SET YOUR TITLE USING \title

I. Introduction

1.1 Background

In recent years, smart home devices have become one of the most popular categories in the internet of things (IoT) accounting for $3.5 billion of a $292 billion industry; over 29 million smart home devices are expected to ship in 2017, a 63 percent increase over 2016 [1]. Informed purchasing is of primary concern as retailers provide smart home devices from manufacturers with little scrutiny in regards to device security or known vulnerabilities. These devices are relatively inexpensive and can be purchased, shipped, and integrated into a smart home in days; the barrier of entry is very low. As smart home technologies become more popular and easier to obtain, the increased prevalence of IoT devices in the home necessitates the need for investigation into what kind of privacy information these devices inadvertently broadcast, what vulnerabilities exist, and how privacy leakage can be used against consumers. **To do** (1)

1.2 Problem Statement

Wi-Fi and Bluetooth Low Energy (BLE) are two protocols increasingly used in a range of IoT devices such as security cameras, locks, medical devices, sensors, and a myriad of other devices. These protocols broadcast some information in the clear that anyone with a properly-tuned receiver can observe. Smart home devices using these technologies are at risk of leaking privacy data that an outside observer may

use to infer facts about the smart home such as what devices are in the home and when is the user away. Foremost, smart home owners must be informed of potential physical security implications IoT devices can introduce to their home. For example, installing a vulnerable BLE lock can allow attackers unfettered access to the home. Consumers must also have a way to defend against privacy leakage in their homes and mitigation methods need to be developed. The problem statement this thesis answers is what kind of privacy data do smart home devices leak, how can an attacker exploit this leakage to gain physical access to a home, and are there ways to defend against these vulnerabilities?

1.3 Research Goals

This work attempts to investigate this problem of data leakage in smart home devices and to see what extent information is sent in the clear by devices. It observes what reconnaissance methods an eavesdropper can use to collect wireless traffic from devices without being connected to the smart home environment and what kind of knowledge can be inferred about the smart home and its users. After collecting data from devices, this research attempts to analyze what physical security ramifications this leakage introduces. It also attempts to defend against data leakage by mitigating these findings.

1.4 Hypothesis

This research hypothesizes that IoT device leakage can be used to classify smart home devices, track whether a user is in the home or not, and identify events such as when a door is opened or when a light is turned on with a success rate of above 90%. It also theorizes that impact of data leakage can be mitigated using existing methods and techniques at a success rate of above 90%.

1.5 Approach

To represent a realistic smart home environment, a voice activated digital assistant and IoT architecture is developed by integrating a variety of commercial off-the-shelf (COTS) Wi-Fi and BLE devices with Apple's home automation application, HomeKit. Furthermore, a device classifier and pattern-of-life analysis tool is created to analyze data leakage within the smart home architecture attempting to classify devices, identify events, and track whether a user is in the home or away. Findings are synthesized to observe physical security implications and ways to mitigate vulnerabilities.

1.6 Assumptions/Limitations

The following assumptions/limitations are understood when designing and executing for the Classification, Identification, an Tracking of IoT (CITIoT) tool:

- The devices selected and smart home architecture are representative of a realistic environment.
- Wi-Fi device categories are limited to the following: outlet, sensor, and camera.
- All Wi-Fi devices must be compatible with the Homebridge server.

1.7 Contributions

This thesis contributes to the field of IoT security, specifically privacy within a smart home through four principal contributions:

- **Smart home architecture.** To analyze IoT data leakage in the wild, a realistic Smart Home Automation Architecture (SHAA) is provided that integrates Wi-

Fi and BLE COTS devices with Apple's home automation application, HomeKit.

- **Vulnerability Analysis.** This work explains how an eavesdropper can use device vulnerabilities, characteristic data exchanges, and packet sizes to create a classifier able to identify components and events within the smart home environment.

- **Classification, Identification, an Tracking of IoT (CITIoT).** It presents a tool that demonstrates four capabilities enabled by data leakage: network mapping, device classification, event identification, and user tracking.

- **Synthesis.** It stresses the importance of smart home operational security by demonstrating how CITIoT can be used to gain physical access to a smart home when a user is away.

1.8 Thesis Overview

This thesis document is arranged in six chapters. Chapter 2 provides a brief summary of relevant wireless protocols, an outline of open-source security analysis tools used, and other relevant research. Chapter 3 presents the system design details, smart home architecture, and mitigation techniques developed to analyze, exploit,and prevent smart home privacy leakage. The experiment methodology and the analysis of results are presented in Chapters 4 and 5 respectively, while Chapter 6 summarizes the research and discusses opportunities for future work in this domain.

To do...

- ☐ 1 (p. 1): get new numbers for 2018 or actual numbers from 2017

Bibliography

1. Consumer Technology Association. "Record Year Ahead: Consumer Enthusiasm for Connectivity to Propel Tech Industry to Record-Setting Revenues," 2017. [Last accessed August 27, 2017], *https://www.cta.tech/News/Press-Releases/2016/January/Record-Year-Ahead-Consumer-Enthusiasm-for-Connect.aspx*.