LIMITED RESULTS
OCT. 2018
Pwned by

Don’t toss your lightbulbs

LimitedResults
16th of March 2019
BSIDES Ljubljana

Summary

- Introduction
  - About me
  - Hardware Hacking
  - The IoT security context
- Security review
  - Why to hack lightbulbs?
  - Threats modeling 101 & 102
- The results
  - Inside a Wi-Fi lightbulb
  - Xiaomi Yeelight
  - LIFX Mini
  - WIZ and Tuya
- Discussions
  - IoT Experience
  - Conclusion

Booting

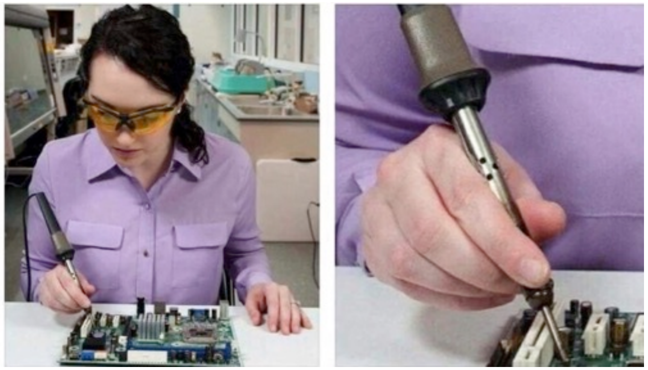
INTRODUCTION

UID – about me

- LimitedResults
  - Focus on **Results**
    - Recent diversification to IoT
  - I am **Limited** ☺
    - By the time, the $, my skills sometimes…
  - www.LimitedResults.com
- I like to
  - focus on hardware
  - attack real products
  - stay low-cost
- Opinions are my own

Hardware Hacking

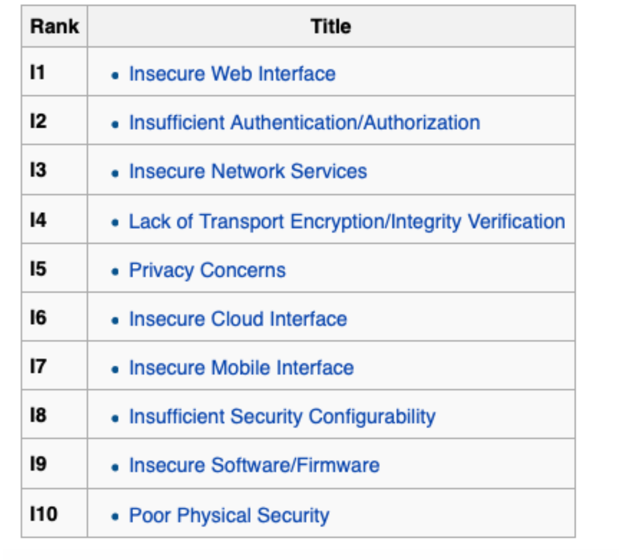
- Mistaken beliefs
  - You need Physical access!
    - Yes but depends on the attack scenario…
    - And reverse begins by physical access
  - It’s expensive!
    - 500-1000$ to start
    - Is it such a big security barrier?
- True facts about HW Vulns
  - Difficult to patch
  - Affect full range of products
  - Sometimes trivial
- So buy an iron solder!
  - Be careful, it is hot



The security context in IoT

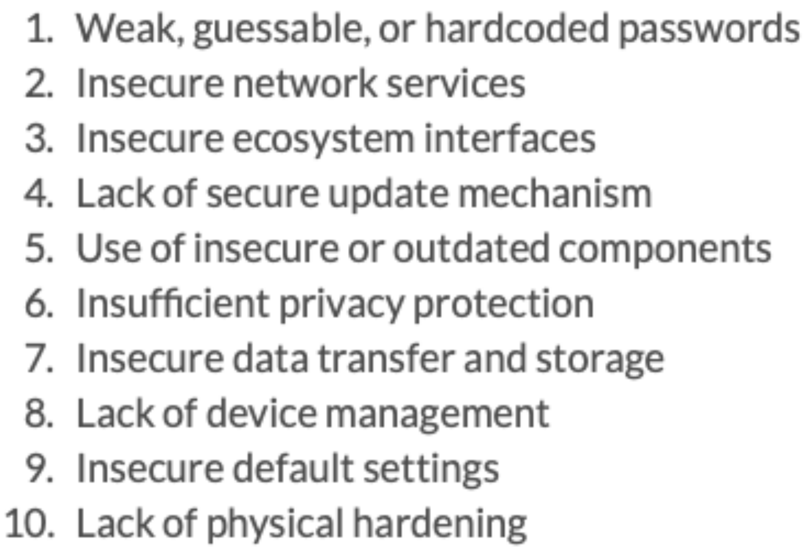
- Top 10 IoT Vulns are the same since 5 years
  - https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

2014



Rank	Title
I1	• Insecure Web Interface
I2	• Insufficient Authentication/Authorization
I3	• Insecure Network Services
I4	• Lack of Transport Encryption/Integrity Verification
I5	• Privacy Concerns
I6	• Insecure Cloud Interface
I7	• Insecure Mobile Interface
I8	• Insufficient Security Configurability
I9	• Insecure Software/Firmware
I10	• Poor Physical Security

2018



1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

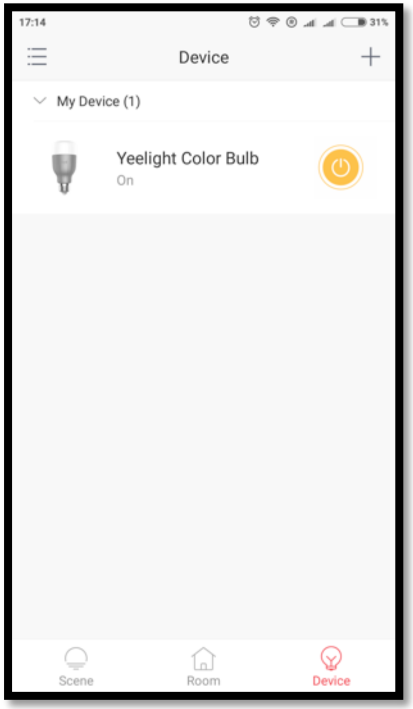
  - It is a terrible statement but it is the reality
  - Don’t worry, that will continue…

Still booting

SECURITY REVIEW

Why hacking Lightbulbs?!?

- There are lightbulbs…and lightbulbs
  - BLE
  - BLE/Wi-Fi through an hub
  - **Wi-Fi. This talk is about Wi-Fi bulbs**
- Wi-Fi bulbs:
  - Popular
  - Cheap like 20-40
  - You receive one for Christmas, house-warming… such a little sneaky device!
- Setup is easy
- If vulns are present, people understand what's going wrong
  - Not only security experts



Yeelight Color Bulb
On

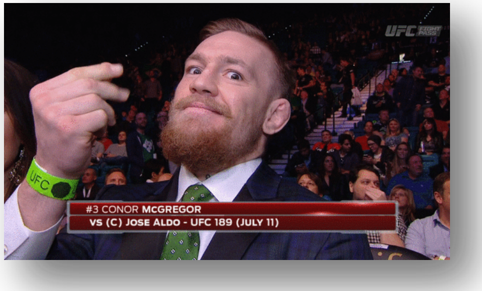
Yeelight on android

Threats modeling 101

- What are the critical assets ~~to protect~~ to hack?
  - User account
    - Lifx account, Xiaomi account…
  - Authentication key, device ID for the Cloud Access
    - Used for Onboarding, MQTT protocol…
  - User Data
    - Private Data, GDPR ☺…
  - Wi-Fi credentials
    - SSID and WPA2 key
- Main threats
  - Control other people’s lamps
    - Access to Users accounts or to Cloud authentication keys
  - Retrieve Data, Cloud database
    - Spying neighbors or Famous people perhaps? Big leak of accounts…
  - Access the User Network
    - Wi-Fi credentials
- Three axis of investigations
  - The mobile App, the Cloud and the Device

Threats modeling 102

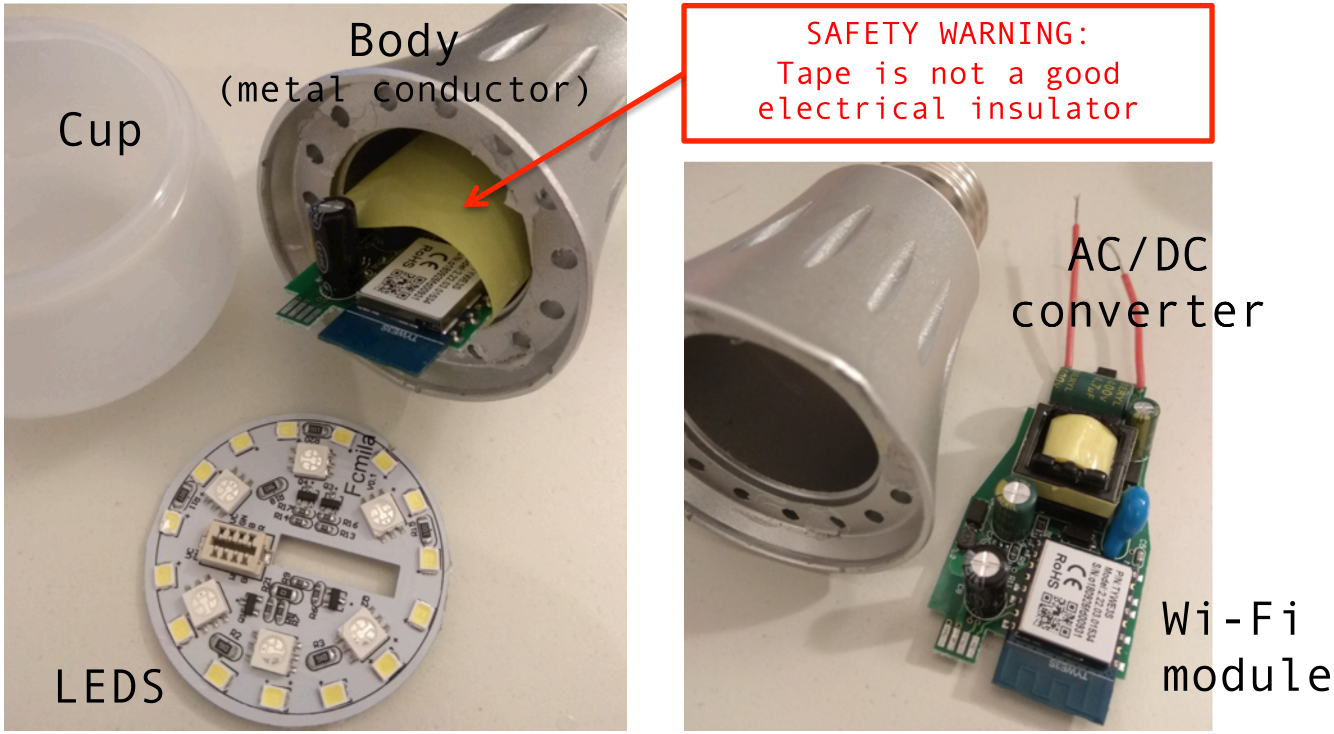
- I decide to focus on the device(Hw+Fw)
- The Product Life Cycle?
  - Development > Production > On the Field > **Garbage**
- New threat is Attacking from/Into the Garbage
  - Physical access? Not a problem here
    - Contact inside waste recycling companies
    - Buy second hand devices
    - Just steal devices
  - Imagine how much devices you can get...
    - How much SSID and passwords you can get…
- The vendor threat model doesn’t think about the product’s end of life.
  - Physical access rated as ‘**Out of Scope**’.
  - I rate that as **an ‘opportunity’**
  - Wi-Fi Light bulbs have a design weakness
    - The Wi-Fi credentials are inside the end-node device



Running now

THE RESULTS

Inside a random Wi-Fi lightbulb



SAFETY WARNING:
Tape is not a good electrical insulator

Teardown of a (random) bulb, 10 euros on Aliexpress

- Focus on the Wi-Fi module
  - The brain of the device

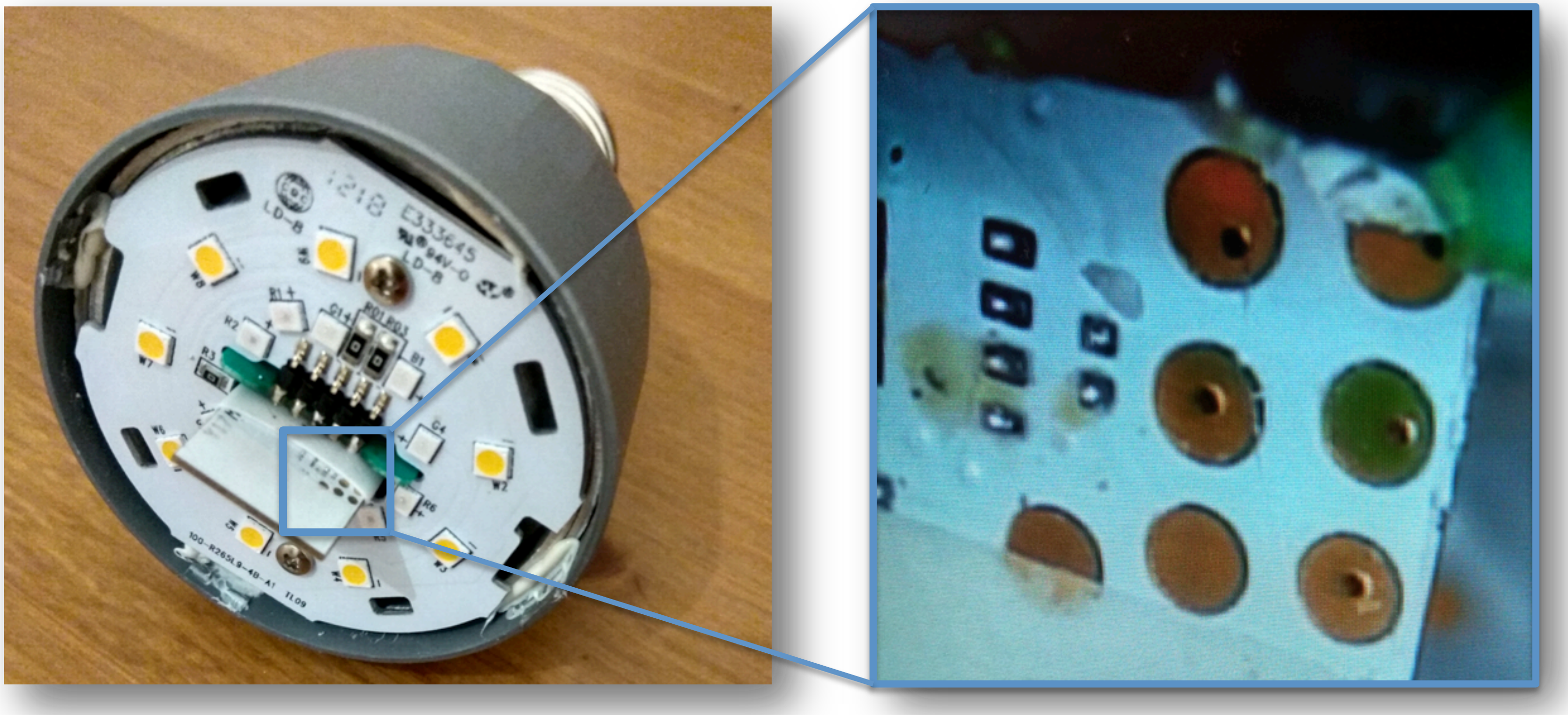
Xiaomi

- The ‘*super*’ IoT company
  - They sell everything
    - Mobile phones, toothbrush, e-bikes…
  - They have a big Cloud
    - Yes, really big…
  - A golden mine of devices…and vulns
    - But no Bug Bounty

- Focus on the Xiaomi Yeelight
  - 20 euros on Amazon

Pwn the Xiaomi Yeelight

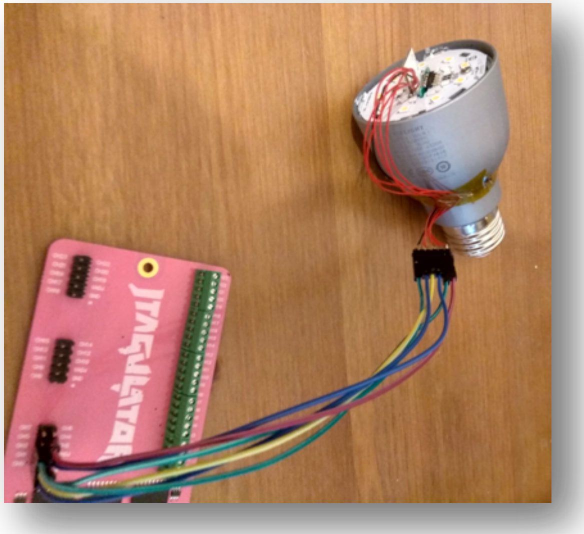
- Once the device is configured, the cup is removed:



- Flying probes used during the production
  - Five marked tests points, coincidence?

The Xiaomi setup

- Identify the debug interface
  - JTAGulator
    - **Marvell 88mw300**
  - JTAG = TMS, TCK, TDI, TDO and RST
- Connect these pins to
  - Debug probe (FT232H board or Segger)
  - Run OpenOCD + mw300 config
    - *config is on the website*
- Full access to memory, regs, PC…
  - Make it dance like a puppet

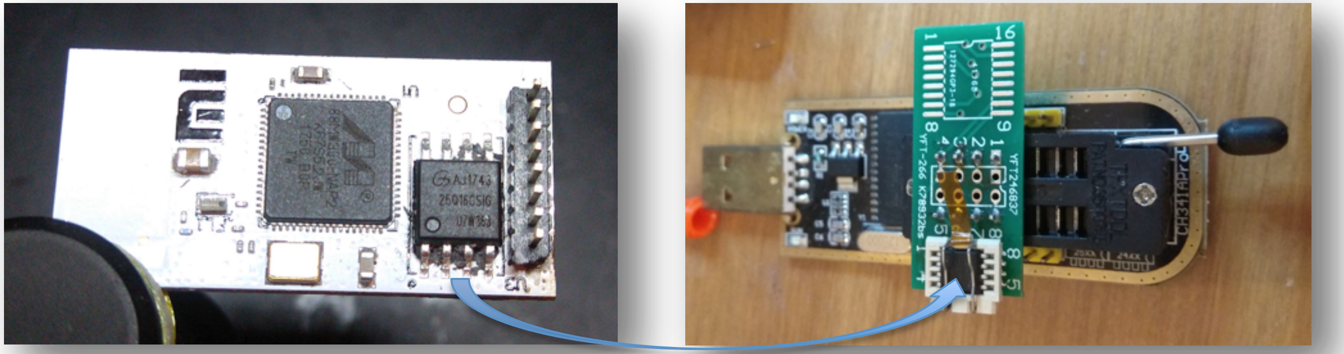


The Results

- JTAG not disabled
  - Firmware extracted
    - Wi-Fi credentials in Plaintext
  - Full control of the Marvell mw300
    - R/W, code exec
    - Make easier the reverse
  - Possibility to flash the device to insert persistent backdoor
    - Supply chain attack
- Low cost attack
  - Less than 150$, one hour, no skills
  - Device still OK, can be sold/reused

Cheaper attack?

- No JTAG probe? or even JTAG disabled?
  - Not a problem, let's dump the SPI flash
    - CH341a usb programmer + Flashrom

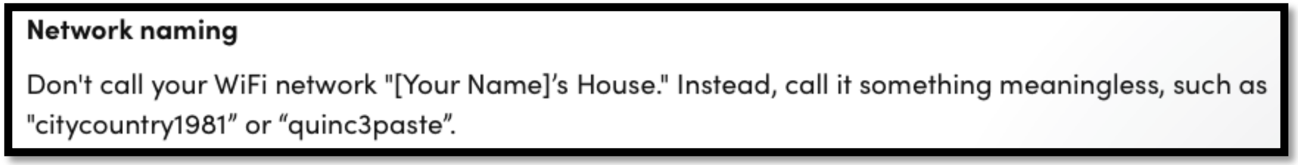


Unsolder the SPI flash to read it directly

- Cheapest attack
  - Less than 10$, one hour, no skills
  - You got the firmware now with the credentials
- Marvell 88mw300… nice target by the way ☺

LIFX

- IoT Light Company
  - Already hacked in the past
  - Now they have a real security policy
    - https://www.lifx.com/pages/keeping-your-devices-and-yourself-secure



Network naming

Don't call your WiFi network "[Your Name]'s House." Instead, call it something meaningless, such as "citycountry1981" or "quinc3paste".

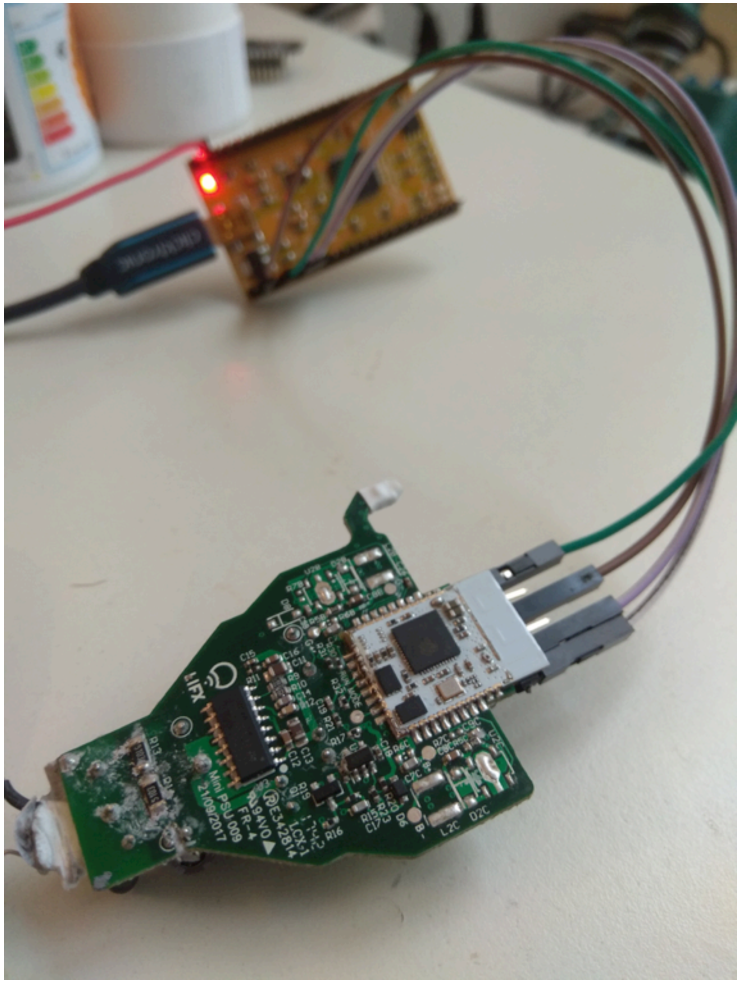
Are you Serious?

- Focus on the LIFX Mini
  - 30$ on Amazon
    - Discount! 15$ now

Pwn the LIFX like a butcher

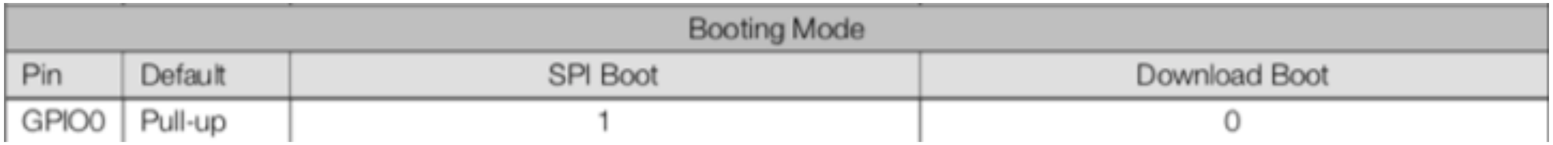
- Access the PCB
  - Saw and Vice

- Reverse the PCB
  - ESP32
- **Prepare a little setup**



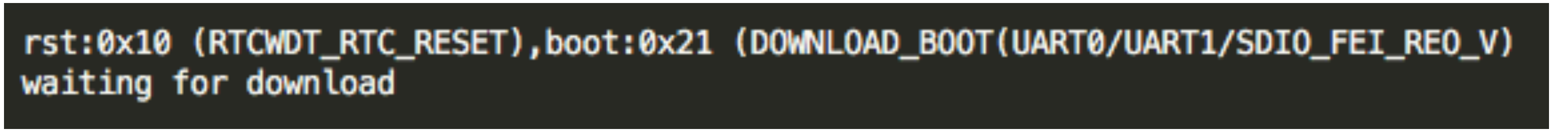
Pwn the LIFX like a butcher

- Plug a FT232H board
  - Only 4 wires to solder
  - Io0 grounded + PowerON to access download boot



Booting Mode			
Pin	Default	SPI Boot	Download Boot
GPIO0	Pull-up	1	0

ESP-32 Datasheet



```
rst:0x10 (RTCWDT_RTC_RESET),boot:0x21 (DOWNLOAD_BOOT(UART0/UART1/SDIO_FEI_REO_V)
waiting for download
```

Device serial output, it is still alive!

- Extract the firmware
  - https://github.com/espressif/esptool
  - *esptool.py -p /dev/ttyUSB0 -b 460800 read_flash 0 0x200000 flash.bin*
- Reverse and Profit!

The Results

- Main issues
    - Wi-Fi credentials in Plaintext
    - Unsecure configuration
    - RSA private key in Plaintext (onboarding)
- The REAL issues
    - Serial Bootloader cannot be disabled in ESP32
        - Offer an easy access to the FW (always)
    - ESP32 has interesting (not used) security features
        - Secure boot and Flash encryption
- Low cost attack
    - 25$, 30min, no skills
    - Device is destroyed. OK, who cares?

LIFX Mitigations

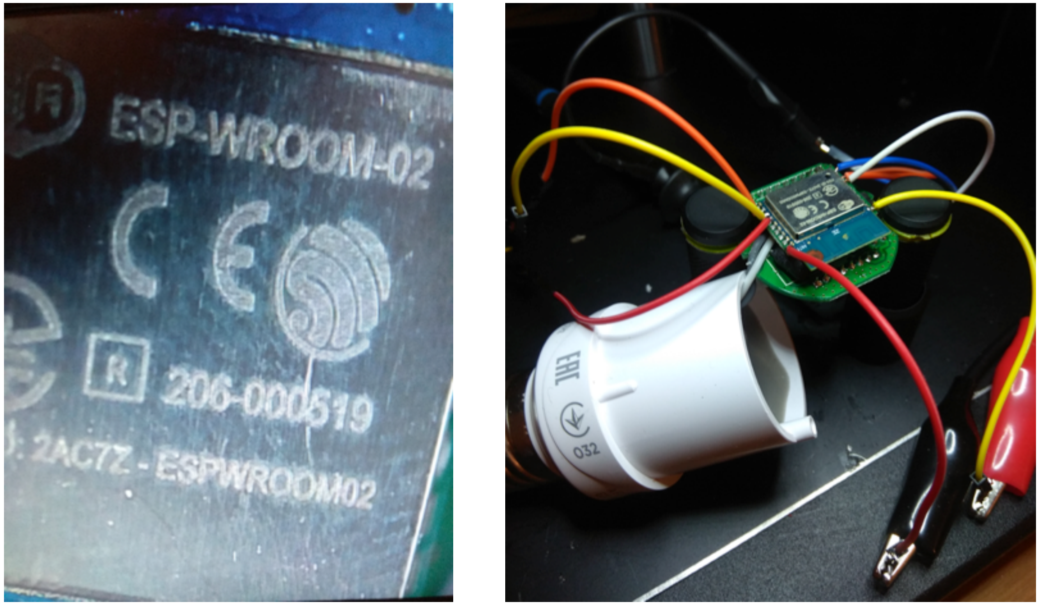
- Communication with LIFX was ~~difficult~~ limited
  - https://www.lifx.com/pages/privacy-security
- LIFX mitigations
  - Encryption of the sensitive data!
  - New security settings!
  - RSA private key encrypted too!

- Is it SECURE now?
  - The firmware v3.42 has been extracted
    - Access to the serial download still active
      - Bootrom feature, good luck to patch it
    - Still possible to dump the Flash memory directly
  - The firmware v3.42 has been reversed
    - LIFX custom Encryption is ~~bad…~~ broken
    - Ugly patch, sorry

- More **results** to come…

WIZconnected & Tuya

- Based on ESP8266



ESP-WROOM-02 embedded in WIZ devices (a little bit modified)

- Easy hack without damaging anything
- ESP8266 has no HW protection
- SDK doesn’t support encryption/obfuscation of sensitive data
- Same vulnerabilities in these products
  - The vendors do not want patch, enjoy!

Power Off

DISCUSSIONS

Back to Basics

- Basic rules (To apply to all IoT devices)
  - Network Segregation
    - Create an AP dedicated to IoT devices
  - Renew Passwords & apply Updates
    - No comment (I am lazy to do that…)
  - Think about the data you share
    - A bulb knows when you are at home, when you go to sleep…
      - Pretty scary, isn’t it?

- Medias, companies, schools should educate how to deal with connected objects
- Warning Labels on package/website such as
    - *“No security inside”*
    - *“This product will share/store your private data”*
    - *“This product must not be installed on your private network”*

IoT Experience

- (Most of) IoT vendors do not care about security
  - Priority to dev. costs & time to market
- Bug reports are often “complicated” or even impossible
  - No security contact
  - Security researchers considered as troublemakers
  - Responsible disclosure just used as ‘damage control’
    - By the way, resp. disclosure is not mandatory!
  - Need to use medias as leverage
- IoT vendors should learn from mobile phone industry
  - Bug bounties, mutual respect, continuous efforts to fix bugs…

Conclusion

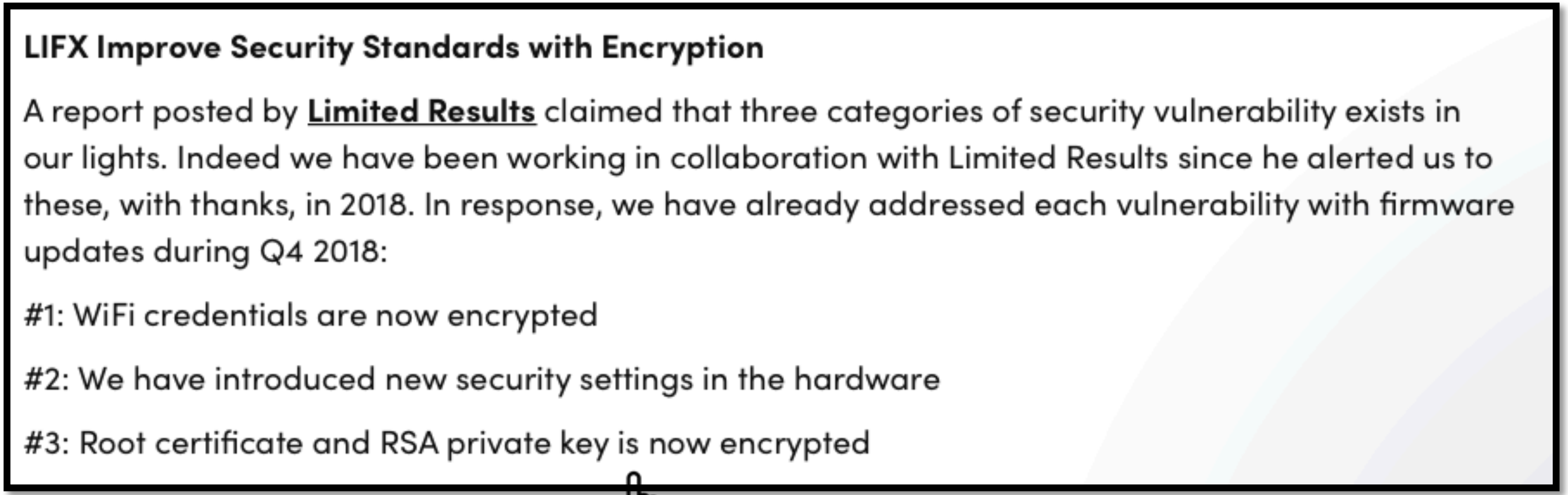
- Hardware Hacking is pretty efficient to find vulnerabilities
- IoT ecosystem needs
  - A FULL secure Product Life Cycle
  - Regulations/Sanctions for 0-security Vendors
  - Security ratings, certifications
  - Stop to consider security guys/girls as a threat
  - Hire security engineers
  - Develop an internal security policy
- The customers have to be informed/ educated
  - Then people can make their choice
  - Who really needs connected light bulbs? :-/

Thank you!

- More details? www.limitedresults.com
- Questions?

The limited game

- Here is the LIFX official statement.
- Find the little ‘bug’ inside ☺



LIFX Improve Security Standards with Encryption

A report posted by **Limited Results** claimed that three categories of security vulnerability exists in our lights. Indeed we have been working in collaboration with Limited Results since he alerted us to these, with thanks, in 2018. In response, we have already addressed each vulnerability with firmware updates during Q4 2018:

#1: WiFi credentials are now encrypted

#2: We have introduced new security settings in the hardware

#3: Root certificate and RSA private key is now encrypted

- Congrats! You win a lightbulb