Wiz Light Bulb: An introspective into the dangers that insecure IoT devices bring to the house

1nd Daniel Alejandro Leon Ortiz 2nd Dominykas Baronas 3rd Jose Fredy Navarro Motta
Daniel.A.Leon.Ortiz-1@ou.edu *Dominykas.Baronas-1@ou.edu* *Jose.Fredy.Navarro.Motta-1@ou.edu*
OU ID: 113631377 *OU ID: 113648310* *OU ID: 113641709*

***Abstract*—This paper focuses on exploiting and exposing vulnerabilities found in readily available consumer focused IoT devices, in specific the Wiz Light Bulb, with the purpose of informing readers of potential breaches of privacy and the dangers that come with them, that they may inadvertently bring to their houses or buildings.**

***Index Terms*—wiz, security, internet of things, internet, network, privacy breach**

I. Introduction

In recent years, the utilization of Internet of Things (IoT) devices has experienced an unprecedented surge. This remarkable growth can be attributed to the increasing interconnectedness of our world, as more and more devices, from everyday appliances to industrial machinery, become equipped with IoT technology, for example this exponential growth can be put into perspective in the graph found in figure 1.

These smart devices have revolutionized the way we live, work, and interact with our surroundings, offering enhanced convenience, efficiency, and data-driven insights. However, as the adoption of IoT devices continues to rise, so do the possibilities of experiencing security vulnerabilities and cyber-attacks. This underscores the critical importance of addressing IoT security concerns to safeguard our increasingly connected digital ecosystems.

Recent statistics paint a concerning picture of the IoT security landscape - a 2018 study by Gemalto found that nearly half (48%) of companies cannot detect if their corporate IoT devices are being breached. With the global IoT market expected to reach $520 billion by 2021 [1], the scale of vulnerabilities will only increase.

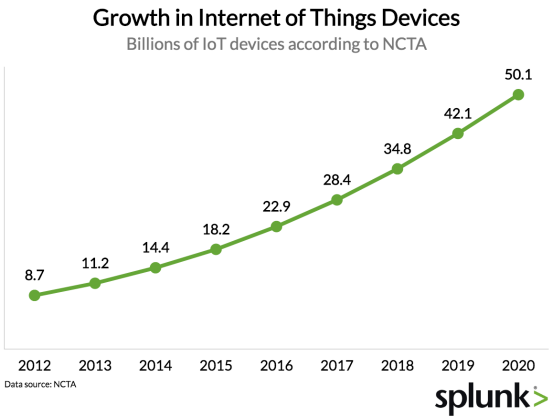

Fig. 1. Growth of IoT devices, from [11]

With the growing rise of IoT devices, their availability has become common place in most supermarkets and retail stores, leading most households to give them a try and many companies are trying to capitalize on this boom, one such device that we will look at in detail is the Philips manufactured Wiz Light Bulb, a simple smart LED light, with a mobile application attached to change and modify the properties (brightness, color and scenes) of the light.

Such a device when looked into detail revealed easily exploitable vulnerabilities in its security and

protocols, leading us to discover and launch attacks that could be potentially used by malicious attackers to expose the daily activities of households or buildings and the individuals within them, allowing a breach of privacy on the victims.

The approach we took is quite different from what others before have thought, instead of infecting the device with malware through insecure protocols, using the light and its physical properties to cause harm to a household or self-replicating attacks that infect a whole network, we decided to focus on a non-harmful attack, that taps into and records data from the light, that we then package and analyze, generating potentially harmful data that an attacker can use or sell in a variety of dangerous ways.

II. Overview

A. Background

Due to the rising popularity of IoT devices, a lot of papers have discussed the risks and how to conduct a proper security analysis of these machines, how to properly rank them and how to give insight to consumers in a concise manner, as such inspiration for this project, it led us to want to explore the security of a particularly popular and cheap device, in the following paragraphs we explore these papers.

Firstly, an interesting point was raised by S. Agarwal et al., and that is that IoT devices do not have host-centric security solutions like antiviruses, firewalls or malware detection in general, they run on firmware that is hardware-specific, and each device type has different protocols on how to run. These devices also collect a lot of data and most manufacturers do not develop with security in mind, this means that criminals can gain a lot of sensitive information [2], from their assessment, it was determined that most IoT makers do not secure their devices and that in some cases it is not even possible to modify credentials, so these are some crucial aspects to test and determine in our project.

Now as far as language and mass consumer knowledge, these devices need to be treated in a more particular manner, since most users are not tech-savvy, they don't know if what they're buying is actually secure or not, so M. Allifah et al. promote the usage of Analytic Hierarchy Process to solve the Multi-Criteria Decision-Making problem of whether or not a specific device is actually secure or not [3], setting up priorities for certain criteria to give mathematical analysis and real comparisons, and using language that can better inform consumers about risks and give manufacturers accountability for the faulty security protocols they use.

Related to real tests and factual evidence of very specific vulnerabilities M. Yu et al actually document some possible avenues of attack with their paper, exposing three very important layers in the attack surface [4]:

- Hardware layer: Unsafe debugging interfaces, unprotected flash chips and leakage of sensitive hardware information.
- Software layer: Unsafe bootloaders, unsafe operating systems, leaks of information in the firmware, unsafe application services and incorrect configurations.
- Protocol interface layer: Unsafe interface of remote management, leaks in the information transmission and weak authentication.

These possible avenues will be taken into account for the analysis of each device, and will serve as a guide to follow and to possibly look at other types of attacks or vulnerabilities.

According to M. Ravi, Faculty of Informatics at Eötvös Loránd University, in his survey on security risks in the Internet of Things (IoT) environment, the research delves into the evolution of IoT and its impact on daily life. [5] It highlights the rapid growth of Internet-connected devices and their integration into various aspects of our lives. While IoT devices offer convenience, they often have limited processing and memory capacities, making them vulnerable to security threats and attacks. Thus, convenience is typically exchanged for protection.

The survey strongly emphasizes the importance of addressing vulnerabilities in IoT security, particularly in sensitive domains like healthcare. Nonetheless, the research acknowledges the challenge posed by IoT devices' constrained computational power in implementing secure communication protocols such as SSL.

Security issues associated with the Internet of Things (IoT) are classified into four categories: application layer, architecture, communication, and data protection. The research lists common threats related to IoT, such as intensified surface attacks, legacy systems, undetected devices, unauthorized remote access, and exposure to sensitive data. The importance of addressing these threats is emphasized, with a focus on network-based security. Physical attacks, encryption attacks, software attacks, and network attacks are discussed, along with specific threats like node tempering, interference of RF with RFIDs, physical damage, traffic analysis attacks, and man-in-the-middle attacks.

According to Y. Alotaibi et al. survey, it presents the pivotal role of the Internet of Things (IoT) in our daily lives, where virtually everything is connected and accessible via the internet, enabling data collection and exchange among devices. Despite significant technological advancements, IoT faces security challenges, particularly due to the limited resources of IoT devices, making them vulnerable to cyberattacks. [6] The survey highlights challenges related to security and privacy, given the widespread connectivity of IoT devices and the anticipated growth of AI-driven decision-making processes.

Security attacks are discussed in the context of IoT across different layers of its architecture. In the perception layer, it highlights the vulnerability of IoT devices and suggests the need for automated, lightweight, and cost-effective security solutions. It mentions specific attacks like "Tag Cloning", "Radio Frequency (RF) Jamming" and "Tampering" that target this layer. Moving to the network layer, it discusses "Distributed Denial of Service (DDoS)", "Man in the Middle (MIM)", "Blackhole", and "Sleep Deprivation" attacks, emphasizing the importance of detection mechanisms like JPCAP and robust authentication. In the middleware layer, the survey mentions "Unauthorized Access to the Tags" and "Malicious Insider" attacks, with a focus on access control and role-based authorization. Finally, in the application layer, "Phishing attacks" are highlighted, which aim to steal user information through deceptive methods. The research underscores the multifaceted nature of security challenges in IoT and the importance of addressing them at various architectural layers.

Another take based on S. Agarwal et al.'s perspective, their research discusses widespread adoption of Internet of Things (IoT) devices and the security risks associated with them. It introduces a novel method to detect and identify IoT devices, including their manufacturer, model, and firmware version, by analyzing web user interfaces. [2] The study emphasizes the importance of securing IoT devices, as they often lack traditional security solutions and can be vulnerable to cyber threats. It categorizes identified IoT devices and highlights potential vulnerabilities, stressing the significance of addressing security risks in large, heterogeneous networks.

The assessment involves inspecting the web interfaces of IoT devices for potential security vulnerabilities and checking for network-side vulnerabilities through port scanning. The results showed identified vulnerable devices, and vulnerabilities were categorized into groups like "Out of the box configured", "Easily vulnerable", and those prone to known exploits. Mitigation efforts involve reporting vulnerabilities to device administrators. The study emphasizes the importance of security awareness and offers tools like NetScanIoT and Web-IoT Detection (WID) for detecting and identifying IoT devices. Taking everything into consideration, the research discusses the effectiveness of the approach and plans for future work in identifying new types of IoT devices.

As per Y. Jia et al.'s research, it addresses the issue of Chaotic Device Management (Codema) in

the context of IoT devices, which can be managed through various channels, including manufacturer apps and third-party platforms like Apple's HomeKit. These channels, termed Device Management Channels (DMCs), often lack coordination in their security policies, creating vulnerabilities that malicious users can exploit. Real-world IoT devices, including locks and smart home devices, are found to be vulnerable to Codema attacks. To mitigate this threat, the paper introduces CGuard, an access control framework for cross-DMC security management. The framework is designed to enhance security, privacy, and usability in IoT systems. [7].

This study distinguishes between Manufacturer DMCs (m-DMCs) and Third-party DMCs, including HomeKit, Zigbee/Z-Wave, and Smart-speaker Seamless DMCs. Manufacturer DMCs have cloud-based, local-control, or hub-based architectures. Third-party DMCs like HomeKit enable users to control IoT devices through uniform management consoles. These DMCs have specific communication protocols and security mechanisms for device pairing and control. The research emphasizes the lack of coordination between co-located DMCs, leading to the Codema issue, where one DMC can bypass the security controls of another. The threat model considers temporary access rights and identifies Codema flaws using a model-guided approach. The Codema problem affects various mainstream IoT devices and underscores the importance of responsible disclosure to manufacturers, who have acknowledged the issues and initiated mitigation efforts.

Finally, Kim-Kwang Raymond Choo, Keke Gai, Luca Chiaraviglio and Qing Yang in their paper titled 'A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management' compiles a comprehensive list of multiple research papers that collectively underscore the paramount importance of security within the realm of IoT (Internet of Things). [8] These papers shed light on the critical nature of safeguarding IoT devices and systems in our daily lives, encompassing smart homes, wearables, industrial control systems, and autonomous vehicles. The compilation serves as a testament to the growing concerns surrounding cybersecurity in the IoT landscape and highlights the need for collaborative efforts among researchers, policymakers, and industry experts to develop robust security solutions.

B. Device chosen

As previously mentioned, our device in question for this paper is the Wiz light bulb, a Philips-manufactured and Wiz-designed product that is sold in most retail stores in the US and across the sea, it is a cheap, portable and easy to install device that does not require a central hub to work, just connection to a light socket is required, download and open Wiz mobile phone application, log in and then a user can begin an easy to follow process to connect it to your network.

Fig. 2. Wiz Light Bulb
Image Courtesy Of: bedbathandbeyond.com

C. Security analysis

Once we started analyzing the device, we immediately found out that you could just send packets to the device and change its properties without being its owner ie. as a different device in the same network, meaning it had no user authentication embedded and enabled remote access of the light.

We then analyzed the packets over the Wi-Fi connection using popular network traffic sniffing programs such as WireShark and BetterCap, we found out that when the user or victim, in this case, used their mobile phone to modify the properties of the light, a TLSv1.2 and UDP packets were being sent with every change, pondering at the many possibilities that this opened we then came up with two attacks that can take advantage of these packets,

more specifically the UDP packets, since it is not a secure protocol.

TABLE I
COMPARISON OF UDP AND TLSV1.2 PROTOCOLS

Aspect	UDP	TLSv1.2
Protocol Type	Connectionless	Connection-oriented
Reliability	Low (Unreliable)	High (Reliable)
Security	No encryption	Strong encryption
Performance	Lightweight	Overhead due to encryption
Use Cases	Real-time applications	Secure communication

III. EXPERIMENT

A. Environment

A LAN network was used to perform the tests, set up with a 2.4 Ghz band hotspot in a laptop, that is connected to the LAN2 interface, the 2.4 band is a requirement that most IoT devices have, both the mobile phone and the light bulb are connected, and another laptop device acting as the attacker, all are in the same network.

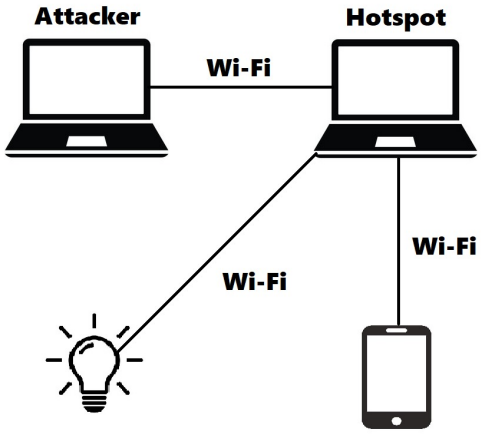

Fig. 3. Diagram of experiment setup

B. Case study

Other attacks against Wiz devices were studied closely, such as one deployed by the website LimitedResults in 2019 [9], that involved a physical exploit, requiring opening the device, resoldering some wires and dumping the firmware, they found multiple vulnerabilities in the device. Such as storing Wi-Fi credentials in plaintext in the flash memory, the firmware can be easily reflashed, as the integrity of each stage is checked by just one checksum byte or even able to see the SSID and password of the network when connecting to the device through a terminal.

Another such case was a vulnerability found by Aleksandr Rogozin in 2021 [10], that by knowing the light bulb's IP address, it was found that by sending specific JSON payloads, you could modify the lights properties, without any proper authentication. Also, he came up with a way to scan for all Wiz light bulbs in the network using a UDP broadcast packet, receiving the IP address and status of every light.

C. Overview of code

The code that was written aims to exploit a vulnerability in the TLS protocol and in the UDP protocol, for the UDP section, there are 2 files: getData.sh, which collects UDP packets by using the Netcat command every 30 seconds and saves its data on a JSON file; and dataAnalysis.py, which takes the JSON file generated from last file to transforming it into a CSV file, a type of file which will result in an easier analysis of the information. For the TLS section, there is the bulb.py file, this Python script utilizes the PyShark library to capture network traffic on a specified interface, filtering packets with a target IP address associated with a light. The code focuses on extracting and saving the payload of Transport Layer Security (TLS) packets containing encrypted application data.

Once all the data from the two sections is saved, it goes through an analysis on the ipynb file, which, alongside the graphical module pandas, shows some statistics that will be discussed in the next section of this document.

The overwall code in the end simulates two types of attacks:

- Firmware attack: The vulnerability in the light bulb's security arises from its design; it is intended to exclusively receive TLS (Transport Layer Security) packets. However, due to a lack of security measures in the firmware, UDP (User Datagram Protocol) packets are also

accepted. This oversight allows an at
to send UDP packets and retrieve ser
information, as the figure 4 shows.

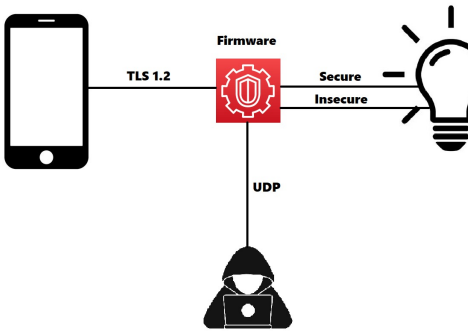

Fig. 4. Diagram of the firmware exploitation attac

- Privacy atttack: Observing traffic over the TLS protocol essentially provides insightful information when the user sends requests from the smartphone to the light bulb. This capability enables the construction of data analyses for IoT device usage, as the figure 5 shows.

D. Statistical analysis

These analyses refer to privacy and utilize gathered data. Hence, generating tangible graphs enables an attacker to reach important conclusions about an individual or family's actions. Conducted data analysis reveals confidential information:

- Light usage during the day and throughout the week indicates when the user is at home.
- The patterns of turning the light on and off may suggest when the user potentially leaves the house or goes to sleep.
- Knowing the user's favorite color discloses a personal preference.

The patterns derived from light usage not only unveil potential opportunities for burglary but also lay the groundwork for more sophisticated targeted attacks. Moreover, the knowledge of personal preferences, such as favorite color, can contribute to profiling. Therefore, that is what makes these analyses worthwhile and concerning from a privacy and security standpoint.

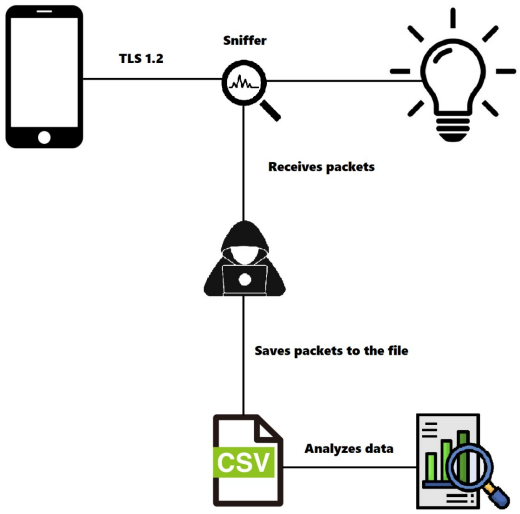

Fig. 5. Diagram of the privacy attack

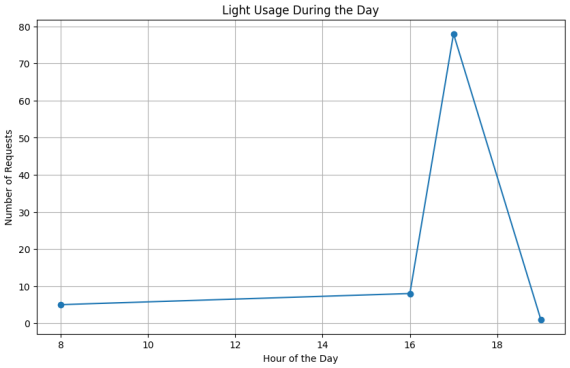

Fig. 6. Lights usage during the day

E. Influential factors

Keep in mind this attack was launched over a hotspot connection, if it were to be deployed over a real network, problems could arise with the router and its firewall, potentially stopping the recording or sending of packets through the network

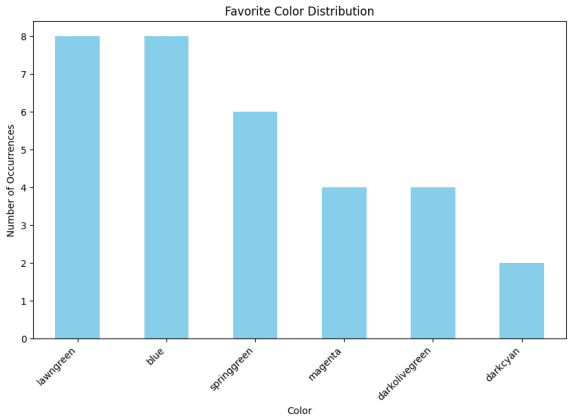

Fig. 7. Favorite color distribution

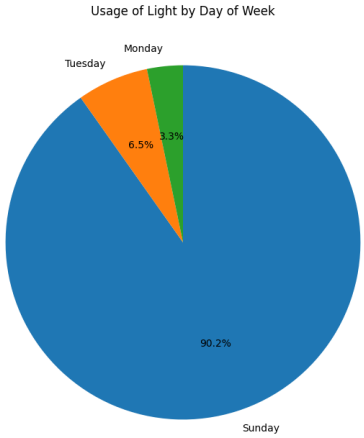

Fig. 8. Usage of light by day of the week

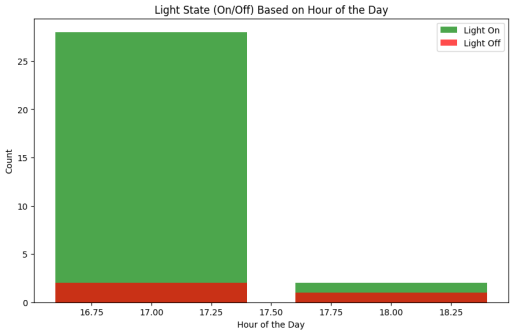

Fig. 9. State of light based on hour of the day

IV. Conclusion

We conclude that this device and its insecure protocols, can bring harm to a household or building and potentially expose the privacy of the users within them, and that not only holds for this particular device but others in the same category as well. In the grand scheme of things, this brand is arguably one of the most well-known out there in the market, leading one to wonder whether other less-known brands care enough to protect their devices.

From reading this paper, you should come to realize that the use of these devices poses a risk to the security and the privacy of the places they are put at, from previous attacks in previous years to our proposed privacy breach capability.

We recommend the use of devices that have a central hub, most of them offer a certain degree of security that is superior to those that do not, especially those like the Philips Hub that require a physical button to authorize devices into a network and have their own secure communication protocols. However, as always with enough expertise these systems can also be vulnerable, the best advice is to constantly keep devices up to date and to do the research before buying any random device from your local store or online.

We also urge manufacturers to bolster the security of their IoT devices, pay more attention to the hardware and software they produce, use secure communication protocols, and safeguard the users' privacy and ease of mind at the forefront, since the amount of these devices will only increase in the coming years we need to be cautious and start looking at ways that we can prevent incidents and potentially massive attacks.

V. Future work

As for other avenues that could further the effectiveness of our attack, there exists the possibility of using a physical device such as Raspberry Pi with some modifications that could sniff Wi-Fi networks, identifying the smart light bulbs and potentially sending the packets to a remote server, just by leaving it close to a house or building.

Another area for some improvements would be to infect the firmware as was demonstrated by

another researcher, and potentially use the light bulb to spread malware to other networks, use it to analyze the traffic of other nearby lights, and other possibilities as such.

REFERENCES

[1] Explority, "1 in 2 Companies Can't Detect IoT Device Breach; Software Testing Firms Called to Curb IoT Security Crisis," PR Newswire, Mar. 2019.

[2] S. Agarwal, P. Oser, and S. Lueders, "Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk," Sensors, vol. 19, no. 19, p. 4107, Sep. 2019, doi: 10.3390/s19194107.

[3] N. M. Allifah and I. A. Zualkernan, "Ranking Security of IoT-Based Smart Home Consumer Devices," in IEEE Access, vol. 10, pp. 18352-18369, 2022, doi: 10.1109/ACCESS.2022.3148140.

[4] M. Yu et al, "A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices," Future Internet, vol. 12, (2), pp. 27, 2020. doi: 10.3390/fi12020027.

[5] M. Ravi, "A Survey on Security Risks in Internet of Things (IoT) Environment," Journal of Computational Science and Intelligent Technologies, vol. 1, no. 2, pp. 1–8, 2020, doi: https://doi.org/10.53409/mnaa.jcsit20201201.

[6] Y. Alotaibi, A. Alrefaei, and M. Ilyas, "Security Risks in Internet of Things (IoT): A Brief Survey," Proceedings of the World Multi-Conference on Systemics, Cybernetics and Informatics, Jul. 2022, doi: https://doi.org/10.54808/wmsci2022.01.6.

[7] Y. Jia et al., "Who's In Control? On Security Risks of Disjointed IoT Device Management Channels," Nov. 2021, doi: https://doi.org/10.1145/3460120.3484592.

[8] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. Khurram Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," Computers & Security, vol. 95, p. 101871, Aug. 2020, doi: https://doi.org/10.1016/j.cose.2020.101871.

[9] LimitedResults, "Pwn the WIZ connected," LimitedResults, Feb. 06, 2019. https://limitedresults.com/2019/02/pwn-the-wiz-connected/.

[10] "Hacking Philips Wiz lights via command line," Aleksandr Rogozin, Aug. 13, 2021. https://aleksandr.rogozin.us/blog/2021/8/13/hacking-philips-wiz-lights-via-command-line (accessed Dec. 04, 2023).

[11] Priceonomics-media.com, 2023. https://pix-media.priceonomics-media.com/blog/1387/image4.png (accessed Dec. 04, 2023).