JoJo Petersky

CPE 400.4001

August 14th, 2024

## Final Project Report: Network Traffic Analysis

## of Feit Electric BPA800/RGBW/2 Smart Bulb

**Project Overview**

**Objective:** This project aimed to analyze the network traffic of the Feit Electric BPA800/RGBW/2 smart bulb to identify the protocols used in its communication and determine whether the data was encrypted or sent in plaintext.

**Motivation:** With the increasing integration of IoT devices in homes, ensuring the security and integrity of their communications is crucial. This project sought to understand the nature of the smart bulb's communication with its controlling device, focusing on protocol identification, encryption status, and potential security vulnerabilities.

**Results and Detailed Analysis**

**A screenshot of a computer screen

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Traffic and Protocol Analysis:** Two main protocols were identified during the analysis of the smart bulb's communication:

1. **Google Cast Protocol:**
   * **Instances Identified:** 120
   * **Significance:** The presence of Google Cast protocol traffic indicates that the smart bulb might support or interface with Google Cast technology, which could involve media streaming, device control, or integration with other Google-enabled devices.
   * **Payload Observations:** The payloads often began with \x17\x03\x03, a sequence typically associated with TLS/SSL encryption handshakes. This suggests that even within the Google Cast protocol, some communications might be encrypted.
2. **Custom Protocol:**
   * **Instances Identified:** 119
   * **Significance:** The Custom Protocol appears to be a proprietary communication method used by the smart bulb. The nearly equal distribution between this protocol and Google Cast indicates that it plays a critical role in the bulb's operations.
   * **Payload Observations:** Similar to Google Cast, the Custom Protocol also showed payloads beginning with \x17\x03\x03, implying potential encryption or secure communication practices.

**Payload Content Review:**

* **Unique Payloads:** The most common payload was \x17\x03\x03, a marker often seen in encrypted communication. This suggests that while the protocols are identifiable, the data within them might be protected or encoded, limiting the ability to easily interpret the exact nature of the commands or information being exchanged.
* **Command Markers:** No explicit command or status markers were found within the payloads, indicating that if commands or statuses are communicated, they might be encoded or represented in a different format, possibly proprietary to the device.

**Cross-Comparison Between Packet Captures:**

* Both packet captures showed consistent use of the Google Cast and Custom Protocols, with similar payload patterns across the captured traffic. This consistency suggests stable communication practices by the smart bulb, potentially pointing to routine operations or regular updates.

**Conclusion**

**Consistency with Expectations:**

* The results aligned with initial expectations, confirming the use of encrypted communication protocols for some parts of the smart bulb's data transmission. The presence of proprietary communication methods highlights the device's reliance on custom protocols, which are common in IoT devices.

**Implications for Security and Interoperability:**

* The identification of Google Cast integration raises questions about the smart bulb's potential interoperability with other Google-enabled devices. This could enhance its utility in a smart home setup but also introduces additional security considerations, particularly around the encryption and privacy of the data transmitted via this protocol.

**Future Research:**

* **Deeper Analysis of the Custom Protocol:** A detailed reverse engineering effort could shed light on the exact nature of the Custom Protocol, its structure, and the type of data being communicated.
* **Exploration of Google Cast Capabilities:** Investigating the specific uses of Google Cast by the smart bulb could provide insights into its broader functionalities and potential vulnerabilities.
* **Encryption Investigation:** Efforts could be made to decrypt the TLS/SSL traffic to fully understand the underlying data, which might reveal more about the device's operations and any associated risks.

**Key Learnings:**

* This project underscored the importance of understanding the specific communication protocols used by IoT devices, particularly when considering their role in a broader smart home environment. The findings highlight both the potential benefits and the security challenges posed by the integration of proprietary and standard protocols.