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

Daniel Alejandro Leon Ortiz, Dominykas Baronas, Jose Fredy Navarro Motta
The University of Oklahoma, School of Computer Science

Introduction

IoT 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 cyberattacks.

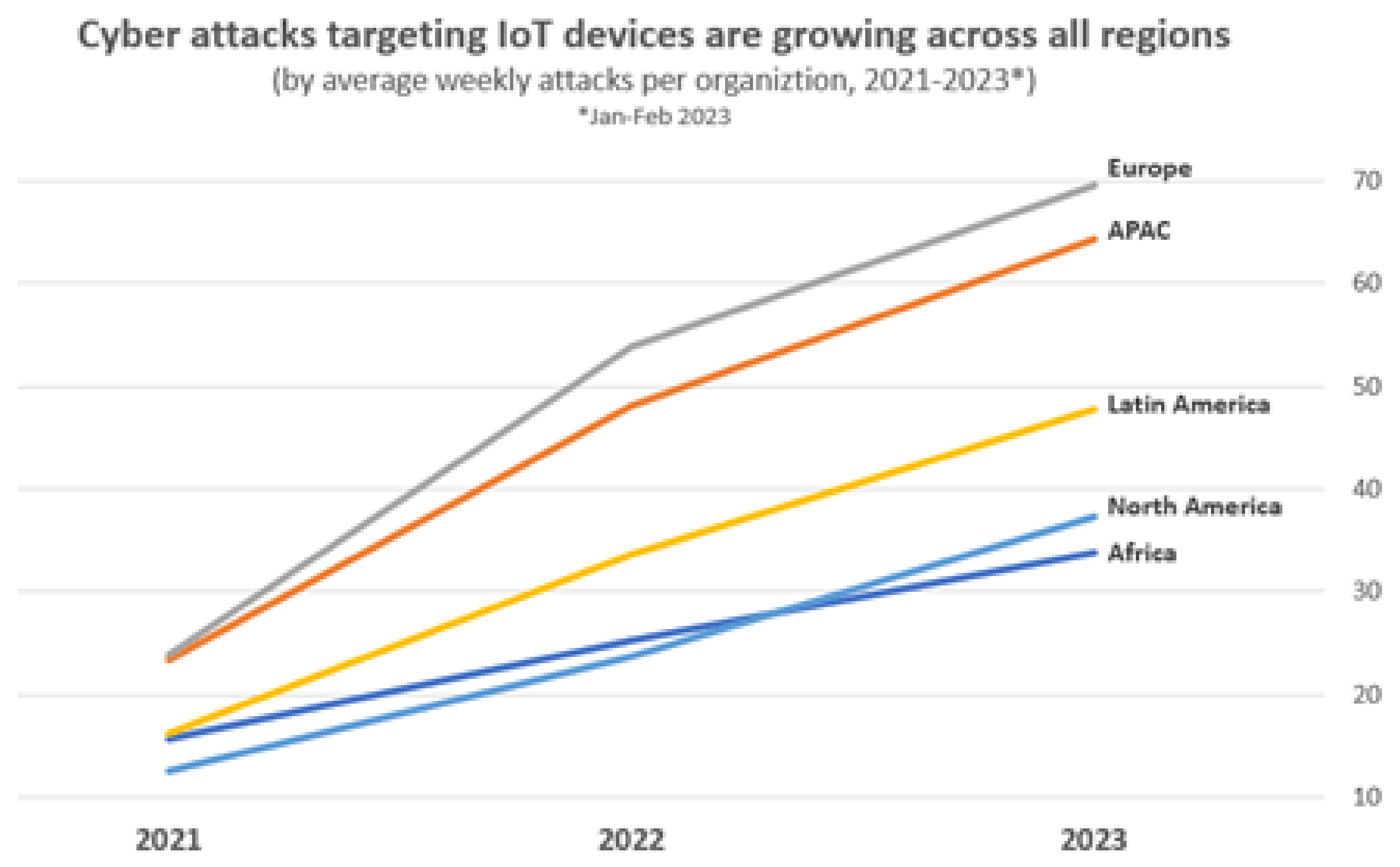

Figure 1. Attacks targeting IoT devices across all regions

Attacks performed in the project:

Firmware Exploitation Attack - inherent lack of security in firmware enables sending unauthorized requests to manipulate a device's behavior.

Privacy Attack - Implemented sniffing programs observe network traffic, gather, and analyze data about light usage, allowing for observations that compromise user’s confidentiality.

How it works

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.

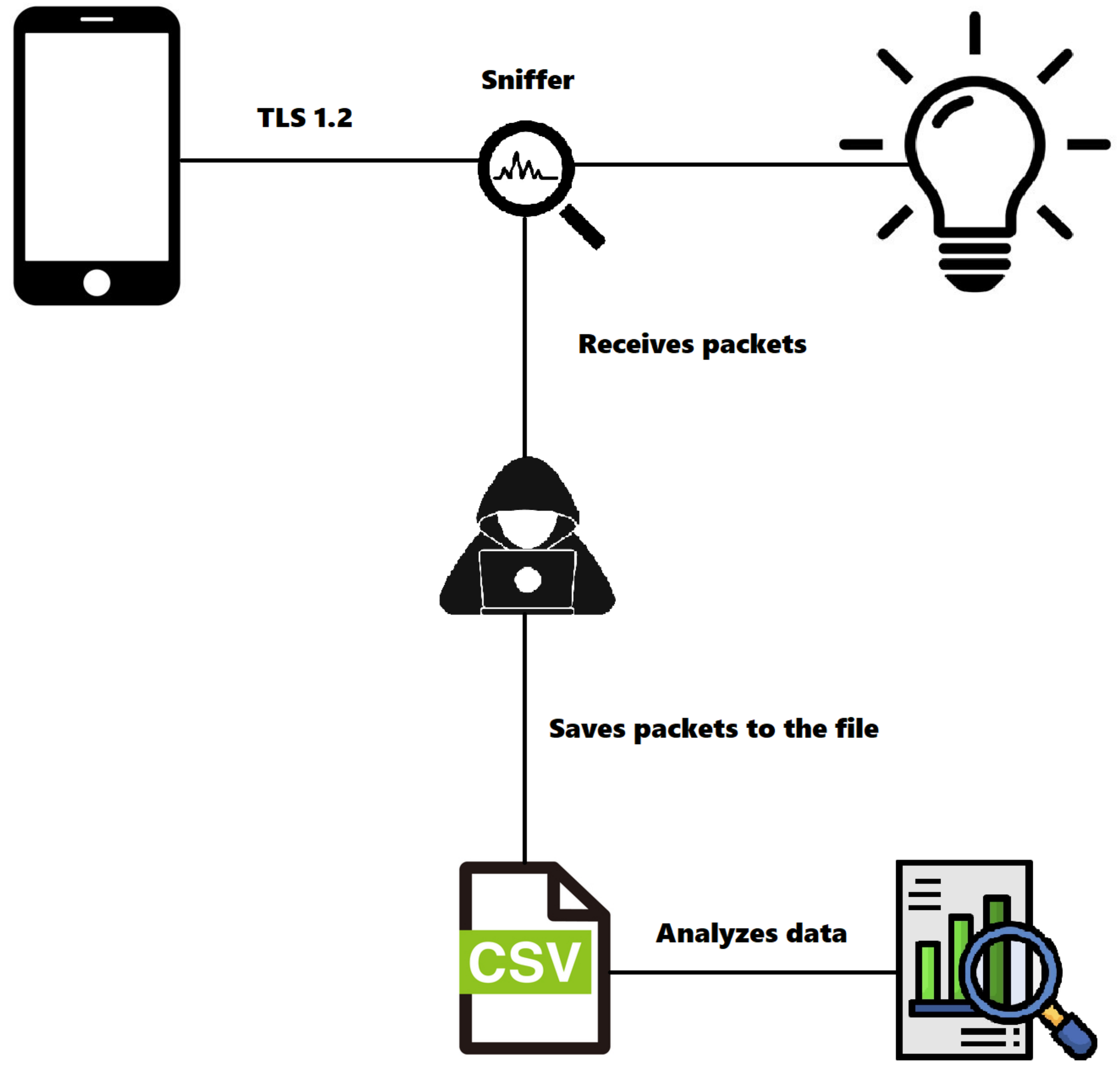

Figure 2. Privacy Attack

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 attacker to send UDP packets and retrieve sensitive information.

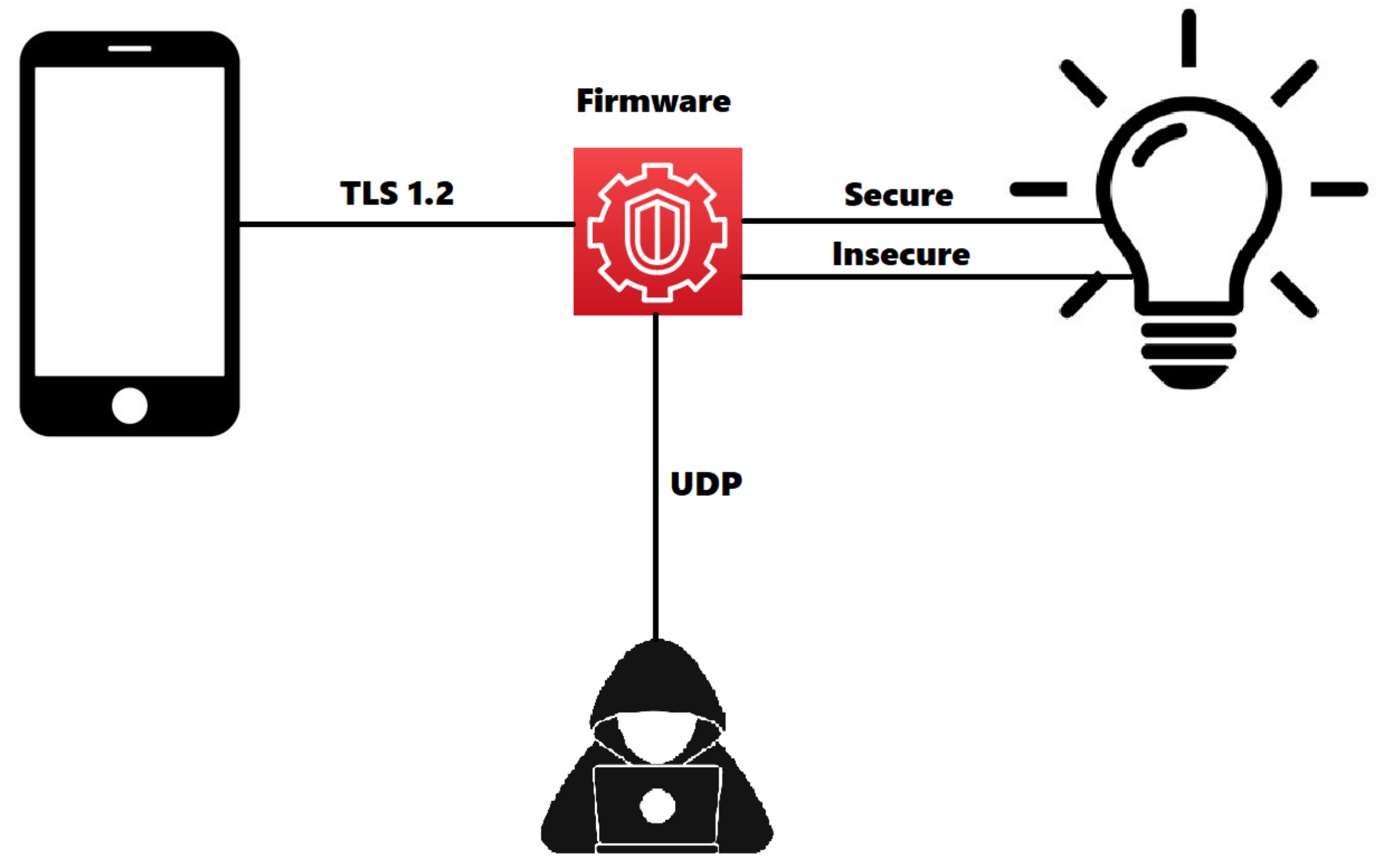

Figure 3. Firmware Exploitation Attack

Results

Through the **privacy attack**, gathered user's sensitive data is analyzed, revealing results such as their favorite color, light usage throughout the day, and patterns of light usage by the day of the week.

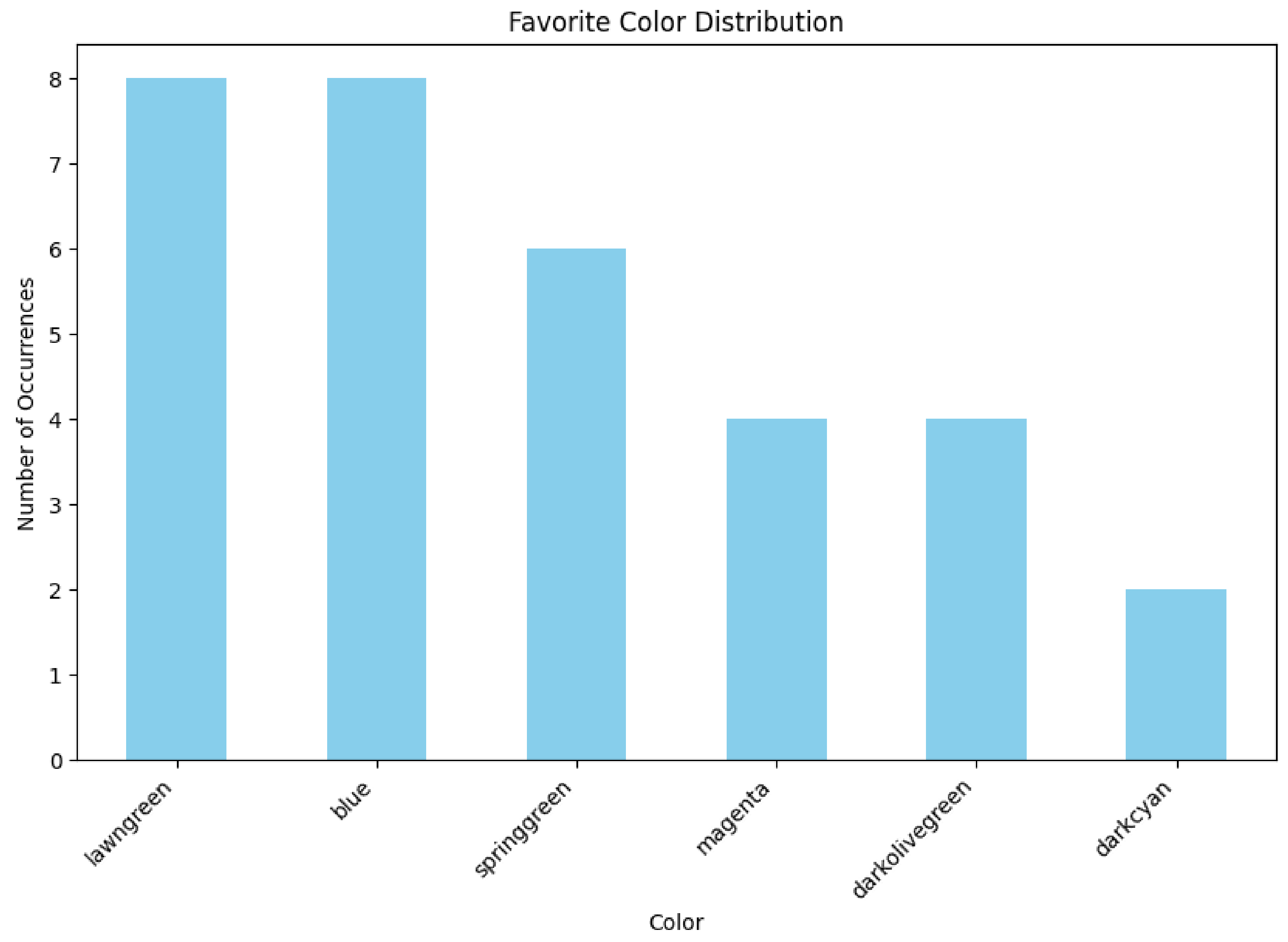

Figure 4. Favorite Color distribution

Contact

The University of Oklahoma, School of Computer Science
Email: Daniel.A.Leon.Ortiz-1@ou.edu Dominykas.Baronas-1@ou.edu Jose.Fredy.Navarro.Motta-1@ou.edu
Phone: +14052748825

References

1. etal, “The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally,” *Check Point Blog*, Apr. 11, 2023. https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/
2. R. O. Andrade, S. G. Yoo, I. Ortiz-Garces, and J. Barriga, “Security Risk Analysis in IoT Systems through Factor Identification over IoT Devices,” Applied Sciences, vol. 12, no. 6, p. 2976, Mar. 2022, doi: 10.3390/app12062976.
3. 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.
4. 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.