DAT 235

IoT & Security

IoT assign 3 Malware

Author:
Bendik Egenes Dyrli
Nikolai Kjærem Ellingsen
Jens Martin Håsæther
Mathias Solheim Jansen

Supervisor:
Geir Myrdahl Køien

2017

Contents

Chapter 1

Overview

The light bulb attack is a test done by Ronen, O'Flynn, Shamir and Weingarten that targets Philips Hue smart lamps. The purpose of the attack is to see how easy a hacker can take control of IOT devices and to share light on how badly secured our everyday IOT devices that normal people buy are.

The attack spreads from light bulb to light bulb as long as they are close enough to each other, this means that highly populated areas like dense cities could loose control over all smart bulbs. The virus only needs to be in one plugged in bulb, and if the other bulbs are close enough, the worm will spread from one to another. [2, p. 1]

Chapter 2

Analyzing weaknesses and Threats

When it came to analyzing the products weakness we started with looking at the product itself, and thinking what could we see as a threat to the product. When saying threat we mean things that could cause a discomfort to others that i.ex, might have a condition like photo-sensitive-epilepsy that are sensitive to light flashing at a high rate.

2.1 Injecting unsigned firmware

When it came to taking over a Philips Hue system, you could inject it with a "special" made software that would infect the light bulb so that it could give the attacker access to do what ever he wanted to do.

2.1.1 How does one find vulnerabilities?

When it comes to finding the vulnerabilities, there are a few different ways of doing this, you can start with looking in the software if there is some bugs that you can exploit.

But what most so called hackers do, when they want to find exploits in a piece of hardware connected to the Internet is to start looking at the hardware itself. This means by taking it apart, and looking at what kinds of chips are in use. What can be taken out from the device, like the boot loader and so on.

Chapter 3

How does it work?

The program itself is a theoretical malicious program implemented as an idea to show why it is important to improve the security of PLS units, and Zigbee connected sensors.[2]

The program itself takes advantage of the fact that it can self-replicate throughout the network(worm based), therefor spreading by little or no user interaction apart from the initial infection.

The attack main target were smart lamps that used "Philips Hue" smart lamps and various types of protocols connecting them together among others:

- ZLL - Zigbee Light Link
- ZLL Touchlink Commission protocol
  - Touchlink's proximity check protection mechanism
- Philips Hue personal wireless lighting system
- Philips Hue light hardware and software

The aforementioned above allows the worm to spread from one unit to another without user interaction and essentially create a "virus" that spreads like wildfire.[2, p.6]

The next problem comes in executing the code is the persistence of code execution as they do not allow direct code execution from memory. One option here would be to resort to Return Oriented Programming (ROP) but since this will require knowledge of each individual model it is unfeasible for spreading in large varied systems. What instead is targeted is the ZigBee Over-the-Air Upgrading Cluster standard [2, p.7] as is contains customization that solves a lot of the problems with ROP.

Now everything is in place for both to have the worm be able to infect, but also spread.

The next area is looking at possible attack surface and width. Assuming that Light-bulb A and Light-bulb B share the same network and/or key, the spreading is seamless. However if the network gets branched or the keys get altered in transit during an attempt for infection

and the key altering does not affect any infected units the infection also comes to a halt. So a good way to contaminate a supposed worm would be to separate the network into several sections, each with its own altering key, but assuming the attacker is still semi-close then this is for nought, as the attacker can use a initial infection for a new subsection and let itself spread again.

3.1 Suggested countermeasures

Suggested countermeasures to prevent such an attack is to use unique keys for all the light bulbs so that the bulbs can't encrypt firmware for other smart bulbs. The paper states that this is already supported by the Zigbee OTA and that all it needs to work is to implement it in the backend server. [2, p. 14]

They also state that the attack can be countered by using asymmetric cryptography for verification of software. However they also state that this may cost too much for these type of IOT devices. It will also not protect against other methods of leaking the keys.[2, p. 14]

One of the bugs that was used to create the attack can be found by doing a negative test in the ZLL transaction ID field this is done by trying to send the value 0 for every message of the protocol. this means that if it was done more extensive tests on beforehand the bug could have been found and fixed.[2, p. 14]

Chapter 4

Impact

4.1 Bricking

When a device has been infected, it may be tricked to do numerous actions. For example bricking the device, making it unusable. Since the worm replaces the devices firmware, it can permanently cause constant flickering or similar. The only way to fix this is by accessing the PCB, but when the device is potted, this proves troublesome.

4.2 Jamming

Since ZigBee runs on the 2.4 GHz band(IKEK 802.15.4) which is also used in WiFi protocol(IEEE 802.11b/g). And the test mode included in the device transmits a continuous wave signal without checking if channels are clear. This can therefore be used to cause interference with WiFi.

4.3 Infiltration

The device can also be used to infiltrate air gapped systems. They can be set to blink data either too rapidly for the human eye to detect or at wavelengths that are hard to detect. Data can be transferred with a simple telescope aimed at the device. This has been proven to work at 100m with a speed of 10KB per day. Not a lot, but still a huge breech of security within an air gapped system. [1]

4.4 Epilepsy

Since as mentioned previously, the device can be set to blink. This means that it can be used to cause epileptic seizures in susceptible individuals. This is perhaps the most unethical usage of the hack.[3]

4.5 Actual impact

The actual impact of this hack has been minuscule compared to IP cameras and similar from less reputable sources. As they can be used to DOS systems, which is far more profitable than controlling light bulbs. The security impact however is still present. This is particularly evident in the number of articles and news sites that have picked up this story. This may be the largest impact of this hack, more knowledge of the dangers that IoT systems may pose.

Bibliography

[1] Ingenious Light bulb Hack Can Cause Seizures, Spy On 'Air-Gapped' Networks [Online] https://www.forbes.com/sites/thomasbrewster/2016/04/01/philips-lightbulb-hack-epileptic-seizures-data-theft/63ce9e8378de [Accessed:11.October 2017]

[2] IoT Goes Nuclear: Creating a ZigBee Chain Reaction kek [Online] http://iotworm.eyalro.net/iotworm.pdf [Accessed:13.October 2017]

[3] Hackers Attack Epileptics Forum With Snow Crash-like Seizure Inducing GIFs https://gizmodo.com/373768/hackers-attack-epileptics-forum-with-snow-crash-like-seizure-inducing-gifs [Accessed:15.October 2017]