Security Assessment of a Feit Electric Smart Bulb Built on the Tuya Platform-Via pen test

Team Members – Kanipakam Vijay Prathap Reddy, Sai Spandana, Mark mutua

1. Introduction

The rapid adoption of smart home devices has led to widespread integration of Internet of Things (IoT) technologies. However, security in many of these devices has not evolved at the same pace. This project focuses on a security assessment of a Feit Electric Smart Bulb, which uses the Tuya IoT platform — a widely adopted backend for many rebranded smart devices. Our objective was to analyze the device's communication behavior, identify exposed ports, evaluate data encryption, and check for potential vulnerabilities.

2. Background: The Tuya IoT Platform

Tuya is a global IoT solution provider offering firmware, cloud services, and mobile app platforms to OEM brands. Devices from Feit, Gosund, and Teckin often used Tuya's backend infrastructure.

Tuya's architecture typically includes:

- Device firmware (e.g., ESP8266 or BK7231 chips)
- Tuya Cloud services
- Mobile apps (white-labeled or Tuya Smart Life)
- Communication over UDP port 6667 for device pairing
- TCP port 6668 for encrypted cloud control

Older Tuya implementations were criticized for insecure design practices such as:

- Plaintext Wi-Fi credentials being sent in EZ Mode
- Hardcoded or shared encryption keys
- Exposed local admin interfaces

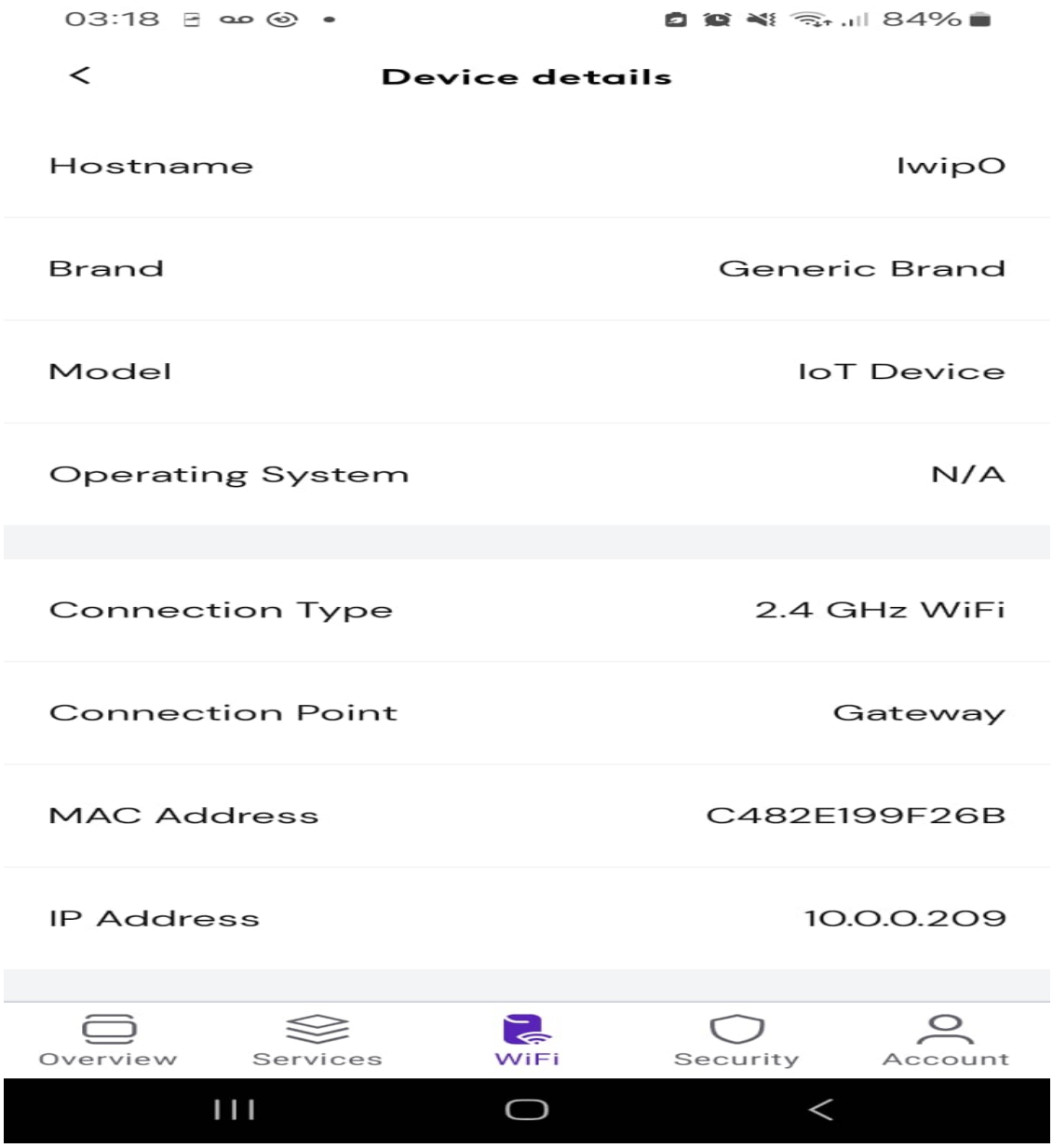
Modern Tuya systems now include improvements such as:

- TLS 1.2+ encryption
- Device-specific onboarding keys
- No exposed local access points

3. Methodology

3.1 Reconnaissance

The bulb was connected to a 2.4GHz Wi-Fi network. Its IP address (10.0.0.209) and MAC address (C4:82: E1) were identified using the router interface.



IP and MAC Discovery from Router Interface]

3.2 Scanning

Network scanning was performed using the following command:

sudo nmap -sV -O 10.0.0.209

Only TCP port 6668 was found open. No local interfaces such as HTTP, SSH, or Telnet were detected.

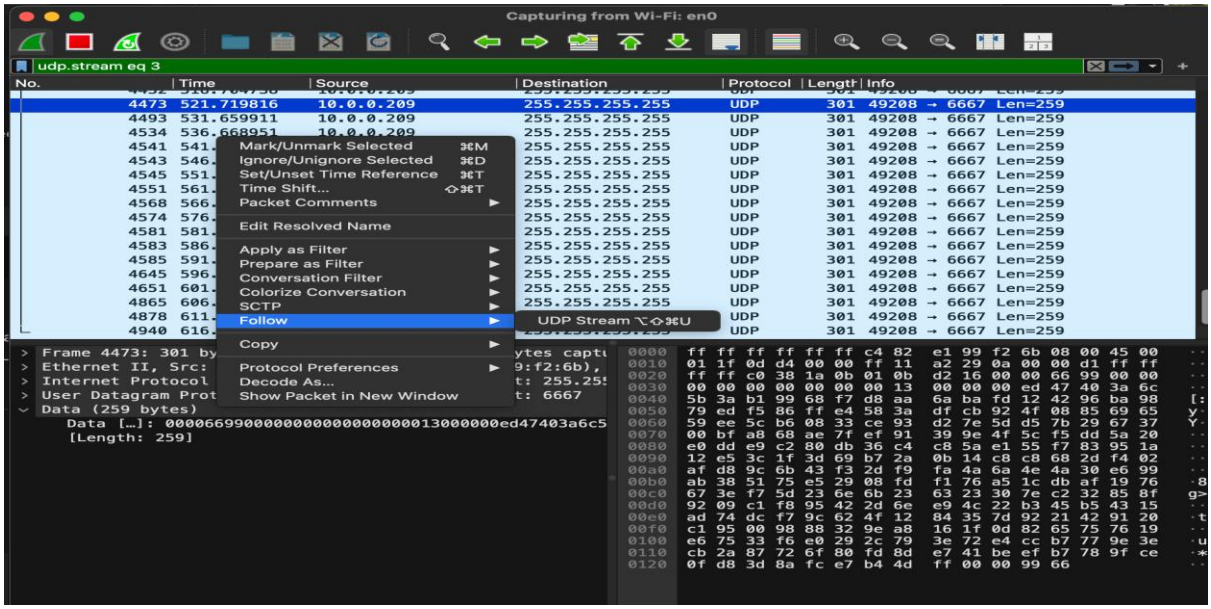
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 02:22 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.0.0.209
Host is up (0.090s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
6668/tcp open  irc?
MAC Address: C4:82:E1:99:F2:6B (Tuya Smart)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=4/11%OT=6668%CT=1%CU=41552%PV=Y%DS=1%DC=D%G=Y%M=C482E1
OS:%TM=67F8B77B%P=x86_64-apple-darwin23.6.0)SEQ(SP=51%GCD=1%ISR=7F%TI=I%CI=
OS:I%II=RI%SS=O%TS=U)SEQ(SP=53%GCD=1%ISR=7F%TI=I%CI=I%TS=U)SEQ(SP=55%GCD=1%
OS:ISR=7F%TI=I%CI=I%II=RI%SS=O%TS=U)SEQ(SP=57%GCD=1%ISR=7F%TI=I%CI=I%II=RI%
OS:SS=O%TS=U)SEQ(SP=58%GCD=1%ISR=7F%TI=I%CI=I%II=RI%SS=O%TS=U)OPS(O1=M5B4%O
OS:2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=1C84%W2=1C84%W3=1C84%W4=1C
OS:84%W5=1C84%W6=1C84)ECN(R=Y%DF=N%T=FF%W=1C84%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%T
OS:=FF%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=N%T=FF%W=1C84%S=O%A=S+%F=AS%O
OS:=M5B4%RD=0%Q=)T4(R=Y%DF=N%T=FF%W=841C%S=A%A=S%F=AR%O=%RD=0%Q=)T5(R=Y%DF=
OS:N%T=FF%W=841C%S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=FF%W=841C%S=A%A=S%F
OS:=AR%O=%RD=0%Q=)T7(R=Y%DF=N%T=FF%W=841C%S=A%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
OS:F=N%T=FF%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=FF
OS:%CD=S)

Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 614.05 seconds
mk@MKs-MacBook-Pro Desktop %
```

Nmap Scan Results

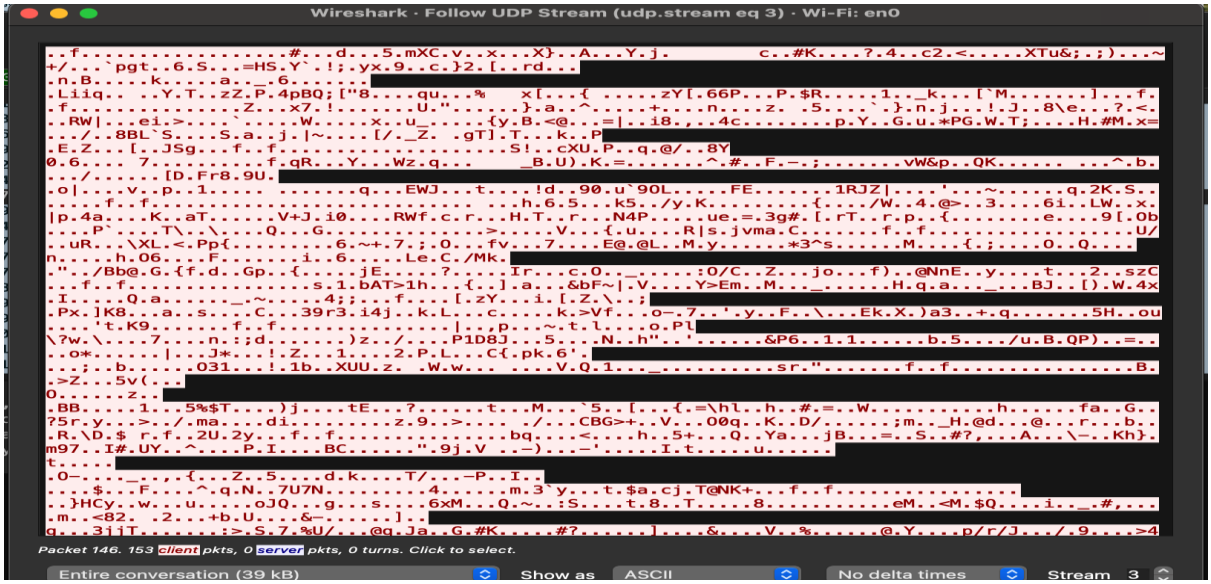
3.3 Traffic Analysis

Wireshark was used to capture traffic between the bulb and the app during initial pairing and operation. It revealed:

- UDP port 6667 was used during the pairing phase
- Packet contents appeared encrypted or obfuscated
- TCP 6668 was not captured directly, but its use for secure cloud communication is confirmed by Tuya documentation



Wireshark Capture – UDP 6667 Pairing Traffic



Wireshark Capture – Encrypted TLS

3.4 Device Identification

The Feit Electric mobile app was used to control the bulb. The app interface and behavior closely resemble that of Tuya's official "Smart Life" app, confirming the underlying platform.

Feit Electric App Interface

4. Findings

- Tuya platform confirmed via MAC vendor lookup and communication behavior
- UDP port 6667 used for initial pairing
- Only TCP port 6668 open — consistent with Tuya's cloud control protocol
- No local services (HTTP, SSH, Telnet) were exposed
- Communication was encrypted or obfuscated
- Bulb follows a cloud-only control model

5. Comparative Review of Tuya Security

Legacy Issues:

- Wi-Fi credentials were transmitted in plaintext during pairing using EZ Mode
- Devices often relied on hardcoded or shared encryption keys
- Many exposed local admin services such as HTTP, SSH, and Telnet
- LAN-based spoofing and unauthorized access were possible due to poor traffic validation

Current Observations (Tested Device):

- No plaintext credentials were observed during pairing; traffic appeared encrypted or obfuscated
- Communication was found to be encrypted, likely using device-specific keys and TLS
- No local services were exposed — only TCP port 6668 was open for secure cloud control
- All traffic was routed through the Tuya cloud, reducing LAN spoofing risk

6. Recommendations

For Vendors:

- Fully remove legacy EZ Mode pairing methods
- Provide secure LAN fallback control options
- Adopt periodic security audits and update policies

For Users:

- Use guest networks or VLANs to isolate IoT devices
- Keep firmware updated through the official app
- Avoid using public Wi-Fi for controlling smart devices

7. Conclusion

The Feit Electric smart bulb appears to follow a secure-by-default design. Communication is encrypted, no local ports are exposed, and the device functions through Tuya's cloud infrastructure only. This demonstrates improvement over older Tuya-based devices which suffered from plaintext pairing and exposed interfaces.

Although this device showed no vulnerabilities during assessment, best practices should always be followed by both users and vendors to mitigate evolving risks in the IoT landscape.

8. References

- Tuya Smart. Tuya IoT Developer Guide. https://developer.tuya.com
- Nmap Project. https://nmap.org
- OWASP IoT Project. https://owasp.org/www-project-internet-of-things
- Fernandes et al. (2016). *Security Evaluation of Smart Home Apps*. IEEE
- Ronen & Shamir (2016). *ZigBee Attacks in IoT Devices*. USENIX
- NISTIR 8259 (2020). *Basic Cybersecurity Features for IoT De*