# ON ESP32: TIME TO RELEASE HW EXPLOITS

LimitedResults ZeroNights 2019 12-13 November, St. Petersburg

> • Limited • By Time, \$\$\$, Skills too... • Results • www.LimitedResults.com • Offensive Side • Focus on HW, Low-Level Vulns... • No Affiliation • Time to play!

### \$ whoami



### POWER ON INTRODUCTION

ZERONIGHTS.ORG

### The Entry Point

- Last April, I decide to break investigate into the ESP32
  - System-on-Chip (SoC) released in 2016 by Espressif
  - Widely-deployed (> 100M of devices) [1]
  - Wireless MCU/SoC Market leader
  - Claim to have 'State-of-the-Art' Security
  - 12 years-longevity commitment
- General Use
  - IoT
  - Wireless peripheral

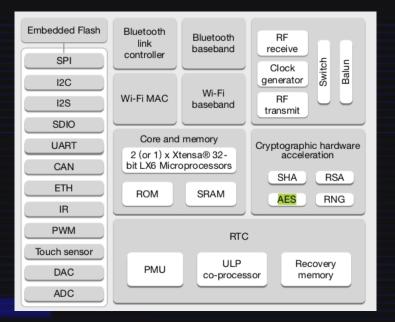
#### • ESP32

- Techno 40nm node
- QFN 6\*6, 48 pins
- Overview
  - Wi-FI (2.4GHz) & BT v4.2
  - Ultra Low-Power
  - Xtensa Dual-Core LX6
    - up to 240MHz
    - ROM, SRAM, no CPU caches
  - GPIOs, Touch sensor, ADC...
  - 4 SPI, 3 UART, Ethernet...
  - No USB

5

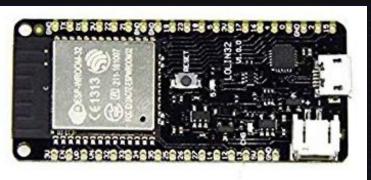
### The target





### ESP32 Form Factor

- ESP32 SiP module (ESP32-WROOM-32)
  - Easy to integrate in any design
  - Flash storage 4MB
  - FCC certified
- ESP32 Dev-Kit (Lolin ESP32)
  - Micro-USB
    - Power
    - ttyUSB0 port
    - Pin headers
  - Limited Cost
    - 15\$





### ESP32 Software

• Esp-idf Dev. Framework on Github

- xtensa-esp32-elf toolchain
- Set of Python Tools (esptool)
- Good Quality of Documentation
  - Datasheet and TRM available [2]
- Arduino core supported
  - I don't like pre-compiled libraries, I don't use it
- •Official Amazon AWS IoT Platform
  - FreeRTOS, Mongoose OS...

## Agenda Today

### • Focus on Built-in Security

• Just Grep the Datasheet

• Four Points

- Crypto HW accelerator
- Secure Boot
- Flash Encryption
- OTP

8

•Let's start!

#### 1.4.4 Security

- Secure boot
- Flash encryption
- 1024-bit OTP, up to 768-bit for customers
- Cryptographic hardware acceleration:



### OPTIONS MENU SETTINGS



10

### The Limited Plan

- The Context
  - 3 months to investigate (spare time)
- My Objective
  - Break one by one the Security Features
    - Physical Access Required (plausible attack scenario nowadays)
- So, I will probably use HW Techniques
  - Fault Injection, Side Channel maybe?
  - Micro-soldering, PCB modification
  - Reverse
  - And Code Review  $\odot$

### Fault Injection

- Voltage glitching
  - Well-known, still efficient and Low-cost FI technique nowadays
    - Public ressources about voltage glitching [3][4][...]

•Goal

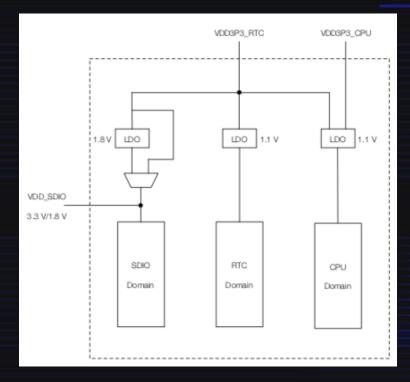
11

- Perturb the Power of the chip to induce a fault during critical SW/HW operations
- Expected effects
  - Skip instruction
    - Checks…
  - Data/Code modification
    - Branch conditions...
  - Sometimes difficult to predict/understand
    - especially with complex CPU architecture (cache effects?, pipeline?...)

12

### Power domains inside ESP32

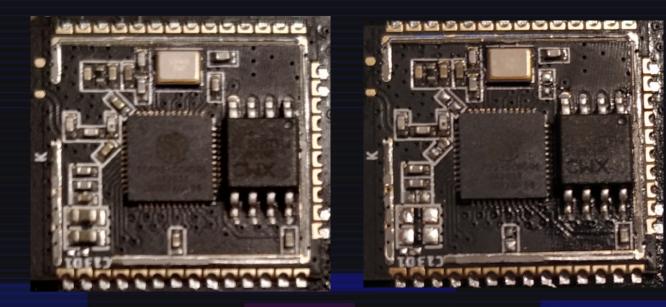
- 3 separate Power domains
- CPU domain shares two Power Signals
  - VDD3P3\_CPU && VDD3P3\_RTC (not common)
- Low Drop-out regulators (LDO)
  - Stabilize internal voltages
    - Filter effect against glitches?
- Brownout Detector (BOD)
  - « If the BOD detects a voltage drop, it will trigger a signal shutdown and even send a message on UART »
    - Able to detect glitches?
- BoD only effective on VDD\_RTC
- So, I will Glitch on VDD3P3\_CPU



Brownout detector was triggered ets Jun 8 2016 00:22:57 COM is not ok ['']

### Target Preparation

- ESP-WROOM-32 Module
  - Shield is removed
- No silkscreen but Schematic available
- I remove Capacitors connected to VDD\_CPU and VDD\_RTC



### PCB Modification

- Three steps
  - Expose the VDD\_CPU trace (Pin 37)
  - Cut the trace
  - Solder the glitch output to VDD\_CPU pin and GND



### HW Setup

#### • Home-made Glitcher (10\$)

- Based on MAX4619
- Add passive components
- SMA connectors
- Synchronised by a Scope
- Triggered by Signal Generator
  - USB commands to set parameters
    - Delay
    - Width
    - Voltage

#### Python scripts for full-control

• Can run during days...

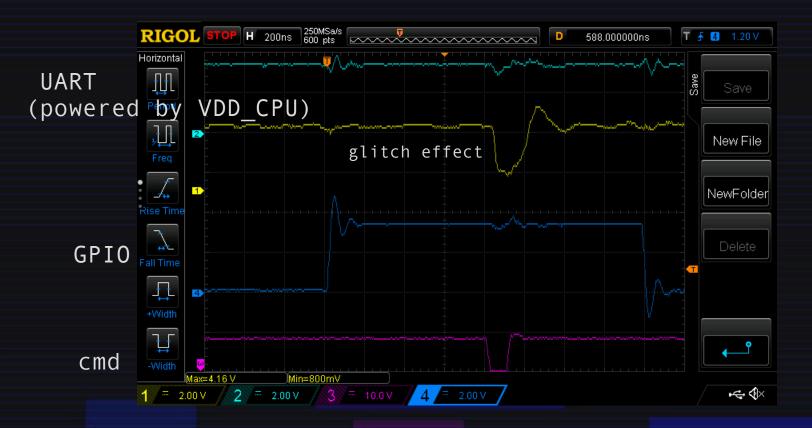




16

# Voltage Glitching effect

### • Effect Looks good



17

# THE CRYPTO-CORE



# Crypto-Core/ Crypto-Accelerator

- Just a peripheral to speed-up the computation
  - AES, SHA, RSA...
- •Why is it interesting to pwn?
  - Espressif Crypto-Lib
  - HW accel. used by default in MBedTLS
    - MBedTLS is the ARM crypto-library (all IoT are using it)
- •My Goal

18

- Focus on the CPU/Crypto interface (crypto-driver)
  - Do not expect to find 'pure' Software Vulns
- Looking for vulns triggered by Fault Injection
- It is Time for Code Review

### Design Weakness

### •AES operation

• Datasheet

#### Single Operation

- 1. Initialize AES\_MODE\_REG, AES\_KEY\_n\_REG, AES\_TEXT\_m\_REG and AES\_ENDIAN\_REG.
- 2. Write 1 to AES\_START\_REG.
- 3. Wait until AES\_IDLE\_REG reads 1.
- 4. Read results from AES\_TEXT\_m\_REG.

• Design Weakness

 AES\_TEXT\_m\_REG registers used to store plaintext and also ciphertext

#### • Encrypt-In-Place can be risky

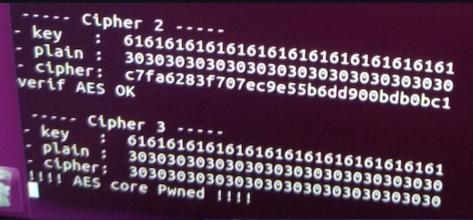
- If something goes wrong during AES call, pretty sure I can retrieve the plaintext
  - Pretty cool & simple to exploit as first PoC

## Vuln n\*1 = AES Bypass

- Previous Weakness is confirmed
- Multiple spots to trigger
  - AES call
  - The while condition
  - The For loop
- PoC

20

• Output = Input



\* Call only while holding esp\_aes\_acquire\_hardware().
\*V4.0-dev-141-g106dc0590-dirty

static inline void esp\_aes\_block(const void \*input, void \*output)

```
const uint32_t *input_words = (const uint32_t *)input;
uint32_t *output_words = (uint32_t *)output;
uint32_t *mem_block = (uint32_t *)AES_TEXT_BASE;
```

```
for(int i = 0; i < 4; i++) {
    mem_block[i] = input_words[i];
}</pre>
```

DPORT\_REG\_WRITE(AES\_START\_REG, 1);

```
DPORT_STALL_OTHER_CPU_START();
{
    while (_DPORT_REG_READ(AES_IDLE_REG) != 1) { }
    for (int i = 0; i < 4; i++) {
        output_words[i] = mem_block[i];
    }
}
DPORT_STALL_OTHER_CPU_END();</pre>
```

## Vuln n\*2 = AES SetKey

#### • Vuln to trigger

• Unprotected loop for to load the key into the crypto-core

• PoC

- Key ZEROized
- Persistent key value until the next setkey()
- Nice for attacking AES Cipher Block Chaining Mode

static inline void esp\_aes\_setkey\_hardware( esp\_aes\_context \*ctx, int mode)

const uint32\_t MODE\_DECRYPT\_BIT = 4; unsigned mode\_reg\_base = (mode == ESP\_AES\_ENCRYPT) ? 0 : MODE\_DECRYPT\_BIT;

```
for (int i = 0; i < ctx->key_bytes/4; ++i) {
    DPORT_REG_WRITE(AES_KEY_BASE + i * 4, *(((uint32_t *)ctx->key) + i));
```

DPORT\_REG\_WRITE(AES\_MODE\_REG, mode\_reg\_base + ((ctx->key\_bytes / 8) - 2));

```
>>> from Crypto.Cipher import AES
>>>
>>> aes = AES.new(b'\x00' * 0x10, AES.MODE_ECB)
>>> cipher = aes.encrypt(b'0' * 0x10)
>>> print(''.join('{:02x}'.format(x) for x in cipher))
e08682be5f2b18a6e8437a15b110d418
```

22

# Crypto-Core Conclusion

- •Crypto-core does not improve security
- Six Vulns with PoCs in AES and SHA
  - Espressif HwCrypto in esp-idf 4.0
  - ARM MbedTLS v2.13.1
- Resp. disclosure
  - No answer from Espressif & ARM during 1 month 🐵
  - BugBounty Program from ARM MBedTLS is Fake ☺
  - Silent Patch attempt 🐵
- •I am (a little bit) in a FURY now...
- •...and I am going to pwn HARDer



23

# SECURE BOOT

ZERONIGHTS.ORG

## Role of Secure Boot

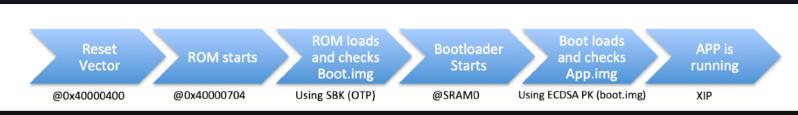
- Protector of FW Authenticity
- Avoid FW modification
  - Easy to flash new Firmware in SPI Flash
  - CRC? Not sufficient sorry...
- It will Create a Chain of Trust
  - BootROM to Bootloader until the App
- It Guarantees the code running on the device is Genuine
  - Will not boot if images are not properly signed

### ESP32 SecBoot during Production

- Secure Boot Key (SBK)
  - SBK burned into E-Fuses BLK2
  - This SBK cannot be readout or modified (R/W protected)
  - Used by bootROM to perform AES-256 ECB
- ECDSA key pair
  - Created by the App developer
  - Priv. Key used to sign the App
  - Public Key integrated to bootloader.img
- The Bootloader Signature
  - 192 bytes header = 128 bytes of random + 64 bytes digest
    - Digest = SHA-512(AES-256((bootloader.bin + ECDSA PK), SBK))
  - Random at 0x0 in Flash Memory layout, digest at 0x80

### Sec. Boot on the Field

• Boot process



#### • Verification Mechanisms

- BootROM (Stage 0)
  - Compute Digest with SBK and compare with 64-bytes Digest at 0x80
- ECDSA verification by the Bootloader (Stage 1)
  - Micro-ECC is used
- •I will Focus on Stage 0
  - Signature based on Symmetric Crypto
  - SBK = AES-Key used to sign the bootloader (CRITICAL ASSET)
    - Stored in E-Fuses, R/W protected

27

### Set the Secure Boot

- Can be done automatically by ESP-IDF Framework...
- •But I prefer to do it manually
  - Burn the Secure Boot Key into BLK2
    - \$ espefuse.py burn\_key secure\_boot ./secure-bootloader-key-256.bin
  - Burn the ABS\_DONE fuse to activate the sec boot
    - \$ espefuse.py burn\_efuse ABS\_DONE\_0
- E-Fuses Map
  - espefuse.py summary
- •Look JTAG fuse 😳

Security fuses:		
FLASH_CRYPT_CNT	Flash encryption mode counter	= 0 R/W (0×0)
FLASH_CRYPT_CONFIG	Flash encryption config (key tweak bits)	= 0 R/W (0x0)
CONSOLE DEBUG DISABLE	Disable ROM BASIC interpreter fallback	= 1 R/W (0x1)
ABS_DONE_0	secure boot enabled for bootloader	= 1 R/W (0x1)
ABS_DONE_1	secure boot abstract 1 locked	= 0 R/W (0x0)
JTAG_DISABLE	Disable JTAG	= 0 R/W (0x0)
DISABLE_DL_ENCRYPT	Disable flash encryption in UART bootloader	= 0 R/W (0x0)
DISABLE_DL_DECRYPT	Disable flash decryption in UART bootloader	= 0 R/W (0x0)
DISABLE_DL_CACHE	Disable flash cache in UART bootloader	= 0 R/W (0x0)
BLK1	Flash encryption key	
= 00 00 00 00 00 00	00 00 00 00 <sup>°</sup> 00 00 00 <sup>°</sup> 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 R/W
BLK2	Secure boot key	
= ?? ?? ?? ?? ?? ??	זר רו דו	-/- ?? ?? ?? ?? ?? ?? ?? ?? ??
BLK3	Variable Block 3	
= 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 R/W

### Secure boot in Action

#### • Signed App (using SBK)

#### void app\_main()

#### while(1)

printf("Hello from SEC boot K1 !\n"); vTaskDelay(1000 / portTICK\_PERIOD\_MS);

#### • make flash, then it runs

ets Jun 8 2016 00:22:57

rst:0x10 (RTCWDT\_RTC\_RESET),boot:0x13 (SPI\_FAST\_FLASH\_B0OT) configsip: 0, SPIWP:0xee clk\_drv:0x00,q\_drv:0x00,d\_drv:0x00,cs0\_drv:0x00,hd\_drv:0x00,wp\_drv:0x00 mode:DI0, clock div:2 load:0x3fff0018,len:4 load:0x3fff001c,len:8556 load:0x40078000,len:12064 load:0x40080400,len:7088 entry 0x400807a0 D (88) bootloader\_flash: mmu set block paddr=0x000000000 (was 0xffffffff) I (38) boot: ESP-IDF v4.0-dev-667-gda13efc-dirty 2nd stage bootloader ... I (487) cpu\_start: Pro cpu start user code I (169) cpu\_start: Starting scheduler on PRO CPU. Hello from Sec boot K1 !

Hello from Sec boot K1 !

#### • Unsigned App (no Key)

#### void app\_main()

#### while(1)

printf("Sec boot pwned by LimitedResults!\n"); vTaskDelay(1000 / portTICK\_PERIOD\_MS);

#### • Flash it then Fail

#### ets Jun 8 2016 00:22:57

rst:0x10 (RTCWDT\_RTC\_RESET),boot:0x13 (SPI\_FAST\_FLASH\_BOOT) configsip: 0, SPIWP:0xee clk\_drv:0x00,q\_drv:0x00,d\_drv:0x00,cs0\_drv:0x00,hd\_drv:0x00,wp\_drv:0x00 mode:DI0, clock div:2 load:0x3fff0018,len:4 load:0x3fff001c,len:3476 load:0x40078000,len:0 load:0x40078000,len:13740 secure boot check fail ets\_main.c 371 ets Jun 8 2016 00:22:57

#### Stuck in stage0 (perfect)

ZERONIGHTS.ORG

### Bypass the Secure Boot

- •Why?
  - To have code exec
- How?
  - Force ESP32 to execute my unsigned bootloader to load my unsigned app
- Focus on BootROM
  - Always Nice to exploit BootROM vulns
  - Always Difficult to Fix BootROM vulns
- So, I need to reverse the BootROM image
   But first, I need to dump it...

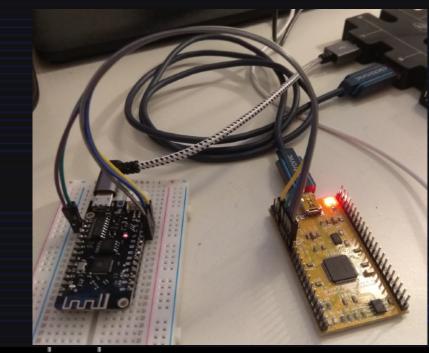
30

### Dump the BootROM

• Memory map

Category	Target	Start Address	End Address	Size		
Embedded Memory	Internal ROM 0	0x4000_0000	0x4005_FFFF	384 KB		
	Internal ROM 1	0x3FF9_0000	0x3FF9_FFFF	64 KB		
	Internal SRAM 0	0x4007_0000	0x4009_FFFF	192 KB		
	Internal SRAM 1	0x3FFE_0000	0x3FFF_FFFF	128 KB		
		0x400A_0000	0x400B_FFFF	120 ND		
	Internal SRAM 2	0x3FFA_E000	0x3FFD_FFFF	200 KB		
	RTC FAST Memory	0x3FF8_0000	0x3FF8_1FFF	8 KB		
		0x400C_0000	0x400C_1FFF	OND		
	RTC SLOW Memory	0x5000_0000	0x5000_1FFF	8 KB		

- Remember I didn't burn JTAG DISABLE E-Fuse?
  - FT2232H board (20\$)
  - OpenOCD + xtensa-esp32-gdb
- Full Debug Access
  - Reset Vector 0x40000400
- BootROM dumped



(gdb) target remote :3333 Remote debugging using :3333 0x40000400 in ?? () (gdb)

### BootROM Reverse

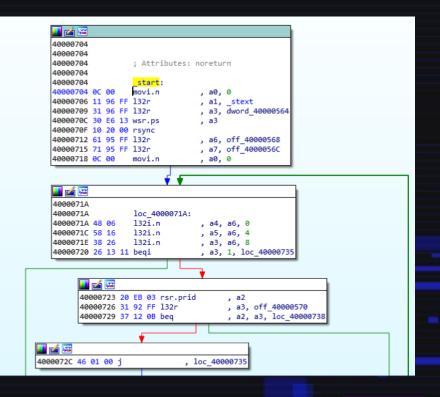
- •Xtensa is 'exotic' arch
  - registers windowing, lengths of instr...
  - ISA [5]
- IDA

31

- ida-xtensa plugin from @themadinventor
- •Secure\_boot.h
  - List all the ROM functions
    - They deprecated since...
- •Call my 'little bro' to check my mess
  - @wiskitki

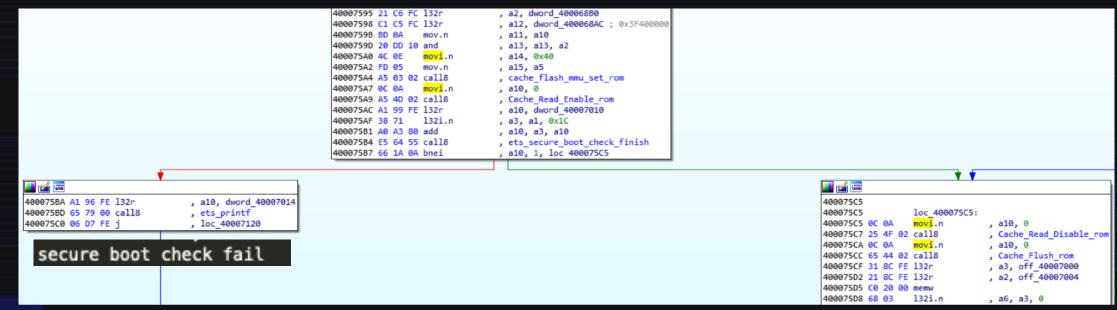
• At the end, not perfect but doable

• \_start at 0x40000704 (as expected)



### The BootROM Vuln

#### •After ets\_secure\_boot\_check\_finish()



Bnei (Branch if not equal immediate)

• Depends on a10 Register value (storing sec\_boot\_check() retvalue)

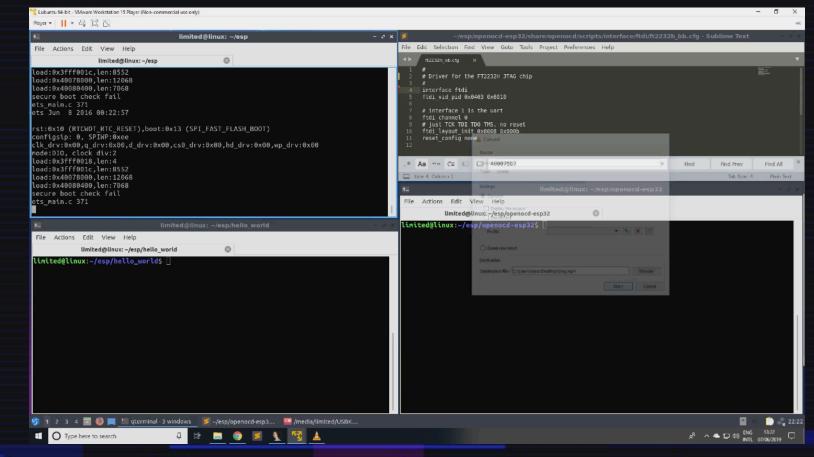
•I want PC jump to 0x400075C5 to execute the bootloader

#### ZERO NIGHTS 2019<sup>EDITION</sup>

33

### Jtag Exploit Validation

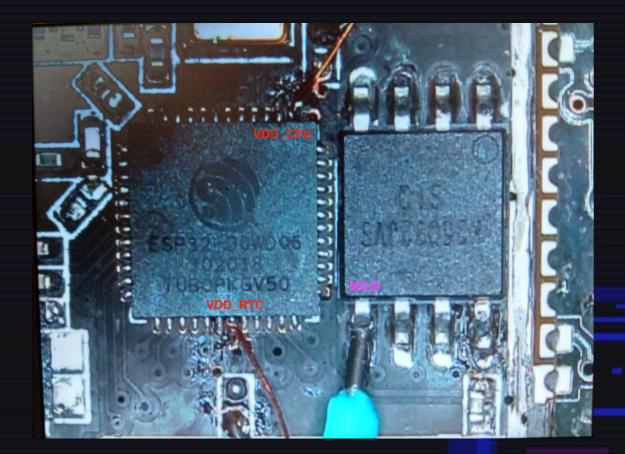
### • Set al0 register = 0 via JTAG to bypass secboot



ZERONIGHTS.ORG

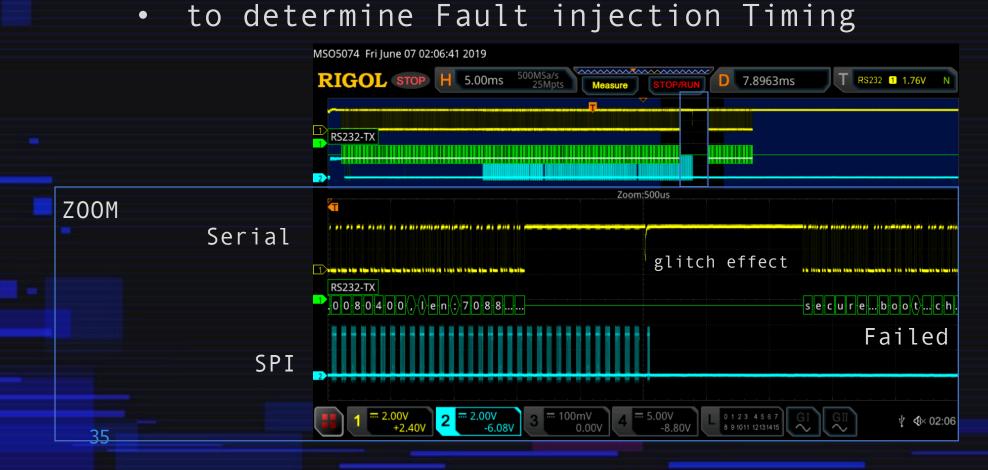
## Time to Pwn (for Real)

- •Real Life
  - JTAG is disabled
  - I could not find a way to exploit this Vuln by SW
- So, Fault Injection is my only way here
  - Simultaneous glitch on VDD\_CPU && VDD\_RTC
  - SPI MOSI is probed to have a timing information



### First attempts during BootROM

• Previous BootROM Reverse is helpful

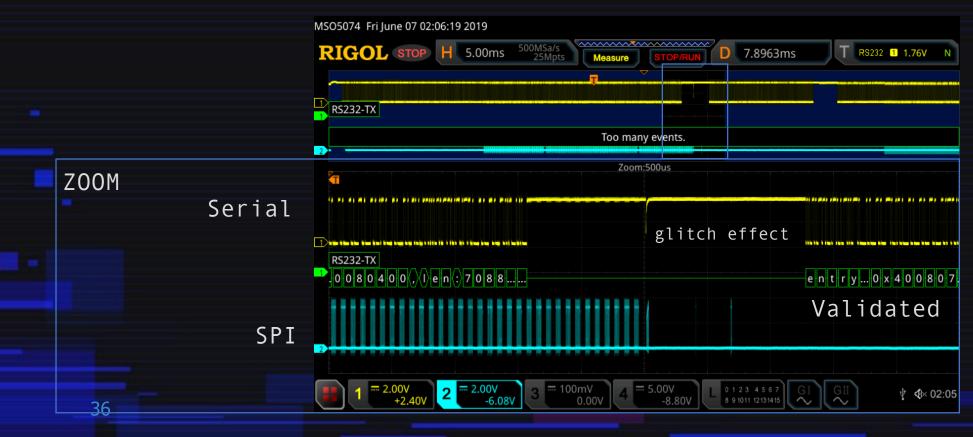


ZERONIGHTS.ORG

# Successful Sec.Boot Bypass

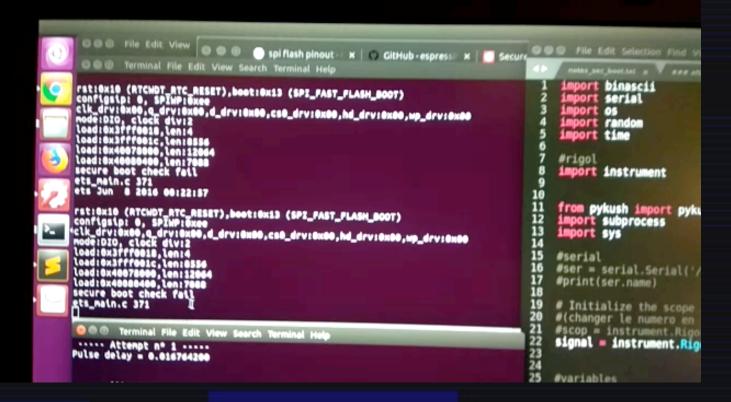
ZERONIGHTS.ORG

# •CPU is jumping to the entry point, Bootloader is executed. Done



### PoC Secure Boot

#### • Sorry for the tilt



### Secure Boot Conclusion

• Secure Boot Bypass exploit

- Stage 0 (bootROM Vuln)
- Triggered by Fault Injection
- Not persistent if Reset occurs
- No way to Fix this without ROM revision
- Resp. disclosure
  - PoC sent on June 4
  - Security Advisory on Sept. 2
    - CVE-2019-15894 (requested by Vendor)
    - Patched by Flash Encryption always enabled
    - A security lab, called Riscure, found the same vuln

• No silent patch attempt this time...



39

# FLASH ENCRYPTION

40

### Role of Flash Encryption

• Protector of FW Confidentiality

- Protect against Binary extraction and Reverse
- •Without FE, it is easy to extract sensitive data
  - Ex: LIFX Wi-Fi lightbulbs [6]
- Firmware Encryption more and more present Today
  - Security by obscurity...
- Espressif recommends Secure Boot + Flash Encryption for maximum Security



HACKADAY IO TINDIE HACKADAY PRIZE SUBMIT

DON'T TOSS THAT BULB, IT KNOWS YOUR PASSWORD



MOTHERBOARD | By Daniel Oberhaus | Jan 31 2019, 627pm

BLOG

This Hacker Showed How a Smart Lightbulb Could Leak Your Wi-Fi Password

The "moderate to severe" vulnerabilities discovered by the hacker LimitedResults have since been fixed, according to the smart bulb company LIFX.

### Flash Encryption Review

- HW AES Enc./Dec. Block in Flash Memory Controller
  - Fetch Key from E-Fuses and other parameters
  - Decrypt/Encrypt I/D into a Cache
  - SW cannot access

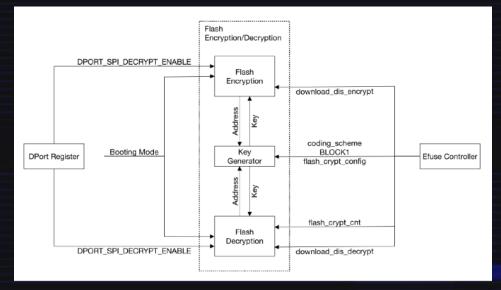
ZERO

NIGHTS

2019 EDITION

41

- Flash Encryption Key (FEK)
  - AES-Key used to decrypt the FW
    - Stored in E-Fuses BLK1 (R/W protected)
  - CRITICAL ASSET (of course)



42

### Set the Flash Encryption

#### • Burn the FEK into BLK1

 \$ espefuse.py --port /dev/ttyUSB0 burn\_key flash\_encryption my\_flash\_encryption\_key.bin

#### • Activate the Flash Encryption

- \$ \$ espefuse.py burn\_efuse FLASH\_CRYPT\_CONFIG 0xf
- \$ espefuse.py burn\_efuse FLASH\_CRYPT\_CNT
- Flash encrypted FW into ESP32
- Verify E-Fuses Map
- Verify encrypted FW

espefuse.py summary espefuse.py v2.7-dev Connecting EFUSE_NAME	Description = [Meaningful Value] [Readable/Writ	eable] (Hex Value)	
Security fuses: FLASH_CRYPT_CNT FLASH_CRYPT_CONFIG CONSOLE_DEBUG_DISABLE ABS_DONE_0 ABS_DONE_1 JTAG_DISABLE DISABLE_DL_ENCRYPT DISABLE_DL_DECRYPT	Flash encryption mode counter Flash encryption config (key tweak bits) Disable ROM BASIC interpreter fallback secure boot enabled for bootloader secure boot abstract 1 locked Disable JTAG Disable flash encryption in UART bootloader Disable flash decryption in UART bootloader	= 1 R/W (0x1) = 1 R/W (0x1) = 0 R/W (0x0) = 1 R/W (0x1) = 0 R/W (0x0)	
DISABLE_DL_CACHE	Disable flash cache in UART bootloader		
BLK1	Flash encryption key		
	77 77 77 77 77 77 77 77 77 77 77 77 77	?? ?? ?? ?? ?? ??	-/- ?? ?? ?? ??
BLK2	Secure boot key		
	זר <u>זר זר זר זר זר זר</u>	?? ?? ?? ?? ?? ??	-/- ?? ?? ?? -/-
BLK3	Variable Block 3 ag ag a		

flash_contents.bin         ×           *         EditA:HeX'         Run Script'         Run Templats'         0123456789ABCDEF           0000h:         ND         23         45         6         7         8         9         A         B         C         D         E         F         0123456789ABCDEF           0000h:         ND         B3         55         EA         B3         48         97         48         BA         50         34         20         05         B55.63H-H***********************************																		
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	flash_c	onte	nts.	bin	×													
0000h:       N D: 35       95       9. N D: 35       9. N D:	¥ Ed	lit As: I	Hex∿		Ru	n Scr	lpt∨		Rur	n Tem	plate							
0010h: 45 CD 65 33 34 2F 0D 03 1E F8 73 C5 A2 26 D4 DC 0020h: 65 21 63 B7 4F 81 F6 EE 43 27 5E C2 3C 27 B9 AB 0030h: AA DC 12 25 6E F1 D3 2B 82 6E 22 0E 5E D9 A3 D6 0040h: 37 98 4C A2 6A 44 7E 10 E8 7C 51 0B 82 1A 0B 9C 0050h: 60 2D 80 29 09 07 21 E5 76 9E 97 0D 5A 69 2F 38 0060h: 71 3B 44 A2 F8 EF 99 F7 0D AA 85 13 13 BF 93 A8 4 D4 1E 0080h: 22 78 F1 B7 BF CA CD 73 0F F2 B7 31 B0 9D D9 72 0090h: EA 26 AE 5D 8C 66 75 45 BE 49 A2 8E 44 D0 CD B0 0080h: 22 78 F1 B7 BF CA CD 73 0F F2 B7 31 B0 9D D9 72 0080h: 22 78 F1 B7 BF CA CD 73 0F 22 B7 31 B0 9D D9 72 0080h: 27 78 F1 B7 BF CA CD 73 0F 22 B7 41 40 67 B 0080h: 27 78 F1 B7 BF CA CD 73 0F 22 B7 31 B0 9D D9 72 0080h: 28 26 AE 5D 8C 66 75 45 BE 49 A2 8E 44 D0 CD B0 0080h: FF A0 70 F2 96 0D 19 F3 0E BE BD 88 F8 8D EA C6 00E0h: FF A0 70 F2 96 0D 19 F3 0E BE BD 88 F8 8D EA C6 00E0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpax1; d5.Å1i&dA <sup>*</sup> 0100h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 22 24 35 0120h: BA A1 E9 FE 0B F8 CE F2 80 22 0F 79 52 00 6F BF 0130h: BA A1 E9 FE 0B F8 CE F2 80 22 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170																		0123456789ABCDEF
0020h: 6D 21 63 B7 4F 81 F6 EE 43 27 5E C2 3C 27 B9 AB mic $\circ 0.31C^{-3}A^{+1} \approx 0.030h$ : AA DC 12 25 6E F1 D3 2B 82 6E B2 0E 5E D9 A3 0B $\circ 0.5nh0^{-},n^{-1}.^{0}D_{E}$ . 0040h: 37 98 4C A2 6A 44 7E 10 E8 7C 51 0B 82 1A 0B 92 F38 $\circ 0.5nh0^{-},n^{-1}.^{0}D_{E}$ . 0050h: 60 2D 80 29 09 07 21 E5 76 9E 97 0D 5A 69 2F 38 $\circ 0.5nh0^{-},n^{-1}.^{0}D_{E}$ . 0070h: 7F 21 8C AB C3 EA 7A 45 ED 60 EB B3 48 44 D4 12 $\cdot 0.5nh0^{-},n^{-1}.^{0}D_{E}$ . 0080h: 27 8 F1 B7 BF CA CD 73 0F F2 B7 31 B0 9D D9 72 $\circ n.5h^{-}D_{E}$ . 0080h: C7 DE 8B 5A 6C C8 36 FC 3A 22 47 9E 74 14 05 7B $\cdot 0.5h^{-}D_{E}$ . 0080h: F7 A0 70 F2 96 0D 19 F3 0E BE D8 8F 80 DE AC 6 00E0h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 80 DE AC 6 00E0h: E6 FE 35 8C CB F F4 9E 14 C2 CC 69 C8 34 C4 98 $\circ hhat 16^{-}Aht^{-}A$	0000h:	A7	DE		95	EA	B3	48	97	48	BA	50	ЗA	E0	99		05	505•ê³H—H°P:à™ .
0030h: AA DC 12 25 6E F1 D3 2B 82 6E B2 0E 5E D9 A3 0B 0040h: 37 98 4C A2 6A 44 7E 10 E8 7C 51 0B 82 1A 0B 9C 0050h: 60 2D 80 02 90 90 72 1E 57 60 5E 97 0D AA 85 13 11 3B F9 A3 0060h: 71 3B 44 A2 F8 EF 99 E7 0D AA 85 13 11 3B F9 A3 0070h: 7F 21 8C AB C3 EA 7A 45 ED 60 EB B3 48 44 D4 LE 0080h: 22 78 F1 87 BF CA CD 73 0F 2F 37 31 B0 9D 97 7 0090h: EA 26 AE 5D 8C 66 75 45 BE 48 A2 8E 44 D0 CD B0 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 0000h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0000h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0010h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 48 0D CE 34 F1 0B BF 08 7C 0A 6C 1B 2E 24 35 0110h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0100h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0100h: BA A1 E9 FE 0B F3 CE F2 80 2E 0F 79 52 00 6F BF 0100h: BA C3 CC 66 0C 65 4A 77 A9 1E BA B1 E 0170h: 18 E8 80 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 80 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 80 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 80 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 80 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 80 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 80 3F 13 EC 06				65	33	34			03	1E	F8	73		A2	26	D4	DC	Eĺe34/øsÅ¢sÔÜ
0040h: 37 98 4C A2 6A 44 7E 10 E8 7C 51 0B 82 1A 0B 9C 0050h: 60 2D 80 29 09 07 21 E5 76 9E 97 0D 5A 69 2F 38 0060h: 71 3B 44 A2 F9 EF 99 E7 0D AA 85 13 13 BF 9A 0070h: 7E 21 8C AB C3 EA 7A 45 ED 60 EB B3 48 44 D4 1E 	0020h:		21	63	в7		81	F6	EE	43	27	5E		3C	27	В9	AB	m!c.0.öîC'^Â<''«
0050h: 60 2D 60 29 09 07 21 E5 76 9E 97 0D 5A 69 2F 98 0060h: 71 3B 44 A2 F8 EF 99 E7 0D AA 85 13 11 3B F9 A3 0070h: 7F 21 8C AB C3 EA 7A 45 ED 60 EB B3 48 44 D4 0080h: 22 78 F1 B7 BF CA CD 73 0F F2 B7 31 B0 9D D9 72 0090h: EA 26 AE 5D 8C 66 75 45 BE 48 A2 8E 44 D0 CD 08 0000h: F9 00 A1 74 84 D4 9D 09 69 8B 29 90 3A 8E 59 4C 0000h: F9 00 A1 74 84 D4 9D 09 69 8B 29 90 3A 8E 59 4C 0000h: F9 A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 78 0D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 8F 78 0D EA C6 0000h: BA A1 E9 FE 0B F8 CE F74 9E 14 C2 CC 69 C8 34 C4 98 mpax1;∂ã.Å1124Å 0000h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 16%.Å.6[a.B°S.4] 0150h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 7A 91 1E B AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 7A 91 1E B AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 7A 91 1E B AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0	0030h:	AA	DC	12		6E	F1		2B	82		B2	0E		D9	A3	0B	*Ü.%nñÓ+,n².^Ù£.
0060h: 71 3B 44 A2 F8 EF 99 E7 0D AA 85 13 11 3B F9 A3 0070h: 7F 21 8C AB C3 EA 7A 45 ED 60 EB B3 48 44 D4 1E 108A32E1 * 3HDÓ. 0090h: EA 26 AE 5D 8C 66 75 45 EE 48 A2 8E 44 D0 CD 80 0090h: EA 26 AE 5D 8C 66 75 45 EE 48 A2 8E 44 D0 CD 80 0090h: EA 26 AE 5D 8C 66 75 45 EE 48 A2 8E 44 D0 CD 80 0080h: F9 0E A1 74 84 D4 0D 99 69 82 99 03 A8 E5 90 LA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE D0 88 F8 8D EA C6 0000h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 8D EA C6 0000h: A7 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 78.14A02.1.1\$5 0120h: BA A1 E9 FE 0B F8 CE F2 80 22 0F 79 52 00 6F BF 0140h: BA C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 E 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0.7.1.0EF58'&: 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0.7.1.0EF58'&: 0180h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 9C 6 0190h: 51 27 91		37	98	4C	Α2	6A	44		10	E8		51	0B	82	1A	0B	9C	7~L¢jD~.è Q.,œ
0070h: 7F 21 8C AB C3 EA 7A 45 ED 60 EB B3 48 44 D4 1E .1GxAāsEi 6*HDÓ. 0080h: 22 78 F1 B7 BF CA CD 73 0F F2 B7 31 B0 9D D9 72 0090h: EA 26 AB 50 8C 67 54 5 BE 48 A2 8E 44 D0 C1 D 0080h: CF DB 8B 5A 6C C8 36 FC 3A 22 47 9E 74 14 05 7B 0060h: FF A0 70 F2 96 0D 19 F3 0E BE D0 86 F8 6D EA C6 00E0h: FF A0 70 F2 96 0D 19 F3 0E BE D0 86 F8 6D EA C6 00E0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 86 F8 6D EA C6 00E0h: E6 FF E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 00F0h: E6 FF E3 58 EC BF F4 9E 14 C2 CC 69 C6 34 C4 98 00F0h: E6 FF E3 58 EC BF F4 9E 14 C2 CC 69 C6 34 C4 98 00F0h: B6 FF E3 58 EC BF F4 9E 14 C2 CC 69 C6 34 C4 98 0010h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 78. f4n021.\$5 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0;60.sf26yR.o; 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 8D 3F 13 EC 06 70 65 D8 F1 A1 DE 7F E0 C6 0170h: 18 C7 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F E0 C6 0170h: 51 27 91		60		80	29	09	07	21			9E	97			69		38	`-€)!åvžZi/8
0080h: 22 78 F1 B7 BF CA CD 73 0F F2 B7 31 B0 9D D9 72 "xh·c£fs.o·1·.0r 0090h: EA 26 AE 5D 8C 66 75 45 BE 48 A2 8E 44 D0 CD B0 00A0h: CP D8 8B 5A 6C C8 36 FC 3A 22 47 9E 74 14 05 T 00B0h: F9 0E A1 74 84 D4 9D 09 69 8B 29 90 3A 8E 59 4C 00C0h: FF A0 70 F2 96 0D 19 F3 0E BE D8 8F 86 DE AC 6 00E0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAx1;∂5.Åfi£4Å 00F0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAx1;∂5.Åfi£4Å 00F0h: B6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAx1;∂5.Åfi£4Å 00F0h: B6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAx1;∂5.Åfi£4Å 00F0h: B6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAx1;∂5.Åfi£4Å 01F0h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0130h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0170h: 18 EE AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EE AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EE AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 12 79 19 82 C3 C3 A5 02 70 BF F1 A1 DE 7F B9 C6 0190h: 51 27 91 98 2C3 C3 A5 02 70 BF F1 A1 DE 7F B9 C6 0170h: C2 MF3 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC 06 F0 C6 54 A7 PA 91 EB AB 1E 0170h: 18 EF AB 3F 13 EC	0060h:	71	3B	44	Α2	F8	EF	99	Ε7		AA	85	13	11		F9	AЗ	q;D¢øï™ç.ª;ù£
0090h: EA 26 AE 5D 8C 66 75 45 BE 48 A2 8E 44 D0 CD B0 00A0h: CF DE 8B 5A 6C C8 36 FC 3A 22 47 9E 74 14 06 7B 00A0h: CF DE 8B 5A 6C C8 36 FC 3A 22 47 9E 74 14 06 7B 00C0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE B0 88 F8 6D EA C6 00D0h: 56 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpaXi;∂č.Åfi2dÅ: 0100h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0120h: BA A1 E9 FE 0B F8 CE F2 60 2E 0F 79 52 00 6F BF 0130h: BA A1 E9 FE 0B F8 CE F2 60 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7F 90 C 0190h: 51 27	0070h:			8C	AB		EA		45			EB	В3	48	44	D4		.!Œ«ÂêzEí`ë³HDÔ.
$\begin{array}{c} 000 \text{ ADh}: \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$		22	78	Fl	в7	BF	CA	CD	73	OF	F2	в7	31	в0	9D	D9	72	"xñ·;ÊÍs.ò·1°.Ùr
00B0h: F9 0E A1 74 84 D4 9D 09 69 8B 29 90 3A 8E 59 4C 00C0h: FF A0 70 F2 96 0D 19 F3 0E BE DD 86 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE DD 86 F8 6D EA C6 00E0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAX1262.ÅfitA4X 00F0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAX1262.ÅfitA4X 00F0h: B6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAX1262.ÅfitA4X 0100h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 E8 AD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 ER AD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 2F 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7E 99 C6 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 A1 DE 7E 9C6 01*0**********************************	0090h:	EA	26	AE		8C	66		45	BE	48	A2	8E	44	D0		в0	ê&⊗]ŒfuE¾H¢ŽDÐͰ
00C0h: FF A0 70 F2 96 0D 19 F3 0E BE BD 86 F8 6D EA C6 00D0h: FF A0 70 F2 96 0D 19 F3 0E BE BD 88 F8 6D EA C6 00E0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAx1;62.Å1i4Å. 00F0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 00F0h: BA HE 9D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0120h: BA AL E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0120h: BA AL E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 BD 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 51 27 91 98 2C3 C3 A5 02 70 8F E1 AL DE 7E 9C 0190h: 51 27 91 98 2C3 C3 A5 02 70 8F E1A 1D E7 E9 C6 0190h: 51 27 91 90 20 50 50 50 50 50 50	00A0h:		DB	8B	5A	6C		36	FC	ЗA	22	47	9E	74	14	06		ÏÛ <z1è6ü:"gžt{< td=""></z1è6ü:"gžt{<>
00D0h:       FF A0 70 F2 96 0D 19 F3 0E BE B0 86 F8 8D EA C6              ý pô6.44**s.eE              ý pô6.44**s.eE              ý pô6.44**s.eE              ý pô6.44**s.eE              ý pô6.44**s.eE              ý pô6.44**s.eE              ú pô20: A C B              ú pô A C B              vastare              vastare <td< td=""><td></td><td>F9</td><td>0E</td><td></td><td></td><td>84</td><td>D4</td><td>9D</td><td>09</td><td>69</td><td>8B</td><td>29</td><td>90</td><td>ЗA</td><td>8E</td><td>59</td><td></td><td>ù.;t"Ôi&lt;).:ŽYL</td></td<>		F9	0E			84	D4	9D	09	69	8B	29	90	ЗA	8E	59		ù.;t"Ôi<).:ŽYL
00E0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAX1262.Åfit44Å 00FOh: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mpAX1262.Åfit44Å 010Oh: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 44 35 011Oh: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 43 5 012Oh: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 013Oh: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 014Oh: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 015Oh: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 015Oh: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 017Oh: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 017Oh: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 014Oh: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9		FF	A0	70	F2	96	0D	19	F3	0E	ΒE	BD		F8	8D	EA	C6	ÿ pòó.¾½^ø.êÆ
00F0h: E6 FE E3 58 EC BF F4 9E 14 C2 CC 69 C8 34 C4 98 mbAX12/62.AfiE4A- 0100h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0170h: 18 E8 05 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 05 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 05 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 05 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0180h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 96 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0170f: 51 27 91 50 20 20 50 50 50 50 50 50 50 50 50 50 50 50 50			A0			96		19	F3		ΒE	BD	88	F8	8D	$\mathbf{EA}$	C6	ÿ pòó.¾¼^ø.êÆ
0100h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0110h: 37 4B 0D CE 34 F1 DB BF 08 7C 0A 6C 1B 2E 24 35 0120h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0130h: BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 ER 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 15 127 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0140h: 51 27 91 58 20 50 50 50 50 50 50 50 50 50 50 50 50 50		E6		E3	58	EC	$\mathbf{BF}$	F4	9E	14			69	C8	34	C4	98	æþāXì;ôž.ÂÌiÈ4Ä~
0110h:       37       4B       0D       CE       34       F1       DB       BF       08       7C       0A       6C       1B       2E       24       35       7K.14A02.1.155         0120h:       BA       A1       E9       FE       0B       F8       CE       F2       80       2E       0F       79       52       00       6F       BF       °       ?k.02       ?k.22       ?k.0		E6		E3	58	EC	BF	F4	9E	14	C2		69	C8	34	C4	98	acþāXì;ôž.ÂÌiÈ4Ä~
0120h:       BA A1 E9 FE 0B F8 CE F2 00 2E 0F 79 52 00 6F BF       °idp.sldeyR.o;         0130h:       BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF       °idp.sldeyR.o;         0130h:       BA A1 E9 FE 0B F8 CE F2 80 2E 0F 79 52 00 6F BF       °idp.sldeyR.o;         0140h:       BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6       ¿£x.ê.6[s.B°S+4]         0150h:       18 C9 58 16 EA 19 26 50 73 1B DF 93 A7 95 E2 A6       ¿£x.ê.6[s.B°S+4]         0160h:       18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E       .e.?.i.dET5\$*8e.         0170h:       18 E8 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E       .e.?.i.dET5\$*8e.         0180h:       51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6       Q''', <:'e'p,céE		37	4B		CE	34	F1	DB	BF	08		0A		1B		24		
0130h: BA A1 E9 FE 0B F9 CE F2 80 2E 0F 79 52 00 6F BF 0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0160h: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 B0 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0180h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0190h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 01°, ', ', 'E'@p., céE		37				34	F1		BF	08		0A		1B		24		
0140h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0150h: BF C9 58 16 EA 19 26 5B 73 1B DF 93 A7 95 E2 A6 0150h: 18 E8 69 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 69 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0170h: 18 E8 69 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E 0180h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0190h: 51 27 91 90 20 50 50 50 50 50 50 50 50 50 50 50 50 50		BA	A1	Ε9	FE	0B	F8	CE	F2	80	2E	0F	79	52	00	6F	BF	°;éþ.øÎò€yR.o¿
Olsoh:         BF C9 50 16         EA 19 26 5B 73 1B         DF 93 A7 95 E2 A6         ZÊX.â.6[5.8"\$*â]           Olsoh:         18 EB 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E         .a.7.1.8ET\$6*å           Olfoh:         18 EB 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E         .a.7.1.6ET\$6*å           Olfoh:         18 EB 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E         .a.7.1.6ET\$6*å           Olfoh:         18 EB 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E         .a.7.1.6ET\$6*å           Ol8Oh:         51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6         Q''`,<:P'Øbc6E		BA	A1	E9		0B	F8	CE	F2	80	2E	0F	79		00		$\mathbf{BF}$	°;éþ.øÎò€yR.o;
0160h: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E6.?.1.0ÆT56*b%. 0170h: 18 EE 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E6.?.1.0ÆT56*b%. 0180h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 Q <sup>1,*</sup> ,<:P'Øþ¢ÆE 0190h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 Q <sup>1,*</sup> ,<:P'Øþ¢ÆE		BF	C9		16													
0170h: 18 EB 8D 3F 13 EC 06 F0 C6 54 A7 9A 91 EB AB 1E8.?.1.5ÆT58`8«. 0180h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0'', <:P'Ø⊳¢Æ 0190h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 0'', <:P'Ø⊳¢Æ		BF	C9	58	16	EA	19	26	5B	73	1B	DF	93	Α7	95	E2	Α6	¿ÉX.ê.&[s.ß"§•â¦
0180h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 Q'``,<:P'ØbcéE 0190h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 Q'``,<:P'ØbcéE		18	EB	8D	ЗF	13	EC	06	F0	C6	54	Α7	9A		EB	AB	1E	.ë.?.ì.ðÆT§š`ë«.
0190h: 51 27 91 98 2C 3C 3A 50 27 D8 FE 1A 1D E7 E9 C6 Q''~,<:P'ØpçéÆ		18		8D	ЗF	13	EC	06	F0	C6	54	Α7	9A		$\mathbf{EB}$	AB		.ë.?.ì.ðÆT§š`ë«.
		51	27			2C	3C			27	D8	FE	1A	1D			C6	
01100+ 0 nn 58 64 50 00 71 00 90 00 03 10 00 00 66 80 46 \$ \$		51	27		98	2C		ЗA					1A	1D	Ε7			
	01201-	nn	58	64	512	CC	71	22	87	2 n	03	18	ΠQ	017	66	80	46	Ý74^Ì~ŝ∛_₩ ŏf ₽

### How to break Flash Encryption?

- I did some tests (believe me...)
  - Did not find particular Weakness to access the Key by SW or to Attack by DFA
- •My Last Hope is Side Channel Analysis
  - to target the Bootloader decryption
- •But my setup is too 'limited'
  - SPI bus producing a lot of Noise
  - Cannot control the SPI frames
    - Use a kind of SPI emulator but BIG FAIL
  - I tried DPA, CPA...
    - Low SNR, No good Leakage...
- 8-9 NIGHTS, ZERO result...K.O

I (973) cpu\_start: Pro cpu start user code I (320) cpu\_start: Starting scheduler on PRO CPU. I (0) cpu\_start: Starting scheduler on APP CPU. Hello from SEC boot K1 & FE !





45

# OTP/E-FUSES: THE MOTHER OF VULNS

### Role of OTP/E-Fuses

•One-Time-Programmable (OTP) Memory based on E-Fuses

• Non-Volatile-Memory inside the ESP32

- An e-Fuse can be 'programmed' just 'One-Time' from 0 to 1
- Once burned, no possibility to rewrite it or to wipe it
- •Organisation
  - EFUSE\_BLK0 = ESP32 configuration
  - EFUSE\_BLK1 = Flash Encryption Key (FEK)
  - EFUSE\_BLK2 = Secure Boot Key (SBK)
  - EFUSE\_BLK3 = reserved for User Application
- According to Espressif, these E-Fuses are R/W protected and cannot be readout/modified once protection bits set
- E-Fuses are managed by the E-Fuses Controller, a dedicated piece of HW inside the ESP32

### ESP32 E-Fuses Reverse

- Only two identified functions
- •Used during a 'Special Boot mode'
  - interesting...
- BootROM never touch OTP values
- It means only the E-Fuses Controller has access to OTP
  - Pure HW Process
  - Has to be set before BootROM

RCM::40008600         RCM::40008600       ets_efuse_read_op:         RCM::40008600       ets_efuse_read_op:         RCM::40008600       132r       , a9, dword_400085F8         RCM::40008600       132r       , a8, dword_400085F4         RCM::40008600       s22i.n       , a9, a8, 0         RCM::40008600       s22i.n       , a9, a8, 0         RCM::40008600       s22i.n       , a9, a8, 0         RCM::40008611       movi.n       , a9, 1         RCM::40008613       memw       RCM:40008618         RCM::40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         RCM::40008618       loc_40008618       RCM:40008618         RCM::40008610       bnez       , a9, loc_40008618         RCM::40008620       retw.n       RCM:40008620         RCM:40008620       jupte       0         RCM:40008620       .byte       0         RCM:		ROM:40008600	;	== S U B	ROUT	ΙN	E ====================================
ROM:40008600       entry       , a1, 0x20         ROM:40008600       entry       , a9, dword_400085F8         ROM:40008600       132r       , a8, dword_400085F8         ROM:40008600       memw       , a9, a8, 0         ROM:40008600       sizin       , a9, a8, 0         ROM:40008601       132r       , a8, dword_400085F4         ROM:40008602       sizin       , a9, a8, 0         ROM:40008611       movin       , a9, 1         ROM:40008613       memw       ROM:40008618         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ; SODE XREF: ets_efuse_read_op+1D4j         ROM:40008610       bnez       , a9, loc_40008618         ROM:40008620       retw.n       ROM:40008620;         ROM:40008620 ;       .byte       0         ROM:40008620 ;       .byte       0         ROM:40008620 ;       .byte       0         ROM:40008620 ;       .byte       0         ROM:40008623 ;       .byte       0         ROM:40008624 ;       .it 0x5A5A       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008628 ;       .as, dword_40008524       ROM:40008628         ROM:40008628 ;<		ROM:40008600	-				
ROM:40008600       132r       , al, 0x20         ROM:40008603       132r       , al, dword_400085F8         ROM:40008600       132r       , al, dword_400085F4         ROM:40008600       sizin       , al, dword_400085F4         ROM:40008600       sizin       , al, dword_400085F6         ROM:40008601       132r       , al, dword_400085F6         ROM:40008611       movin       , al, dword_400085F6         ROM:40008613       memw       ROM:40008613         ROM:40008616       sizin       , CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ROM:40008618         ROM:40008618       1321.n       , al, al, al, al, al, al, al, al, al, al		ROM:40008600					
ROM:40008600       132r       , al, 0x20         ROM:40008603       132r       , al, dword_400085F8         ROM:40008600       132r       , al, dword_400085F4         ROM:40008600       sizin       , al, dword_400085F4         ROM:40008600       sizin       , al, dword_400085F6         ROM:40008601       132r       , al, dword_400085F6         ROM:40008611       movin       , al, dword_400085F6         ROM:40008613       memw       ROM:40008613         ROM:40008616       sizin       , CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ROM:40008618         ROM:40008618       1321.n       , al, al, al, al, al, al, al, al, al, al		ROM:40008600	ets efuse read of	op:			
R0H:40008606       132r       , a8, dword_400085F4         R0H:40008600       s321.n       , a9, a8, 0         R0H:4000860E       132r       , a8, dword_400085FC         R0H:4000860E       132r       , a8, dword_400085FC         R0H:40008611       movi.n       , a9, 1         R0H:40008613       memw       R0H:40008613         R0H:40008616       S321.n       , a9, a8, 0         R0H:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         R0H:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         R0H:40008620       renu       , a9, a8, 0         R0H:40008620       renu       , a9, loc_40008618         R0H:40008620       .byte 0       ROH:40008622         R0H:40008622       .byte 0       ROH:40008622         R0H:40008622       .byte 0       ROH:40008628         ROH:40008628       renu       S U B R O U T I N E         ROH:40008628       renu       S U B R O U T I N E         ROH:40008628       renu       S U B R O U T I N E </th <th>•</th> <th></th> <th></th> <th></th> <th></th> <th>, a1,</th> <th>, 0x20</th>	•					, a1,	, 0x20
ROM:40008606       132r       , a8, dword_400085F4         ROM:40008609       memw         ROM:4000860E       132r       , a9, a8, 0         ROM:4000860E       132r       , a8, dword_400085FC         ROM:40008611       movin, , a9, a8, 0         ROM:40008613       memw         ROM:40008616       s321.n       , a9, a8, 0         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008610       bmez       , a9, a8, 0         ROM:40008610       bmez       , a9, a0, 0         ROM:40008610       bmez       , a9, a0, 0         ROM:40008620       retw.n       ROM:40008620         ROM:40008620       intotion ets_efuse_read_op         ROM:40008622       .byte 0       ROM:40008622         ROM:40008622       .byte 0       ROM:40008628         ROM:40008628       int 0x5A5A       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008628       int 0x5A5A       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008628       ister op; a0, dword_40008574       ROM:40008528         ROM:40008628       ets_efuse_program_op;       ROM:40008628       ROM:400086574     <	•	ROM:40008603		132r		. a9.	dword 400085F8
ROM:4000860C       \$321.n       , a9, a8, 0         ROM:4000860E       132r       , a8, dword_400085FC         ROM:40008611       movi.n       , a9, 1         ROM:40008613       memw       , a9, a8, 0         ROM:40008616       \$3321.n       , a9, a8, 0         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ; a9, loc_40008618         ROM:40008620       retw.n       ROM:40008620         ROM:40008620 ;	•	ROM:40008606		132r		, a8,	dword 400085F4
RCM:4000860E       132r       , a8, dword_400085FC         RCM:40008611       movi.n       , a9, 1         RCM:40008613       memw         RCM:40008616       s32i.n       , a9, a8, 0         RCM:40008618       icc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         RCM:40008618       memw       RCM:40008618         RCM:40008610       bnez       , a9, loc_40008618         RCM:40008620       retw.n       , a9, loc_40008618         RCM:40008620       icd of function ets_efuse_read_op         RCM:40008620       .byte       0         RCM:40008621       .byte       0         RCM:40008622       .byte       0         RCM:40008623       .byte       0         RCM:40008623       .byte       0         RCM:40008623       .byte       0         RCM:40008624       .int 0x5ASA       ; DATA XREF: ets_efuse_program_op+34r         RCM:40008628       is2r       , a9, dword_40008574         RCM:40008628       is2r       , a9, dword_40008574         RCM:40008628       is2r       , a8, dword_40008574         RCM:40008631       memw       RCM:40008634         RCM:40008634       is32i.n       a9, a8, 0	•	ROM:40008609		memw			-
RCM:4000860E       132r       , a8, dword_400085FC         RCM:40008611       movi.n       , a9, 1         RCM:40008613       memw         RCM:40008616       s32i.n       , a9, a8, 0         RCM:40008618       icc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         RCM:40008618       memw       RCM:40008618         RCM:40008610       bnez       , a9, loc_40008618         RCM:40008620       retw.n       , a9, loc_40008618         RCM:40008620       icd of function ets_efuse_read_op         RCM:40008620       .byte       0         RCM:40008621       .byte       0         RCM:40008622       .byte       0         RCM:40008623       .byte       0         RCM:40008623       .byte       0         RCM:40008623       .byte       0         RCM:40008624       .int 0x5ASA       ; DATA XREF: ets_efuse_program_op+34r         RCM:40008628       is2r       , a9, dword_40008574         RCM:40008628       is2r       , a9, dword_40008574         RCM:40008628       is2r       , a8, dword_40008574         RCM:40008631       memw       RCM:40008634         RCM:40008634       is32i.n       a9, a8, 0	•	ROM:4000860C		s32i.n		. a9.	. a8. 0
ROM:40008611       movi.n       , a9, 1         ROM:40008613       memw         ROM:40008616       s32i.n       , a9, a8, 0         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008619       loc_40008619       ; code XREF: ets_efuse_read_op         ROM:40008620       retw.n       ROM:40008620;         ROM:40008620       ; byte 0       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008622       .byte 0       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008623       .byte 0       ; ROM:40008623         ROM:40008624       dword_40008624       .byte 0         ROM:40008623       .byte 0       ; ROM:40008623         ROM:40008623       .byte 0       ; ROM:40008623         ROM:40008624       dword_40008524       ; ROM:40008625         ROM:40008628       int 0x5A5A       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008628       entry       , a1, 0x20         ROM:40008628       entry       , a9, dword_40008574         ROM:40008621       l32r       , a8, dword_40008574         ROM:40008631       memw       ; CODE XREF: ets_efuse_program_op+104j <t< th=""><th>•</th><th>ROM:4000860E</th><th></th><th>132r</th><th></th><th></th><th></th></t<>	•	ROM:4000860E		132r			
ROM:40008613       memw         ROM:40008616       s321.n       , a9, a8, 0         ROM:40008618       loc_40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       loc_40008618       memw         ROM:40008610       loc_40008618       retw.n         ROM:40008620       retw.n       a9, loc_40008618         ROM:40008620       .byte 0       ROM:40008623       .byte 0         ROM:40008623       .byte 0       ROM:40008624       .int 0xSASA         ROM:40008624       .byte 0       ROM:40008628       .byte 0         ROM:40008628       .byte 0       ROM:40008628       .byte 0         ROM:40008628       .byte 0       ROM:40008628       .byte 0         ROM:40008628       .byte 0       ROM:40008628       .int 0xSASA         ROM:40008628       .byte 0       ROM:40008628       .astriational control of the contro	•	ROM:40008611		movi.n			
ROM:40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       1321.n       , a9, a8, 0         ROM:40008620       retw.n         ROM:40008620       ; End of function ets_efuse_read_op         ROM:40008620       ; byte       0         ROM:40008621       int 0x5A5A       ; DATA XREF: ets_efuse_program_op:34r         ROM:40008628       ; a1, 0x20       ; conextent         ROM:40008628       int 0x7       , a1, 0x20         ROM:40008628       132r       , a9, dword_40008574         ROM:40008631       memw       ; cone xaters         ROM:40008634       s321.n       , a9, a8, 0         ROM:40008639       movi.n       ; a9, a8, 0	•	ROM:40008613		memw			
ROM:40008618       ; CODE XREF: ets_efuse_read_op+1D4j         ROM:40008618       1321.n       , a9, a8, 0         ROM:40008620       retw.n         ROM:40008620       ; End of function ets_efuse_read_op         ROM:40008620       ; byte       0         ROM:40008621       int 0x5A5A       ; DATA XREF: ets_efuse_program_op:34r         ROM:40008628       ; a1, 0x20       ; conextent         ROM:40008628       int 0x7       , a1, 0x20         ROM:40008628       132r       , a9, dword_40008574         ROM:40008631       memw       ; cone xaters         ROM:40008634       s321.n       , a9, a8, 0         ROM:40008639       movi.n       ; a9, a8, 0	•	ROM:40008616		s32i.n		. a9.	. a8, 0
ROM:40008618       memw         ROM:40008610       bnez         ROM:40008610       bnez         ROM:40008620       retw.n         ROM:40008620       retw.n         ROM:40008620       jend         ROM:40008620       jend         ROM:40008620       jend         ROM:40008620       jend         ROM:40008620       jend         ROM:40008620       jend         ROM:40008620       byte         ROM:40008621       byte         ROM:40008622       byte         ROM:40008623       byte         ROM:40008624       int 0x5A5A         ROM:40008628       jend         ROM:40008628       summon         ROM:40008628       summon         ROM:40008628       ets_efuse_program_op:         ROM:40008628       ets_efuse_more         ROM:40008628       llll         ROM:40008628       lllll         ROM:40008628       llllllllllllllllllllllllllllllllllll		ROM:40008618					
ROM:4000861B       132i.n       , a9, a8, 0         ROM:4000861D       bncz       , a9, loc_40008618         ROM:40008620       retw.n         ROM:40008620 ; End of function ets_efuse_read_op         ROM:40008620 ;       byte         ROM:40008621 dword_40008624 .int 0x5A5A ;       DATA XREF: ets_efuse_program_opt34r         ROM:40008628 ;       SUBROUTINE         ROM:40008628 ets_efuse_program_opt:       ROM:40008628 ets_efuse_program_opt;         ROM:40008628 ets_efuse_program_opt;       ROM:40008628 ets_efuse_program_opt;         ROM:40008631 memw       memw         ROM:40008634 s321.n , a9, a8, 0       ROM:40008634 s321.n , a9, a8, 0         ROM:40008638 mew       rowi.n , a9, 2         ROM:40008638 mew       ROM:40008638 mew         ROM:40008638 mew       rowi.n , a9, a8, 0         ROM:40008640 loc_40008640:       ; CODE XREF: ets_efuse_program_op+104j         ROM:40008640 loc_40008640:       s321.n , a		ROM:40008618	loc 40008618:				; CODE XREF: ets efuse read op+1D↓j
L ROM:4000861D bnez , a9, loc_40008618 ROM:40008620 ; End of function ets_efuse_read_op ROM:40008620 ; End of function ets_efuse_read_op ROM:40008620 ;		ROM:40008618	-	memw			
ROM:40008620       retw.n         ROM:40008620       ; End of function ets_efuse_read_op         ROM:40008620       ; Dotta ets_efuse_read_op         ROM:40008620       . byte 0         ROM:40008621       . byte 0         ROM:40008622       . byte 0         ROM:40008623       . byte 0         ROM:40008624       .int 0x5A5A         ROM:40008628       ; DATA XREF: ets_efuse_program_op:34r         ROM:40008628       ; DATA XREF: ets_efuse_program_op:34r         ROM:40008628       ; DATA XREF: ets_efuse_program_op:34r         ROM:40008628       entry       , a1, 0x20         ROM:40008628       entry       , a1, 0x20         ROM:40008628       entry       , a8, dword_40008574         ROM:40008628       l32r       , a8, dword_40008574         ROM:40008631       memw       , a9, a8, 0         ROM:40008634       s321.n       , a9, a8, 0         ROM:40008635       s321.n       , a9, a8, 0         ROM:40008640       memw       ; CODE XREF: ets_efuse_program_op+104j         ROM:40008640       memw       ; CODE XREF: ets_efuse_program_op+104j         ROM:40008640       istin , a9, a8, 0       ; ROM:40008640         ROM:40008640       istin , a9, a8, 0       ; ROM:40		ROM:4000861B		132i.n		, a9,	, a8, 0
ROM:40008620 ; End of function ets_efuse_read_op         ROM:40008620 ;         ROM:40008620 ;         ROM:40008620 ;         ROM:40008621 ;         Dyte 0         ROM:40008622 dword_40008624 .int 0x5A5A ;         DATA XREF: ets_efuse_program_op:34r         ROM:40008628 ;         ROM:40008628 ;         ROM:40008628 ;         ROM:40008628 ets_efuse_program_op:         ROM:40008629 ets_efuse_program_op:         ROM:40008629 ets_efuse_program_op:         ROM:40008631 memw         ROM:40008639 movi.n , a9, a8, 0         ROM:40008640 loc_40008640 is:         ROM:40008640 loc_40008640:         ROM:40008640 loc_40008640:         ROM:40008640 loc_40008640:         ROM:40008640 loc_40008640:         ROM:40008640 loc_40008640:         ROM:40008640 loc_4	- L2	ROM:4000861D		bnez		, a9,	loc_40008618
ROM:40008620	•	ROM:40008620		retw.n			-
ROM:40008620 ;       .byte 0         ROM:40008621 .byte 0         ROM:40008623 .byte 0         ROM:40008624 dword_40008624 .int 0x5A5A ; DATA XREF: ets_efuse_program_op+34r         ROM:40008628 ;         ROM:40008628 ;         ROM:40008628 ets_efuse_program_op:         ROM:40008631 memw         ROM:40008636 ll32r , 88, 0         ROM:40008638 memw         ROM:40008638 memw         ROM:40008640 loc_40008640 imemw         ROM:40008640 loc_40008640 memw         ROM:40008640 loc_40008640 memw         ROM:40008643 ll32i.n , 99, a8, 0         ROM:400086443 ll32i.n , 99, a8, 0         ROM:400086448 retw.n		ROM:40008620	; End of function	on ets ef	use_rea	d op	
ROM:40008622       .byte 0         ROM:40008623       .byte 0         ROM:40008624       dword_40008624         ROM:40008624       dword_40008624         ROM:40008628       .int 0x5A5A         ROM:40008631       .int memw         ROM:40008634       .int 0x5A5A         ROM:40008639       .int 0x1, not 0x		ROM:40008620					
RCM:40008623       .byte 0         RCM:40008624       .int 0x5A5A         RCM:40008624       .int 0x5A5A         RCM:40008628         RCM:40008631         memw         RCM:40008634         RCM:40008639         movi.n         RCM:40008639         movi.n         RCM:40008639         meww         RCM:40008639         RCM:40008639         RCM:40008639         RCM:40008639         RCM:40008640         RCM:40008640         RCM:40008640         RCM:40008640         RCM:40008640         RCM:40008640         RCM:40008643         1321.n         , a9, a8, 0         RCM:40008645         bnez         , a9, l		ROM:40008620	;				
ROM:40008624 dword_40008624 .int 0x5A5A       ; DATA XREF: ets_efuse_program_op+34r         ROM:40008628 ;       S U B R O U T I N E         ROM:40008628 ets_efuse_program_op:       ROM:40008628 ets_efuse_program_op:         ROM:40008628 ets_efuse_program_op:       ROM:40008628 ets_efuse_program_op:         ROM:40008628 ets_efuse_program_op:       a9, dword_40008624         ROM:40008628 ets_efuse_program_op:       a9, dword_40008624         ROM:40008628 ets_efuse_program_op:       a9, dword_40008574         ROM:40008631 memw       a9, a8, 0         ROM:40008636 132r       a8, dword_40008576         ROM:40008636 312r       s 232i.n       a9, a8, 0         ROM:40008631 memw       ROM:40008631       s 232i.n         ROM:40008631 32r       s 32i.n       a9, a8, 0         ROM:40008631 32r       s 232i.n       a9, a8, 0         ROM:40008631 size       s 22i.n       a9, a8, 0         ROM:40008640 loc_40008640 size       s CODE XREF: ets_efuse_program_op+104j         ROM:40008640 size       a9, a8, 0         ROM:40008640 size       a9, a8, 0         ROM:40008643 132i.n       a9, a8, 0         ROM:40008643 132i.n       a9, a8, 0         ROM:40008644 cost       a9, a8, 0         ROM:40008643 132i.n       a9, a8, 0         ROM				.byte	0		
ROM:40008628         ROM:40008631         memw         ROM:40008636         ROM:40008638         memw         ROM:40008638         ROM:40008638         ROM:40008638         ROM:40008640         ROM:400086	- 1						
ROM:40008628 ;			dword_40008624	.int 0x5	A5A		; DATA XREF: ets_efuse_program_op+3↓r
ROM:40008628         ROM:40008628         ROM:40008628         ROM:40008628         entry       , a1, 0x20         ROM:40008628       arry         ROM:40008628       132r         ROM:40008628       132r         ROM:40008628       132r         ROM:40008621       memw         ROM:40008631       memw         ROM:40008634       s32i.n         ROM:40008639       movi.n         ROM:40008638       memw         ROM:40008638       memw         ROM:40008638       s32i.n         ROM:40008638       s32i.n         ROM:40008638       s32i.n         ROM:40008640       c_40008640         ROM:40008640       s32i.n         ROM:40008640       s32i.n         ROM:40008640       s32i.n         ROM:40008640       s2i.n         ROM:40008640       s2i.n         ROM:40008640       s2i.n         ROM:40008640       s2i.n         ROM:40008640       s2i.n         ROM:40008640       s2i.n         ROM:40008640       s32i.n         ROM:40008640       s32i.n         ROM:400086640       s32i.n							
ROM:40008628         ROM:40008628 ets_efuse_program_op:         ROM:40008621 ets_efuse_program_op:         ROM:40008631 memw         ROM:40008636 ets_program_op:         ROM:40008638 memw         ROM:40008638 memw         ROM:40008640 loc_40008640 toc_40008640         ROM:40008640 loc_40008640 toc_40008640         ROM:40008640 loc_40008640 toc_40008640 toc_40008640 toc_40008640         ROM:40008640 toc_40008640 toc_40008640 toc_8008640         ROM:40008640 toc_40008640 toc_9008640 toc_9008640         ROM:40008640 toc_40008640 toc_9008640 toc_9008640         ROM:40008640 toc_9008640 toc_9008640         ROM:40008640 toc_9008640 toc_9008640         ROM:40008640 toc_9008640 toc_9008640         ROM:40008640 toc_9008640 toc_9008640         ROM:400008640			;	== S U B	ROUT	IN	E
ROM:40008628 ets_efuse_program_op:         ROM:40008628 ets_efuse_program_op:         ROM:40008628 ll32r , 99, dword_40008624         ROM:40008628 ll32r , 99, dword_400085F4         ROM:40008631 memw         ROM:40008636 ll32r , 99, a8, 0         ROM:40008638 memw         ROM:40008638 memw         ROM:40008638 memw         ROM:40008638 memw         ROM:40008638 memw         ROM:40008640 loc_40008640 is s321.n , 99, a8, 0         ROM:40008640 loc_40008640 memw							
RCM:40008628       entry       , a1, 0x20         RCM:40008628       132r       , a9, dword_40008624         RCM:40008628       132r       , a8, dword_400085F4         RCM:40008631       memw       , a8, dword_400085F4         RCM:40008634       532i.n       , a9, a8, 0         RCM:40008636       132r       , a8, dword_400085FC         RCM:40008639       movi.n       , a9, 2         RCM:40008631       s32i.n       , a9, a8, 0         RCM:40008640       loc_40008640       ; CODE XREF: ets_efuse_program_op+104j         RCM:40008643       132i.n       , a9, a8, 0         RCM:40008643       loc_13i.n       , a9, a8, 0         RCM:40008643       loc_40008643       loc_40008643         RCM:40008643       loc_12i.n       , a9, a8, 0         RCM:40008643       loc_12i.n       , a9, loc_40008640         RCM:40008643       loc_12i.n       , a9, loc_40008640         RCM:40008643       loc_12i.n       , a9, loc_40008640							
ROM:4000862B       132r       , a9, dword_40008624         ROM:40008621       132r       , a8, dword_400085F4         ROM:40008631       memw         ROM:40008634       s32i.n       , a9, a8, 0         ROM:40008636       132r       , a8, dword_400085FC         ROM:40008639       movi.n       , a9, 2         ROM:40008631       memw       ROM:40008638         ROM:40008631       memw       ROM:40008640         ROM:40008640       s32i.n       , a9, a8, 0         ROM:40008640       nc_40008640       remw         ROM:40008640       nc_40008640       nc_40008640         ROM:40008640       loc_40008640       nc         ROM:40008643       132i.n       , a9, a8, 0         ROM:40008645       bnez       , a9, loc_40008640         ROM:40008648       retw.n	•					- 1	020
ROM:4000862E       132r       , a8, dword_400085F4         ROM:40008631       memw         ROM:40008634       s32i.n       , a9, a8, 0         ROM:40008636       132r       , a8, dword_400085FC         ROM:40008638       memw         ROM:40008638       memw         ROM:40008638       memw         ROM:40008640       s32i.n       , a9, a8, 0         ROM:40008640       loc_40008640       s32i.n         ROM:40008640       loc_40008640       is code in the immw         ROM:40008640       memw       go a8, 0         ROM:40008643       132i.n       , a9, a8, 0         ROM:40008645       bnez       , a9, loc_40008640         ROM:40008648       retw.n	•						
ROM:40008631       memw         ROM:40008634       s32i.n         ROM:40008636       l32r         ROM:40008636       l32r         ROM:40008636       movi.n         ROM:40008638       memw         ROM:40008638       s32i.n         ROM:40008638       s32i.n         ROM:40008640       memw         ROM:40008640       memw         ROM:40008643       l32i.n         ROM:40008645       bnez         ROM:40008645       bnez         ROM:40008648       retw.n	•						
ROM:40008634       s32i.n       , a9, a8, 0         ROM:40008634       132r       , a8, dword_400085FC         ROM:40008639       movi.n       , a9, 2         ROM:40008638       memw         ROM:40008631       s32i.n       , a9, a8, 0         ROM:40008632       s32i.n       , a9, a8, 0         ROM:40008640       loc_40008640       remw         ROM:40008640       loc_40008640       loc_40008640         ROM:40008640       loc_40008640       s32i.n         ROM:40008640       loc_40008640       s32i.n         ROM:40008640       loc_40008640       s40008640         ROM:40008643       l32i.n       , a9, loc_40008640         ROM:40008648       retw.n       s40, a9, loc_40008640	•					, ao,	, unoi u_4000001 4
ROM:40008636       132r       , a8, dword_400085FC         ROM:40008639       movi.n       , a9, 2         ROM:40008638       memw         ROM:40008640       s32i.n       , a9, a8, 0         ROM:40008640       loc_40008640       ; CODE XREF: ets_efuse_program_op+1D4j         ROM:40008643       132i.n       , a9, a8, 0         ROM:40008645       bnez       , a9, loc_40008640         ROM:40008648       retw.n	•					a9.	
ROM:40008639       movi.n       , a9, 2         ROM:4000863B       memw         ROM:4000863E       s32i.n       , a9, a8, 0         ROM:40008640       loc_40008640       ; CODE XREF: ets_efuse_program_op+1D4j         ROM:40008640       memw         ROM:40008643       132i.n       , a9, a8, 0         ROM:40008645       bnez       , a9, loc_40008640         ROM:40008645       bnez       , a9, loc_40008640	•						
ROM:4000863B       memw         ROM:4000863B       s32i.n         ROM:4000863C       s32i.n         ROM:40008640       s32i.n         ROM:40008640       s32i.n         ROM:40008640       s32i.n         ROM:40008640       memw         ROM:40008640       memw         ROM:40008643       l32i.n         BOM:40008645       bnez         ROM:40008648       retw.n	•						
ROM:40008640       ; CODE XREF: ets_efuse_program_op+1D4j         ROM:40008640       memw         ROM:40008643       132i.n         ROM:40008645       bnez         ROM:40008645       cale         ROM:40008645       bnez         ROM:40008648       retw.n	•					,,	-
ROM:40008640       ; CODE XREF: ets_efuse_program_op+1D+j         ROM:40008640       memw         ROM:40008643       132i.n         ROM:40008645       bnez         a9, a8, 0         ROM:40008645       bnez         ROM:40008648       retw.n	•	ROM:4000863E		s32i.n		. a9.	, a8, 0
Point         Rown:40008640         memw           Rown:40008643         132i.n         , a9, a8, 0           L         Rown:40008645         bnez         , a9, loc_40008640           Rown:40008648         retw.n		ROM:40008640					
ROM:40008643     132i.n     , a9, a8, 0       ROM:40008645     bnez     , a9, loc_40008640       ROM:40008648     retw.n		ROM:40008640	loc 40008640:				; CODE XREF: ets efuse program op+1D↓j
ROM:40008645 bnez , a9, loc_40008640 retw.n				memw			
ROM: 40008648 retw.n	•	ROM:40008643		132i.n		, a9,	, a8, 0
	- L 🛃	ROM:40008645		bnez		, a9,	, loc_40008640
	•	ROM:40008648		retw.n			
ROM:40008648 ; End of function ets_efuse_program_op		ROM:40008648	; End of function	on ets_ef	use_pro	gram_	_op

### Special Boot Mode

- Special Boot Mode (Download\_Boot)
  - Management mode to Flash FW, and Set E-Fuses
  - IOO connected to GND then Power-up

rst:0x10 (RTCWDT\_RTC\_RESET),boot:0x21 (DOWNLOAD\_BOOT(UART0/UART1/SDI0\_FEI\_RE0\_V)
waiting for download

- Esptool is python utility to communicate with the ROM functions
  - Dedicated commands available from UARTO to deal with E-Fuses
    - dump, program,...

### **E-Fuses** Protection

#### •Any attempt to read BLK1 or BLK2 returns $0 \times 00$

#### • \$ espefuse.py --port /dev/ttyUSB0 dump

Identification of R/W Protection bits in BLK0
 00130180 = 00000000 00010011 00000001 1000 0000
 These two bits are the Read protection bits

### ZERO 2019 EDITION

### NGHTS Wait LR, where is the Vuln?

- I Have no vuln here...
- But I know
  - BootROM does not manage the E-Fuses
  - Obviously, E-Fuses Controller does the job before
  - Special boot mode called 'Download Boot'
  - Read protection bits have been identified
- •The idea

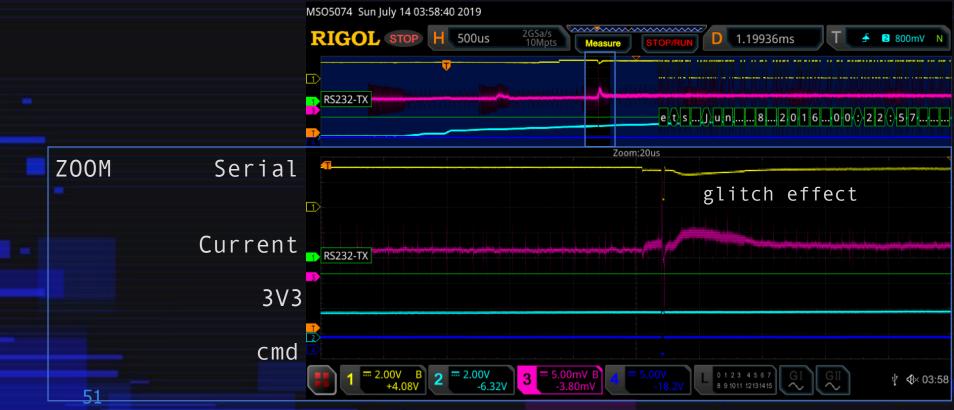
50

- Glitch the E-Fuses Controller initialization to modify the R/W protections
- Then send Dump command in Special Mode
- And get back BLK1 (FEK) and BLK2 (SBK)

### FATAL Attack

ZERONIGHTS.ORG

# Simple Power Analysis on VDD\_CPU to identify Glitch during this identified HW process



### FATAL Results

#### • PoC sent to vendor (on July 24)

Pulse delay = 0.001201670

### One more step

- Sadly, the dumped Keys are not exactly True values
  - Remember I burned the keys 😊
- •Offline Statistical Analysis on 30-50 dumped key values
  - just Keep the most recurrent Bytes (here SBK analysis)
- 1 Byte still unknown and has to be Brute Forced (worst case)
  - Same for FEK

2 3 4 5 e94f5bc2 00370f91 7c897429 2eadd23b c7664f05 5ae3365f d3781029 82e25c4c e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c98 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c98 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c9c e94f5bc2 00370f91 7c89f029 2eadd23b c7664f10 bfe3365f d3781029 82e25c64 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25ce4 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f09 b7e3365f d3781029 82e25cc8 e94f5bc2 00370f91 7c89e029 2eadd23b c7664f04 bbe3365f d3781029 82e25c64 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25ccc e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c1c e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c98 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f08 b6e3365f d3781029 82e25c98 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c9a e94f5bc2 00370f91 7c89e829 2eadd23b c7664f08 b7e3365f d3781029 82e25c62 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0b b6e3365f d3781029 82e25c8c e94f5bc2 00370f91 7c89e829 2eadd23b c7664f09 b7e3365f d3781029 82e25cc8 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c64 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f09 bfe3365f d3781029 82e25cc8 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c98 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c80 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c9a e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c9a e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25ce4 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f08 b7e3365f d3781029 82e25c64 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f08 b7e3365f d3781029 82e25c0c e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25ca4 e94f5bc2 00370f91 7c89e029 2eadd23b c7664f01 bfe3365f d3781029 82e25cc8 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c9c e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c06 e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25cef e94f5bc2 00370f91 7c89f429 2eadd23b c7664f09 fee3365f d3781029 82e25c4c

Appearance 100%	Rate: 100%	100%	100%	60%	60%	100%	0%(1	Byte	by	BF )

Real Secure Boot Key:

e94f5bc2 00370f91 7c89e829 2eadd23b c7664f0a b5e3365f d3781029 82e25c99

### FATAL Exploit step 1: Decrypt FW

- Dump the encrypted FW
  - By Download Mode or by dumping the Flash Content
- Perform FATAL Glitch to extract FEK/SBK values
  - Run Statistical analysis

#### • Confirm the True FEK (by decrypting FW)

limited@linux:~/esp/bin\_decrypt\_dump\$ espsecure.py decrypt\_flash\_data --keyfile my\_dumped\_ fek.bin --output decrypted.bin --address 0x0 flash\_contents.bin espsecure.py v2.7-dev Using 256-bit key

limited@linux:~/esp/bin\_decrypt\_dump\$ strings decrypted.bin | grep Hello
Hello from SEC boot K1 & FE !

#### • IMPORTANT to respect this byte order in key.bin

limited@linux:~/esp/bin\_decrypt\_dump\$ hexdump -C my\_dumped\_fek.bin 000000000 38 c8 75 e3 33 76 41 15 f9 5f 65 43 dd f2 e9 2c |8.u.3vA..\_eC...,| 00000010 78 1f a0 42 53 bf 14 8f ce 68 9f 00 86 55 52 9b |x..BS....h...UR.|

### FATAL Exploit step 2: Sign Your Code

- Firmware is now decrypted
- dd ivt.bin (the first 128 random bytes at 0x00 in decrypted.bin)
- •dd Bootloader.bin at 0x1000
- Confirm the true SBK
  - digest computation command
- •Write your Code
  - a little FW backdoor maybe? ©
- Compile images
  - using FEK and SBK
- •Flash new FW

limited@linux:~/esp/bin_decrypt_dump\$ hexdump -C -n 192 decrypted.bin
00000000 bd 84 e7 f2 39 b8 8f 55 fb d9 48 9b 26 c8 c2 d3 j9UH.&
00000010 9c 13 72 d9 5a 77 94 0d 67 ed 2d 48 fc 69 aa 5f [r.ZwgH.i]
00000020 0d 1c 4d ef 67 ec a1 43 d3 3a 67 86 9f e3 e3 58 [M.gC.:gX]
00000030 9a 80 85 31 b7 9f cb 27 ad 35 e0 bb 2f 93 8d 79  1'.5/y
00000040 22 5e e5 22 ca e1 eb 9c 2e 4d d8 93 fc 97 66 5a  "^."MfZ
00000050 4b 58 8c 24 a9 04 78 e4 45 99 94 37 3d b6 4b 7f [KX.\$x.E7=.K.]
00000060 70 d4 df 56 7f 1f b8 52 24 0c 0d 45 22 e1 d1 d5  pVR\$E"
00000070 cf 2d 85 2b e9 f1 01 9d 04 88 5c bf 17 ab b6 2f   _ +/
_00000080 b5 a5 82 70 5c 3e 1e 25  44 30 92 84 d0 13 a4 bc   p\>.%D0
00000090 b0 d4 ee 63 01 ee a0 d5 72 07 91 51 67 82 a8 8d  crQg
000000a0 6c a5 2a 1e 5e 39 29 d7 60 1b 9d 22 3e dc f4 64  l.*.^9).`">d
<u>000000b0 6f c7 bf 2e ba a7 9a bf 24 4b dc d0 fc 87 ee bb  o\$K </u>
00000000
<pre>limited@linux:~/esp/bin_decrypt_dump\$ espsecure.py digest_secure_bootloaderkey</pre>
ile my_dumped_sbk.biniv ivt.bin bootloader.bin
espsecure.py v2.7-dev
WARNING:iv argument is for TESTING PURPOSES ONLY
Using 256-bit key
digest+image written to bootloader-digest-0x0000.bin
limited@linux:~/esp/bin_decrypt_dump\$ hexdump -C -n 192 bootloader-digest-0x0000.
00000000 bd 84 e7 f2 39 b8 8f 55 fb d9 48 9b 26 c8 c2 d3  9UH.&
00000010 9c 13 72 d9 5a 77 94 0d 67 ed 2d 48 fc 69 aa 5f [r.ZwgH.i]
00000020 0d 1c 4d ef 67 ec a1 43 d3 3a 67 86 9f e3 e3 58  M.gC.:gX
00000030 9a 80 85 31 b7 9f cb 27 ad 35 e0 bb 2f 93 8d 79  1'.5/y  00000040 22 5e e5 22 ca e1 eb 9c 2e 4d d8 93 fc 97 66 5a  "^."MfZ
00000040 22 5e e5 22 ca e1 eb 9c 2e 4d d8 93 fc 97 66 5a  "^."MfZ  00000050 4b 58 8c 24 a9 04 78 e4 45 99 94 37 3d b6 4b 7f  KX.\$x.E7=.K.
000000060 70 d4 df 56 7f 1f b8 52 24 0c 0d 45 22 e1 d1 d5 [pVR\$E"]
00000000 cf 2d 85 2b e9 f1 01 9d 04 88 5c bf 17 ab b6 2f 1+
000000080 b5 a5 82 70 5c 3e 1e 25 44 30 92 84 d0 13 a4 bc  p\>.%D0
000000090 b0 d4 ee 63 01 ee a0 d5 72 07 91 51 67 82 a8 8d  c
0000000a0 6c a5 2a 1e 5e 39 29 d7 60 1b 9d 22 3e dc f4 64 [l.*.^9).`">d
0000000b0 6f c7 bf 2e ba a7 9a bf 24 4b dc d0 fc 87 ee bb [0\$K]
<pre>limited@linux:~/esp/bin_decrypt_dump\$ hexdump -C my_dumped_sbk.bin</pre>
00000000 82 e2 5c 99 d3 78 10 29 b5 e3 36 5f c7 66 4f 0a  \x.)6f0.
00000010 2e ad d2 3b 7c 89 e8 29 00 37 0f 91 e9 4f 5b c2  ; ).70[.]
00000020

### **OTP/EFuses FATAL Conclusion**

- FATAL exploit leading to SBK & FEK extraction
  - Breaking Secure Boot and Flash Encryption
- •An attacker can decrypt the Firmware (access IP and sensitive data)
- An attacker can sign & run his own (encrypted) code PERSISTENTLY
- •Low Cost, Low Complexity
- Easy to reproduce
- •No Way to fix
- All ESP32 versions vulnerable

### Vendor Reaction

#### • Resp. disclosure

- PoC sent on July 24
- CVE-2019-17391 (req. by Vendor)
- Disclosure Today

# The ESP32-D0WD-V3 chip has checks in ROM which prevent fault injection attack. This chip and related modules will be available in Q4 2019. More information about ESP32-D0WD-V3 will be released soon.

## Security Advisory on November 1 [7]No way to Fix but...

• They propose to buy their new chip version 😊 😊 😊

- Millions of vulnerable Devices on the field for the coming years
- What about devices offered for sales? Who want broken platforms?

### Final Conclusion

• Developers are Now aware

• Attacker with physical access can compromise ESP32 security badly

• Fix?

- No fix on current ESP32 version
- Chip is broken FOREVER
- •I identified several companies using Esp32 security features in their products...
- General Message for Vendors
  - Don't patch silently, Reward instead
- •New Results coming soon
  - Stay tuned ;)



### References & Credits

- Fatal Fury Animations
  - www.fightersgeneration.com
- •Espressif
  - [1] Espressif 100-Millions chip shipments
- •ESP32
  - [2] <u>Datasheet</u>, <u>TRM</u>
- Fault injection references
  - [3] Chris Gerlinsky (@akacastor)
  - [4] <u>Colin O'Flynn</u> (@colinoflynn)
- •Xtensa
  - [5] <u>ISA Manual</u>
- •LIFX Pwn
  - [6] <u>LIFX Pwn</u>
- Security Advisory
  - [7] <u>CVE-2019-17391</u>

# Thank you!

#### @LimitedResults