Investigation of Vulnerabilities on Smart Grid End Devices

Yutian Gui
University of North Carolina at Charlotte
Charlotte, USA
ygui@uncc.edu

Ali Shuja Siddiqui
University of North Carolina at Charlotte
Charlotte, USA
asiddiq6@uncc.edu

Suyash Mohan Tamore
University of North Carolina at Charlotte
Charlotte, USA
stamore@uncc.edu

Fareena Saqib
University of North Carolina at Charlotte
Charlotte, USA
fsaqib@uncc.edu

***Abstract*— The Internet of Things (IoT) are paradigm shift transforming embedded objects into a smart connected device, ready to sense, analyze and communicate information with other devices. Nowadays, IoT devices are widely used in smart home systems and smart grid systems at a high level of integration and automation. However, the increasing tendency of the smart device also leads to a problem of security. The recent exploitations of the connected smart devices' vulnerabilities reinforce the importance of security implementation and integration at the system level. In this work, we propose some use cases to show the vulnerability of the smart bulb to different attacks.**

Keywords—IoTs, hardware security, smart homes, smart grids, side-channel attack, firmware attack, reverse engineering

I. INTRODUCTION

With recent advancements in smart grid and home automation, devices have become "intelligent". By integrating microcontrollers, sensors and customized applications, today's home technology is sophisticated and hard to manage and coordinate.

One solution to make all the devices work collaboratively is to connect all the embedded devices together to form an IoT network. There are several standard communication mediums and architectures for connected IoTs to form a Local Area Network (LAN) with centralized management, such as Bluetooth, WiFi, and Zigbee.

Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create small area networks with low-power digital radios, such as for home automation, medical device data collection, and smart grids. [1] Since Zigbee requires an extra, independent module for controlling and communication, Bluetooth is more welcomed because using cellphones to controlling all the smart devices is more convenient. Bluetooth is a wireless technology standard for exchanging data over short distances and it is widely integrated into smartphones and personal computers.

The unified communication standard reduces the complexity of management, but also raises some problems related to security. The smart devices communicate over a similar physical channel with each other and the host machine use same communication standard (for example, Bluetooth), therefore it is possible to exfiltrate information, tamper data and hijack the device even without the permission to accessing the specific device.

In this work, we demonstrate the vulnerability of smart bulbs to invasive and non-invasive attacks. Specifically, we performed eavesdropping/tampering attack, port knocking attack and side-channel attack on the Magic Blue UU Bluetooth Bulb successfully.

Paper organization: The rest of the paper is organized as follows. Section II introduces related work, Section III gives the detail and experimental setup of different attack models. The result of attacks is presented in Section IV and Section V is the conclusion.

II. RELATED WORK

As a typical representative of in-home IoT devices and endpoint devices in the smart grid, smart bulbs [2] are light bulbs that can be programmed remotely, to manipulate lighting options. Compared to traditional bulbs, the smart bulb has two obvious advantages. The first one is that the smart bulb can be controlled through different communication protocols (Zigbee, Bluetooth, and WiFi) from everywhere wirelessly, even far away from home. (The distance depends on which network protocol is used for connection) Another advantage is that the smart bulb is fully controllable. It means that all the parameters, including intensity and color, can be changed freely by using applications on the master controller (For example, a smartphone). Some smart bulbs, like Magic Blue UU, provide more functionalities to satisfy different requirements (For example, timer function and scenes mode).

The current generation of smart home appliances has proven to be vulnerable to remote hijacking attacks [3][4] and nefarious actors [5][6]. Smart home appliances have shown to leak private information, which can consequently be used by

978-1-7281-2925-9/19/$31.00 ©2019 IEEE

malicious entities to either eavesdrop or to gain access to victims' personal space and belongings.

Currently, there is no standardized protection for these IoT devices, leading to different attacks, such as the virus, malware, remote access, eavesdropping attack, port knocking attack, and side-channel attack.

A. Denial of Service (DoS)

Smart bulbs use Bluetooth, Zigbee, and Wifi for remote access. To deny remote access, the radio frequency spectrum can be jammed. Jamming in wireless networks is defined as a disruption by blocking or interfering the authorized communication process. The most common way to realize jamming is to reduce the signal-to-noise ratio and this can be achieved using radio jammers or Bluetooth signal specific jammers. Depending on the application, the impact of jammers can pose safety and security risks.

Currently, the detection of jamming is not difficult to achieve because the choke caused by jamming can be easily detected by real-time monitoring on the traffic. However, there are limited effective countermeasures against Bluetooth jamming. Channel hopping [7] is the most common countermeasure for defending jamming attack which changes the communicating channel after every certain period of time. However, the efficiency of channel hopping can be reduced by using multiple jammers at the same time [8].

B. Eavesdropping: Lack of Authentication and Encryption

The current generation of in-home smart devices provides an open interface for manipulation [9]. Any device that supports the same communication standard as the bulb can connect the bulb without the requirement of permission or certification because there are no authentication or encryption schemes for incoming connections. This lack of security can be used by an attacker to modify the behavior of a bulb without the control as a legitimate user.

Moreover, the risk of eavesdropping is increased more deeply by the loophole of physical accessibility. All the smart bulbs, including the Magic Blue UU bulb used in this work, provide a physical port for debugging and flashing. The built-in programmed code and all the information stored in the memory system can be read and tampered easily.

C. Malicious Firmware Updates

The smart bulb contains a microcontroller which allows Over the Air (OTA) Updates [10]. This feature is provided for developers to update the firmware of a device remotely. However, this feature can be also used for malicious purposes. Attackers can push updates to the code, which can not only perform undesired actions but also repurpose the bulb to leak its information through its side channels. This information can be as trivial as the color of the lights to potentially more invasive information such as operating times. Operating times for a bulb can lead to profiling a user of this bulb to facilitate adversaries to plan theft [11].

In addition to the OTA, the physical access port for firmware access and debugging can be also used for malicious update [9], such as port-knocking. Port Knocking is a technique for implementing security through obscurity [12]. In computer systems domain, each service occupies a unique port. Attackers may misuse the open access to perform Denial of Service (DoS) or brute-force attacks. Port knocking proposes that the initial state of a port should be closed until the host receives the correct pre-determined sequence (trigger).

D. Side-Channel Attack

Different from other attacks, the Side-Channel Attack (SCA) focuses on the physical parameters and the weakness of the implementation of the cryptographic algorithm levels, such as power consumption, time delay, and electromagnetic radiation.

With the running process in a device, some critical information is leaked inevitably. The leaked information, such as power consumption or electromagnetic radiation, reflects the operation on processed in the device correspondingly. The main purpose of SCA is to figure out the relationship between the variation of physical parameters and hardware operation thereby reveal the hidden information, such as the secret key of encryption. SCA can not only exfiltrate information from the communication process but also break encryption based on analyzing the variation of parameters during the runtime.

As an effective method to attack electronic devices, power analysis uses power consumption of the hardware as an information source. Since all the electronic devices work relying on electricity, so power is the easiest physical parameter to acquire and utilize. The power consumption of an integrated circuit reflects the operation of its individual elements, as well as the capacitance and other electrical properties of the system. By collecting power traces and modeling analysis, the hidden information can be extracted.

Simple Power Analysis (SPA) is the simplest type of SCA. The attacker measures variations in the power consumption of a device, hence get the key based on the physical properties of hardware devices. However, the SPA attack has been proved that it is not efficient to attack encryption on the hardware-based implementation [13]. To attack the encryption with smaller power variation on the hardware-based implementation, Differential Power Analysis (DPA) uses a statistical method which compares the difference of each measured power trace to remove the noise and locate the attack point. Another SCA is Correlation Power Analysis (CPA). CPA builds a mathematic model and uses the Pearson correlation coefficient to evaluate the relationship between hypothetical keys and the actual power consumption, thereby extract the key used in the encryption.

Electromagnetic radiation can be also used for performing the side-channel attack. In cryptography, ElectroMagnetic (EM) attacks are side-channel attacks performed by measuring the electromagnetic radiation emitted from a device and performing signal analysis on it. [14] Compared to power analysis, the EM attack provides a more efficient way to exfiltrate data by observing the normal functioning of the target device without physical proximity.

III. Proposed Attacks and Setup

The bulb used in this work is Magic Blue UU Bluetooth Bulb and the System on Chip (SoC) used in the bulb is RTL8762AG from Realtek company. [15]. Figure 1 and figure 2 shows the smart bulb used in this work and the logic board component inside the bulb.

RTL8762AG is an ultra-low-power system-on-chip solution for Bluetooth low energy applications that combines the excellent performance of a leading RF transceiver with a low-power ARM®CortexTM-M0, 256KB eFlash, 80KB RAM, and rich powerful supporting features and peripherals. [15] The ROM contains the operating system, in this case, freeRTOS. Flash is used for storing applications (programmed code) and RAM is used for storing received command message and temporary data. The memory architecture is shown in Figure 3.

Figure 1.Magic Blue UU Bluetooth bulb [2]

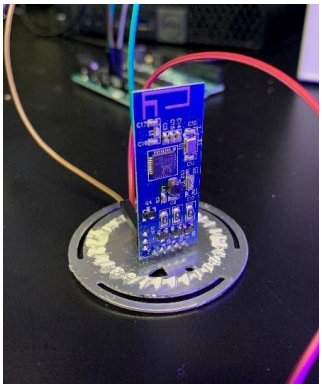

Figure 2. Logic board component

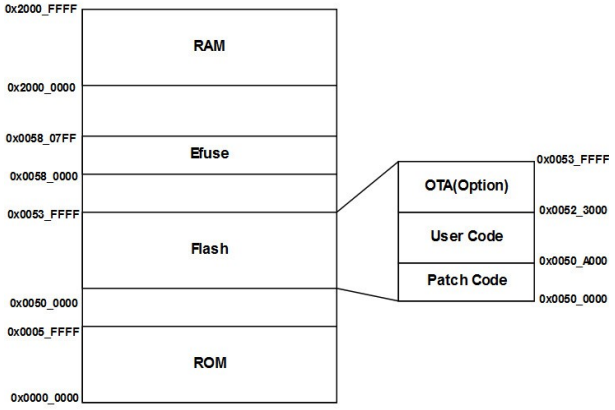

Figure 3. Memory Architecture

The hardware and software we used are shown in the following list:

- Debug tool SEGGER J-Link [16].
- Reverse engineering tools from machine to assembly code.
- Oscilloscope for waveform capture.

A. Eavesdropping/Tampering Attack

In this work, we first demonstrate an eavesdropping attack to reveal the hidden message used for controlling the bulb. RTL8762AG supports the Serial Wire Debug (SWD) interface as a part of the Debug Access Port (DAP). This offers a flexible mechanism for non-intrusive program code debugging and also gives the attacker a chance to invade into the system.

In RTL8762AG, we only use P1_0 (SWDIO, debugging port) and P1_0 (SWDCLK, the pin used for giving clock signal to the circuit.). These two pins are connected to the debug tool (SEGGER J-Link) for debugging and flashing. The pin assignment is shown in Figure 4. The setup for eavesdropping and port knocking includes connecting the ground, clock, and IO pins from the logic board to the power supply and to J-link. J-link connects to a computer via USB. The setup of all the component is shown in Figure 5.

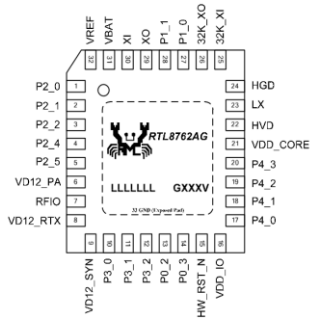

Figure 4. The pin assignments of RTL8762AG. [15]

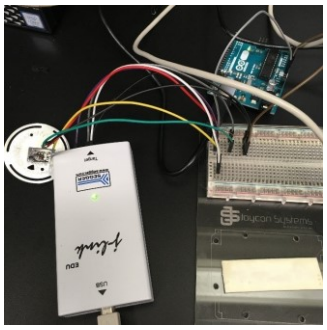

Figure 5. The setup of eavesdropping attack and port knocking attack.

After connection, we used the J-Link Commander (the software for debugging) to extract data from memory systems. As the memory system is shown in Figure 4, the chip has three layers of memory. The ROM contains the operating system, in this case, freeRTOS. Flash is used for storing applications (programmed code). RAM is used for storing data and machine code currently being used. Changing the command message and the device name in the RAM does not allow them to be changed permanently. In order to change the device's name permanently, the flash memory was accessed, and we were able to permanently change the name of the LED device.

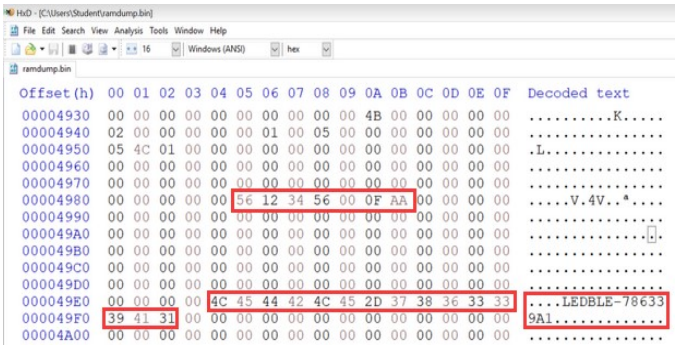

Figure 6. The RAM dump disassembly

Figure 6 shows the RAM dump disassembly. The message **56 12 34 56 00 0F AA** (the standard format is **56 RR** (Red) **GG** (Green) **BB** (Blue) **WW** (Warm) **0F AA**) is the control message and **4C 45 44 42 4C 45 2D 37 38 36 33 33 39 41 31** is the original name of the device (LEDBLE-786339A1).

B. Port Knocking Attack

Port Knocking is a technique for implementing security through obscurity [12]. In computer systems domain, each service occupies a unique TCP or UDP port. These ports are open for an outsider to connect. Port knocking proposes that the initial state of a port should be closed and requires a pre-determined sequence of packets to the host as a trigger. The host opens access to a client when the correct sequence of packets is received. This process can be utilized by the attacker to perform the port knocking attack.

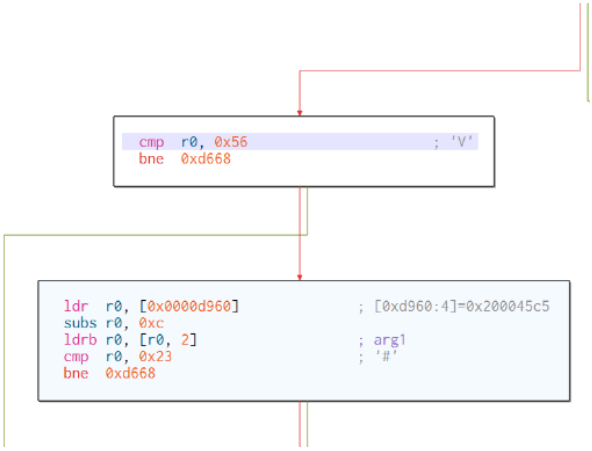

Figure 7. The function of setting colors

In this work, we investigated the port knocking attack on the smart bulb. As shown in Figure 7, 0x56 is the opcode for setting colors. Every time 0x56 is detected, the bulb sets color according to the color value it received. To realize the port knocking attack, a new trigger with a sub-sequential malicious function. Every time the new trigger is activated, the system will jump to the malicious function automatically.

C. Side-Channel Attack

In this work, the real-time fluctuation of the voltage is used for building the mathematic model and extracting the information of command messages.

The bulb has four different sets of light, red (R), green (G), blue (B), and warm (W). The warm lights work alone with RGB lights, and it has no influence on the displayed color. The color and the intensity are controlled by the co-work of RGB lights. The pins of different lights are shown in Figure 8. The real-time fluctuation of the voltage is collected by the oscilloscope (Figure 9) for building the reference model.

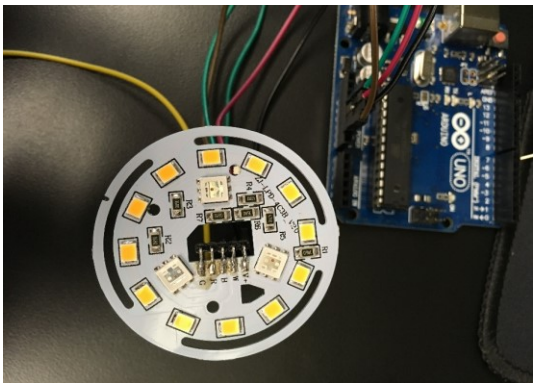

Figure 8. Pins of colors

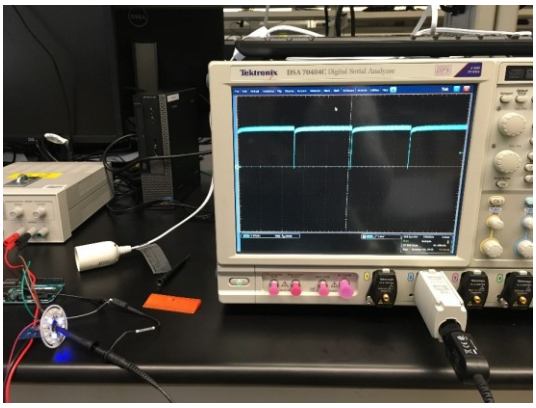

Figure 9. Setup of power measurement

By analyzing the power trace, we found that the color can be distinguished by the amplitude and the intensity can be distinguished by the duty cycle. Figure 10 shows an example of waveforms with different intensities. The uppermost one is the real-time voltage waveform of red light with intensity 10, the middle one is the waveform with intensity 100 and the bottom one is the waveform with intensity 200. With the change of intensity of the light, the duty cycle also changes.

In this attack, we first built the reference database of all the command messages correlated to different duty cycles and amplitudes based on the power traces we collected. Then, every time a new unknown power trace is captured, the message can be easily extracted by comparing its amplitude and duty cycle with the database.

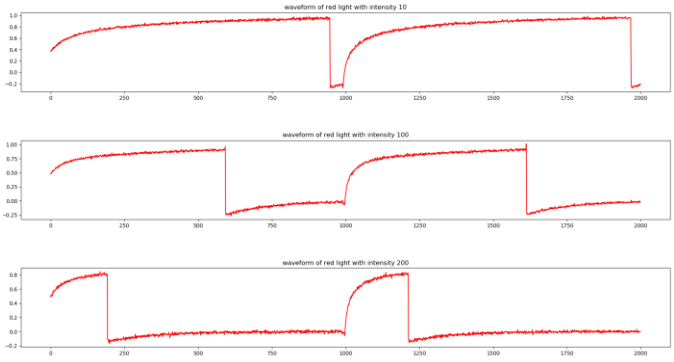

Figure 10. Power traces of red light with different intensities.

IV. Experiment Results

A. Eavesdropping/Tampering Attack

After knowing the meaning of the message, we were able to change the name of the device and the color of the bulb freely by modifying the value.

Figure 11 and figure 12 show the name of the device after tampering. By overwriting the data into RAM, the name of the device was changed to **IOT-UNCC-HACK**.

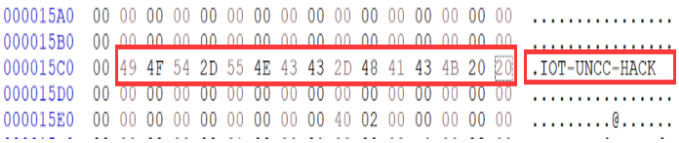

Figure 11. Modified name of the device

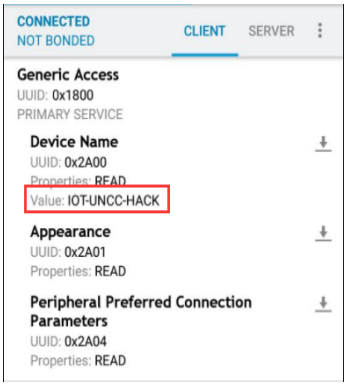

Figure 12. New device name

B. Port Knocking attack

To apply port knocking attack, we added an additional opcode (0x57) as a trigger and added an additional malicious function into the flash to realize the attack. Figure 13 shows the modified code.

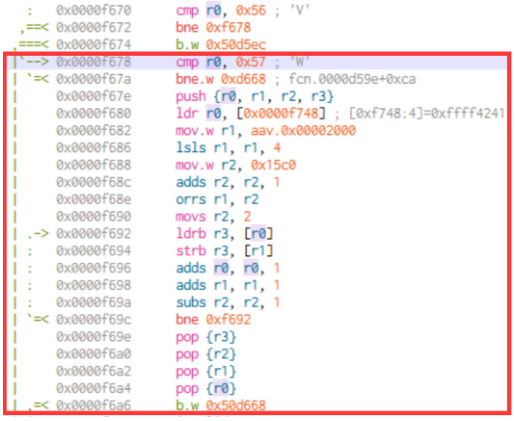

Figure 13. The modified code

After the configuration, every time the system receives the header without value 0x56, it will check if the header is 0x57. If so, the running process will jump to the malicious function and works following the malicious function which is shown in the area bounded by red lines in Figure 13.

C. Power Analysis

Waveforms of different colors are collected and analyzed separately. The value of intensity can be deduced by comparing the duty cycle of unknown trace with the reference database and the color of the unknown trace can be deduced by analyzing its amplitude.

Figure 13 shows the result of power analysis. After comparing the unknown power traces with the reference database, the command ***56 01 01 01 00 F0 AA*** correlated to the unknown traces can be easily extracted.

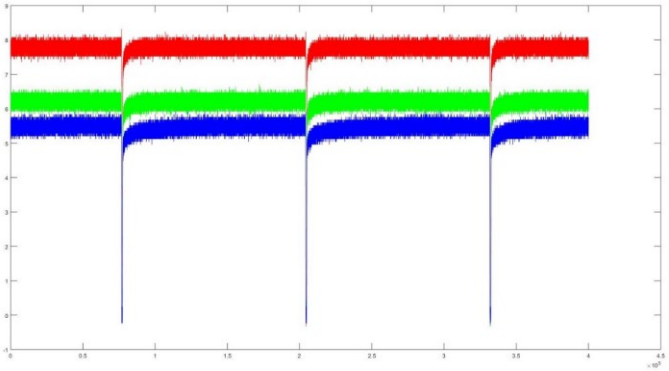

*Figure 14. Power trace with command **56 01 01 01 00 F0 AA**.*

V. Conclusion and Future Work

In this paper, we demonstrate the vulnerability of current IoT devices in the smart home system and grid systems such as a smart bulb, including eavesdropping/tampering attack, port knocking attack, and side-channel attack. The lack of protection and authentication of modern smart devices has brought a serious safety concern which is proved by experiments in this work.

To mitigate the risk of invasive and non-invasive attacks, the future work will include the investigation on the feasibility of security solutions, such as authentication and encryption on the IoT devices deployed in the smart home and smart grid.

Acknowledgment

This research has been sponsored by the National Science Foundation under grant No.1819687 and No.1819694.

References

[1] Z. B. Alliance, ZigBee Specification FAQ. [Online]. Available: https://web.archive.org/web/20130627172453/http://www.zigbee.org/Specifications/ZigBee/FAQ.aspx [Accessed: 17-Mar-2019]

[2] "Magic Blue UU Bluetooth Bulb," *GearBest*. [Online]. Available: https://www.gearbest.com/smart-light-bulb/pp_230349.html. [Accessed: 17-Mar-2019].

[3] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[4] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

[5] L. Hautala, "Send a line of code to a surveillance camera, get the username and password, report says," *CNET*, 07-May-2018. [Online]. Available: https://www.cnet.com/news/hackers-can-peek-through-surveillance-cameras-report-says/. [Accessed: 19-Mar-2019].

[6] A. Greenberg, "How Hacked Water Heaters Could Trigger Mass Blackouts," *Wired*, 13-Aug-2018. [Online]. Available: https://www.wired.com/story/water-heaters-power-grid-hack-blackout. [Accessed: 19-Mar-2019]

[7] S. Khattab, D. Mosse, and R. Melhem, "Modeling of the Channel-Hopping Anti-Jamming Defense in Multi-Radio Wireless Networks," *Proceedings of the 5th International ICST Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2008.

[8] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, "Ares: an anti-jamming reinforcement system for 802.11 networks," *Proceedings of the 5th international conference on Emerging networking experiments and technologies - CoNEXT 09*, 2009.

[9] U. Shaked and U. Shaked, "Reverse Engineering a Bluetooth Lightbulb," *Medium*, 03-Aug-2016. [Online]. Available: https://medium.com/@urish/reverse-engineering-a-bluetooth-lightbulb-56580fcb7546. [Accessed: 10-Apr-2019].

[10] "Porting the OTA DFU to your Custom App (SDK 12)," *Nordic DevZone*. [Online]. Available: https://devzone.nordicsemi.com/b/blog/posts/porting-the-ota-dfu-to-your-custom-app-sdk-12. [Accessed: 10-Apr-2019].

[11] Ali Shuja Siddiqui, Yutian Gui, David Lawrence, Stuart Laval, Jim Plusquellic, Madhav Manjrekar, Badrul Chowdhury and Fareena Saqib. "Hardware-Assisted Security Architecture for Smart Grid", *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018

[12] Krzywinski, M. 2003. Port Knocking: Network Authentication Across Closed Ports. *SysAdmin Magazine* 12: 12-17

[13] Paul C. Kocher, Joshua Jaffe and Benjamin Jun. "Differential Power Analysis," CRYPTO '99 Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, 1999

[14] "Electromagnetic attack," *Wikipedia*, 18-Feb-2019. [Online]. Available: https://en.wikipedia.org/wiki/Electromagnetic_attack. [Accessed: 10-Apr-2019].

[15] "Realtek RTL8762AR/AG/AJ/AK-CG Datasheet 1.3," *Realtek*. [Online]. Available: vrtp.ru/index.php?act=Attach&type=post&id=742189. [Accessed: 11-Apr-2019].

[16] "J-Link EDU," *SEGGER*. [Online]. Available: http://www.segger.com/products/debug-probes/j-link/models/j-link-edu. [Accessed: 11-Apr-2019].