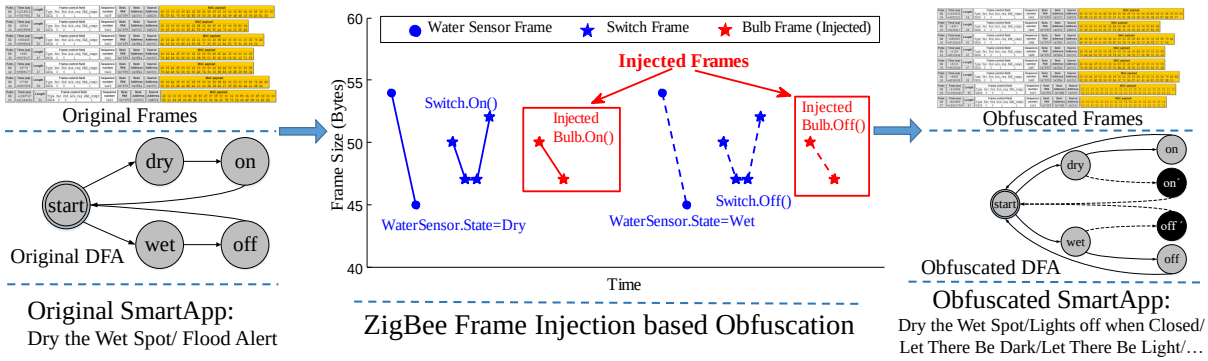

Figure 1: The Workflow of Privacy Enhancement.

Threat Model and Attacker Assumptions. An attacker is assumed to approach the proximity of the victim's home and place the Zigbee sniffer to eavesdrop on the transmitted signals emitted by the SmartThings devices. There are various ways for attackers to set up sniffer devices at the targeted locations. For example, the prevalence of consumer UAVs provides a new approach for the attacker to deliver the equipment to the spot, as pointed out by [1].

Privacy RISK I: Leaking of home occupation information. By analyzing the traffic flows between the SmartThing devices and the hub, the attacker can infer if the resident is at home or not, which poses a serious threat. For example, a burglar may use the information to choose the right time to break into the home. Next, we demonstrate how the home occupation information is leaked via wireless traffic analysis.

For instance, *Vacation Lighting Director* is a SmartApp in the *Safety & Security* category which aims to make the home seem occupied by forging light events randomly when there is no home occupation. Our research shows that, with the inference framework, this seemly "secure" SmartApp will leak out the home occupation information. To perform this experiment, we set up our test infrastructure consisting of an OSRAM Lightify LED bulb, an outlet controlling traditional bulbs, and a SmartThings hub. We set the preferences of the SmartApp in the app panel, including the specific time period, smart home away mode, the cycle of the light operation, and the number of active lights at the given time. With the collected traffic, there are two types of traffic flow vectors ($50\downarrow, 47\downarrow$) and ($50\downarrow, 47\downarrow, 47\downarrow, 52\downarrow$), which are generated by the OSRAM Lightify LED bulb and the outlet, respectively.

Privacy RISK II: Spying on human activities. We perform a proof-of-concept attack that reflects the physical world impact of our work. In the experiment, we set up a smart home with several frequently-used SmartApps, including *Brighten My Path*, which turns on lights when somebody is here, *The Gun Case Moved*, which monitors the gun case moving, *Lock It When I Leave*, which locks the door automatically when the homeowner is out of range, and *Rise and Shine*, which changes the mode when someone wakes up after a set time in the morning. After performing 2-day passive eavesdropping, 63 events are observed, and all of the SmartApps can be uniquely inferred. It demonstrates that the attacker can perform a long-term spy on the victim's daily activities and learn his living patterns, which absolutely compromises his privacy.

Privacy RISK III: Loss of elder care and health care Information. There is a set of SmartApps that are closely related to elder care or health care, which can leak highly sensitive information about the residents. We designed a smart home with two SmartApps: *Medicine Reminder*, *Elder Care: Slip & Fall*. The existence of the former SmartApp reveals that there is at least one patient in the home. The SmartApp may also reveal the residents' daily routine of taking medicines. The latter SmartApp may reveal the fact that an elder is in the bathroom.

3 PRIVACY ENHANCEMENT

In this section, we explore how to prevent privacy leakage due to inference attacks. The basic idea is to inject some bogus Zigbee packets into the traffic of the real SmartApps in order to obfuscate the attacker's traffic inference. As shown in Figure 1, effective obfuscation can be achieved if the injected traffic can spoof that of another SmartApp. Then from the attacker's perspective, it will be difficult to differentiate the spoofed SmartApp from the real SmartApp. The residents' privacy can be protected.

4 CONCLUSION & FUTURE WORK

In this poster, we propose a novel side-channel attack based on wireless traffic, which can infer the working condition of smart home platforms. Then, we describe several case studies to demonstrate that an eavesdropper is able to infer a wide range of sensitive information about the targeted residents. Finally, we propose a traffic obfuscation solution to prevent such serious attacks. We hope our poster can inspire the following works on the privacy issues in smart home networks.

ACKNOWLEDGMENTS

This study was supported by the National Natural Science Foundation of China under Grant No. 61972453.

REFERENCES

[1] Simon Birnbach, Richard Baker, and Ivan Martinovic. 2017. Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones. In *NDSS Symposium*.
[2] Samsung. 2017. SmartThings. https://www.smartthings.com. Accessed Apr, 2017.
[3] Wei Zhang, Yan Meng, Yugeng Liu, Xiaokuan Zhang, Yinqian Zhang, and Haojin Zhu. 2018. HoMonit: Monitoring Smart Home Apps from Encrypted Traffic. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1074–1088. https://doi.org/10.1145/3243734.3243820