Computer Science Department

Project in Computer Security

236349

Spring 2019

Project 1: Attacking Apple HomeKit Framework

Suprevisor: Amichai Shulman (Amichai.shulman@gmail.com)

General Description

Home automation has become a big trend in recent years. The premise of controlling the different components of our leaving environment through new and exciting interfaces appeals to the young techie generation as well as provides unexpected comfort to older generations.

The Apple HomeKit framework is a set of services and specifications created by Apple to facilitate access and control to home automation accessories. It is comprised of an Apple provided app – the Home App – that provides a generic, slick, interface to compliant devices, the HomeKit API (used by the Home App to interact with the Home database and the network) and the HomeKit Accessory Protocol to define communication with the individual accessories.

There are many types of attacks that one can imagine in an environment that works with Apple HomeKit. These include, introducing rogue devices, adding rogue controllers to existing devices, leaking information from device and most notable leaking information or taking over an Apple device through a rogue accessory.

Project Goals

Students will go over the various specification related to HomeKit framework (including the API documentation, the HAP protocol specification and Bonjour protocol documentation). The students will create an environment that can simulate a rogue accessory (baseline implementations exist over NodeJS) and will define and execute multiple attack scenarios against an Apple device (iPhone, iPad or Apple TV).

Deliverables for the project include:

- A working environment that can simulate a rogue accessory
- List of tests performed with the following information
    - Motivation and description
    - Recording of attack

- Description of results

Students will be required to work with NodeJS environment and extend existing code written for NodeJS.

Prerequisites

- Programming experience
- Computer Security knowledge
- Understanding Internet structure and application
- Creativity and hands on capabilities

Suggested Reading

- https://developer.apple.com/homekit/
- https://developer.apple.com/documentation/homekit
- https://github.com/nfarina/homebridge
- https://github.com/KhaosT/HAP-NodeJS
- https://community.ubnt.com/ubnt/attachments/ubnt/airVision_Ideas/2505/1/HAP-Specification-Non-Commercial-Version.pdf
- http://blog.theodo.fr/2017/08/make-siri-perfect-home-companion-devices-not-supported-apple-homekit/
- https://en.wikipedia.org/wiki/Multicast_DNS