universität
innsbruck

Department of Computer Science
Security and Privacy Lab
Course: 703647-0 18S PS3 Netzwerksicherheit

SEMINARTHESIS

IoT Light Bulb Covert Channel

Bennett Piater **0xxxxxxxx**
Julia Wanker **013146957**

Innsbruck, June 2018

Contents

1 Introduction

introduction

2 Related Work

related work chapter

3 IoT Security

IoT security introduction to chapter, short description of state of the art

3.1 Ignoring Functionality Attack

functionality ignoring attacks description

3.2 Extending Functionality Attack

functionality extending attacks description

3.3 IoT Light Bulbs

functionality extending attacks described for light bulbs in more detail

4 Related Topics

description of required knowledge in order to be able to understand and conduct attack

4.1 Covert Channel

describe how covert channel work

4.2 Communication with Light

describe general communication with light

5 Covert Channel on IoT Light Bulb

In order to crate a covert channel and show that data can be transmitted over this channel, a transmitting as well as a receiving setup is needed. For transmission one Philips Hue light bulb together with its controller is used. To receive the data a light sensor connected to an Arduino board as well as a Picoscope was used.

In the following sections first the setup components and their functionality are described in detail. After that the actual attack is elaborated.

5.1 Experimental Setup

IoT Light Bulb. We used the Philips Hue White light bulbs. The bulbs come together with a Wi-Fi bridge which allows to remotely control the them using i. e. a laptop. In order to send brightness change commands we used a command line based version of the Hue API which allows us to easily send the commands via the python script we used for realizing the data transmission. The Philips Hue White has 255 different brightness levels. In order to encode the covert communication channel we need to switch between two nearby intensities at a very high rate, since this produces small changes in the PWM duty cycle. The flickers must be done in a way such that the light sensor can properly detect those changes but a human cannot see them.

Light Sensor. We used the TAOS TCS3200 Color Sensor for measuring the changes in light intensity and get the corresponding frequency output. This sensor can easily be used with Arduino.

Arduino. Other than former researchers [1], we used the Arduino board as power source only, since the frequency output can more easily be measured using the *PicoScope* described below.

Picoscope. To decode out our covert channel we used the PicoScope 3205D MSO since it is capable of sampling 10 MS/s, which we need in order to measure the light sensor's frequency output. Actually, the PicoScope is able to sample up to 1 GS/s, but for our needs 10 MS/s suffice.

5.2 Attack Description

With this setup we were able to prove that an attacker can create a covert communication channel by flickering between two light intensities at a very high rate such that the human eye cannot recognize those changes. In the following paragraphs we give a detailed description of how such an attack can be realized. Therefore we need to look more precisely at the functional principle of the communication between light bulbs and controller. Further we have a look at how smooth brightness changes are achieved and how we actually get data out of the received signal.

Contorlling Smart Light Bulbs.

Crafting PWM Signal.

Getting Data.

6 Results

describe results of attack

7 Conclusion

work out requirements and summarize results

References

[1] Eyal Ronen and Adi Shamir. Extended functionality attacks on iot devices: The case of smart lights. In *EuroS&P*, pages 3–12. IEEE, 2016.