IoT Light Bulb Covert Channel and Other Functionality Extension Attacks: Related Work

Julia Wanker, Bennett Piater

April 11, 2018

1 Security of IoT Devices

1.1 General Security

It is widely known that IoT devices have poor security in general. The most recent state-of-the art security survey was performed by Zhang et al. [11] They provide a detailed analysis of vulnerabilities and defence mechanisms. In particular, they note that much academic literature is overly conservative because most security analyses are published in whitepapers and on blogs, causing them to be ignored in scientific surveys. They suspect either a lack of expertise, or outright neglect of security design on the part of the vendors.

Additionally, Restuccia et al. [8] recently provided a very good analysis and taxonomy of the systematic problems and future challenges of IoT security. The paper strongly advocates for security by design of connected devices from their cradle to their grave.

1.2 Smart Light Security

The security of smart light systems is particularly important because of their ubiquity. Hence, researchers have studied them in detail.

Dhanjani [3] found several ways to initiate *Denail-of-Service* (DoS) attacks. He was able to cause sustained blackouts which can be of high risk i.e. if hospitals are involved. The primary security issue allowing this attack lay in the connection of smart bulbs to their controller. Dhanjani also mentioned the possibility of encryption flaws in the implementation of the *ZigBee Light Link* (ZLL) which is used for communication between the bridge and the light bulbs. However, this attack would only work within close proximity, limiting it's impact.

Morgner et al. [7] further investigated the security of ZLL and showed that the aforementioned attack is more dangerous than anticipated. They were able to control ZLL-certified light bulbs from a distance over 15 to 36 meters. Their research proved and particularized Dhanjani's [3] findings

that exploitable vulnerabilities exist in the design of the ZLL standard. ZLL provides the so-called *touchlink commissioning* which uses a global ZLL master key to secure the setup process. This master key was leaked in 2015 [7] and ever since the touchlink procedure is considered to be insecure. Due to the flaws in the touchlink specification Morgner et al. were able to introduce a new network key which was then accepted by all connected light bulbs, further allowing the authors to send malicious commands.

Ronen et al. [10] also used flaws in ZLL to attack smart light solutions. Their attack was of even higher concern since they were able to exchange the light bulbs firmware with one containing malware, and, because of vulnerabilities in the ZigBee communication, they were able to further spread the malware over all nearby light bulbs. Thus, an attacker would be able to launch a *war-flight* and infect all smart lamps of a whole city.

2 Functionality-Ignoring Attacks

A big portion of the research on IoT security was conducted about attacks ignoring the intended functionality of IoT devices. In particular, the appearance of the Mirai botnet led to multiple papers about botnets comprised of IoT devices.

Angrishi [1] makes the very important point that IoT devices should not be seen as specialized devices with added intelligence, but rather as (general) computing devices that are performing specialized tasks. Attackers are certainly aware of this, and most attacks on IoT devices involve botnets for DDoS or spamming. DDoS-capable malware was surveyed and classified by Donno et al. [4].

The most comprehensive analysis of the Mirai botnet, responsible for the record-breaking 1.3Tb/s DDoS on DynDNS, was published by Antonakakis et al. [2]. In particular, they found a list of default passwords found in the source code of the malware, which clearly show it targeting cheap IoT devices, many of them IP cameras. They clearly show that Mirai succeeded primarily because of incredibly low-hanging fruit: (tiny) dictionary attacks on devices accessible from the open internet were enough.

3 Functionality-Extending Attacks

The most interesting kind of attack is the so called *Functionality-Extending Attack* where e.g. an attacker uses an IoT lightbulb for other purposes than illumination. In particular, an attacker can use light emitting diodes (LEDs) for an optical wireless communication system, which was elaborated several years ago [6, 5]. Since smart light solutions use LEDs, Ronen and Shamir [9] were able to create a covert communication channel using smart lights. As the setup process of an IoT light bulb is vulnerable [3, 7, 10], Ronen and

Shamir were able to abuse the *application programming interface* (API) of the IoT light bulb in order to make the LEDs switch between two light intensities at a very high rate, such that it cannot be noticed by the human eye but can be detected by a light sensor. The light sensor measures the exact duration and frequency of those flickers and converts it to a digital frequency in order to leak sensitive data. Ronen and Shamir showed that this kind of attack can be used to extract data from air-gapped networks. Besides leaking data through a covert channels, they have shown that the light flickering can also be misused for creating epileptic seizures.

References

[1] Kishore Angrishi. Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*, 2017.

[2] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In Engin Kirda and Thomas Ristenpart, editors, *USENIX Security Symposium*, pages 1093–1110. USENIX Association, 2017.

[3] Nitesh Dhanjani. Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system. 2013.

[4] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. Analysis of ddos-capable iot malwares. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *FedCSIS*, pages 807–816, 2017.

[5] H. Elgala, R. Mesleh, H. Haas, and B. Pricope. Ofdm visible light wireless communication based on white leds. In *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pages 2185–2189, April 2007.

[6] T. Komine and M. Nakagawa. Fundamental analysis for visible-light communication system using led lights. *IEEE Transactions on Consumer Electronics*, 50(1):100–107, Feb 2004.

[7] Philipp Morgner, Stephan Mattejat, and Zinaida Benenson. All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. *CoRR*, abs/1608.03732, 2016. Useful to show insecurity of Smart Lights in particular. They give a good overview of attacks (as of 2016) against smart lights in section 5.2! This may be useful to show how dangerous the attack from our main paper can be: They can also take control of ZLL lightbulbs without WIFI access to the controller! This means that one could establish a covert channel from outside the building, or possibly bridge an air gap between networks. Also a fantastic introduction to Zigbee LightLink.

[8] Francesco Restuccia, Salvatore D'Oro, and Tommaso Melodia. Securing the internet of things: New perspectives and research challenges, March 2018.

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

[10] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. Iot goes nuclear: Creating a zigbee chain reaction. *IEEE Security & Privacy*, 16(1):54–62, 2018.

[11] Nan Zhang, Soteris Demetriou, Xianghang Mi, Wenrui Diao, Kan Yuan, Peiyuan Zong, Feng Qian, XiaoFeng Wang, Kai Chen, Yuan Tian, Carl A. Gunter, Kehuan Zhang, Patrick Tague, and Yue-Hsun Lin. Understanding iot security through the data crystal ball: Where we are now and where we are going to be, March 2017.