Exploring Apple Homekit

Kevin Flansburg

Kenton Miller

Overview

- Look at theoretical security decisions made for Homekit's communication.
- Look for ways in which it may not have been implemented properly (fuzzing).
- Look for ways in which third-party manufacturers may cut corners.

Motivation

- Protocol will likely become a pervasive part of many people's homes.
- Many devices wont need to be particularly secure (lights, etc.).
- But some things will need to be very secure (door locks, etc.)
- A connected and automated home is something a lot of people desire, but not if it brings a lot of vulnerability.

Approach

- Not a lot of research can be found.
- Apple does not make protocol widely available (Expensive developer program, NDA).
- Very few products on market yet.
- We will:
- Attempt to learn as much about the protocol as possible.
- Look at some of the products that have made it to market.
- In general, look for lapses in theoretical implementation

Evaluation

- Provide “audit” of the security used for Homekit
- Ensure that Homekit does not have obvious mis-implementations of security protocol
- Ensure manufacturers are held to sufficiently high requirements
- If any vulnerabilities found, document