Estrazione e Analisi Statica del Firmware in dispositivi IoT

Luca Bongiovanni

La sicurezza del firmware

- Il firmware è un programma memorizzato sul dispositivo per il quale è stato specificatamente creato
- Esistono due tipologie di firmware
  - firmware semplici: composti da un unico file binario eseguibile
  - firmware complessi: composti da un sistema operativo ed un filesystem
- Più i dispositivi «intelligenti» si diffondono ed investono un ruolo sempre più importante, più è necessario che i firmware di tali dispositivi siano sicuri:
  - Contengono sempre più informazioni confidenziali
  - Sono collocati in posizioni privilegiate

L’analisi del firmware

- Vi è la necessità di analizzare il firmware per verificare la presenza di eventuali vulnerabilità al suo interno
- Due metodologie di analisi:
  - Analisi statica: si esplora la struttura del filesystem (nel caso di firmware complessi) e si analizza il codice dei programmi presenti
  - Analisi dinamica: si analizza la sicurezza del dispositivo mentre è in esecuzione tramite un’emulazione del firmware
- Uno dei progetti della fondazione OWASP, il *Firmware Security Testing Methodology,* stila un procedimento composto da nove passaggi atto ad eseguire correttamente un test della sicurezza di un firmware

L’acquisizione del firmware

Metodi Software

Basati sugli aggiornamenti:

- Download di un aggiornamento dalla pagina web del produttore
- Analizzare il traffico di rete durante un aggiornamento

✓ Non richiedono un accesso fisico al dispositivo

× Non sempre fattibili (connessione sicura, diff file)

Metodi Hardware

Basati principalmente sulle interfacce di debug:

- UART
- JTAG
- Estrazione diretta dalla memoria

✓ Fattibili nella maggior parte dei casi

× Richiedono un accesso fisico al dispositivo e attrezzature particolari

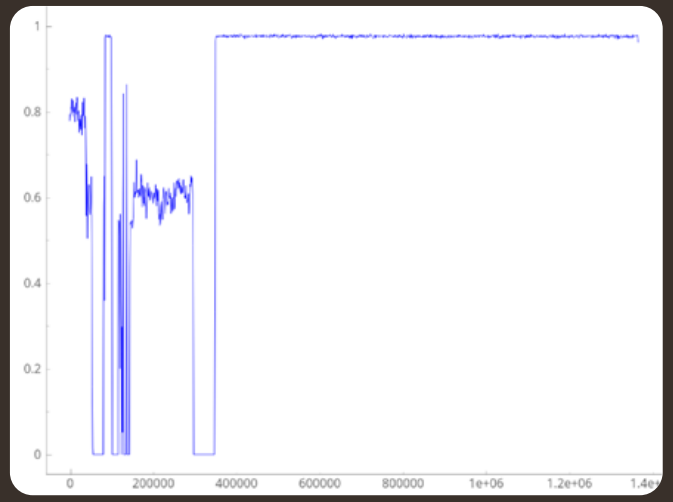
L’ispezione del firmware

All’inizio dell’analisi si utilizzano vari strumenti per ispezionare il firmware, in particolare per:

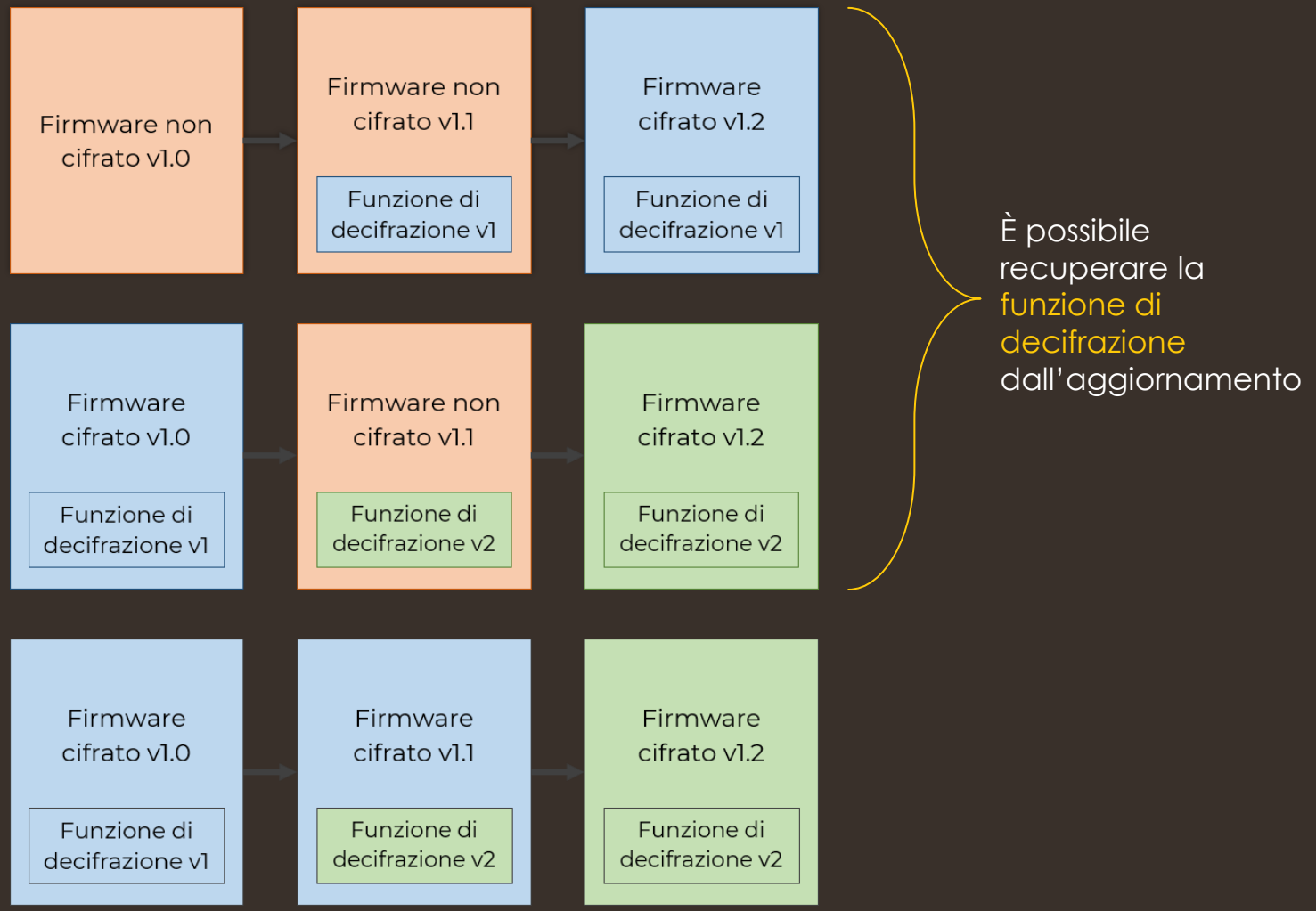
- Visualizzare il contenuto (hexdump, strings): permettono di visualizzare il contenuto del file in vari formati (esadecimale, decimale, ASCII, ecc.) o di mostrare esclusivamente le sequenze di caratteri stampabili
- Identificare il contenuto (file, binwalk): permettono di identificare il tipo di uno o più file eseguendo dei test basati sui *magic numbers*
- Visualizzare graficamente i file binari (binvis.io): permettono di visualizzare l’intero file binario come un’immagine evidenziando con colori diversi porzioni diverse del file (byte nulli, ASCII, ecc.)

La cifratura del firmware

- È possibile identificare la presenza di cifratura tramite il calcolo dell'entropia del firmware
- Ad un valore molto alto corrisponde probabilmente una cifratura
- ! Anche alla compressione corrisponde un valore alto, possono confondersi!



Gli scenari di cifratura

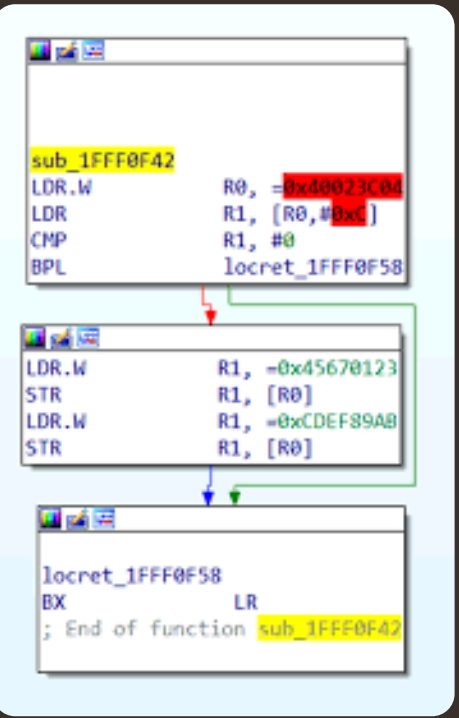


I firmware semplici

- Si risale al codice sorgente tramite l'uso di disassemblatori e decompilatori

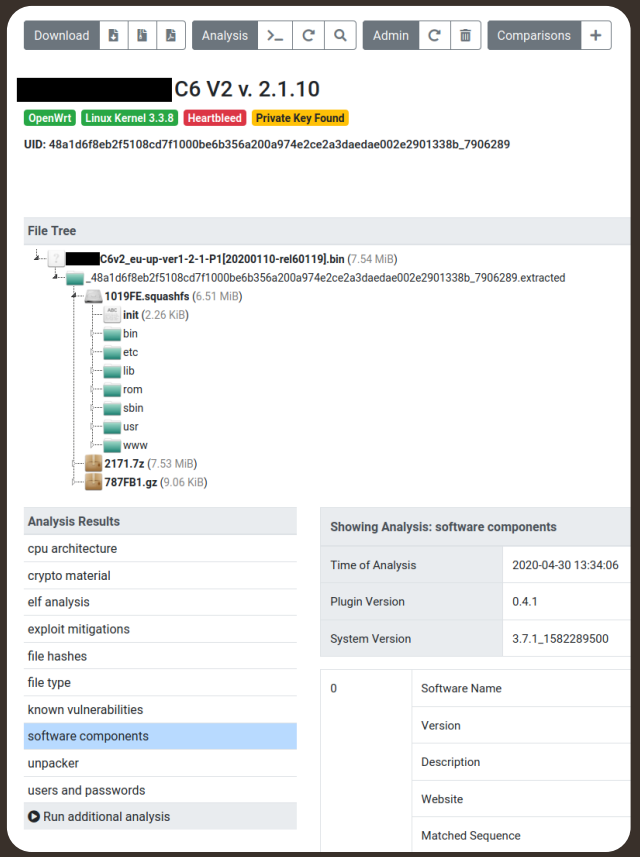
- Non sempre fattibile a causa di:
  - Offuscamento del codice
  - Ottimizzazione del compilatore
  - Stripped binary

- Si utilizzano strumenti grafici che agevolano il processo di analisi:
  - Visualizzazione a grafo delle funzioni
  - Possibilità di commentare/rinominare vari elementi(variabili, funzioni, ecc.)
  - Rilevazione della presenza di librerie conosciute nel caso di stripped binary



I firmware complessi

- Ricerca delle vulnerabilità più comuni all'interno del filesystem:
  - Demoni di rete insicuri (telnet, ecc.)
  - Credenziali hardcoded (username, password, chiavi SSH, ecc.)
  - Analisi dei codici sorgenti e di quelli compilati
  - …
- Possibile automatizzazione tramite appositi strumenti



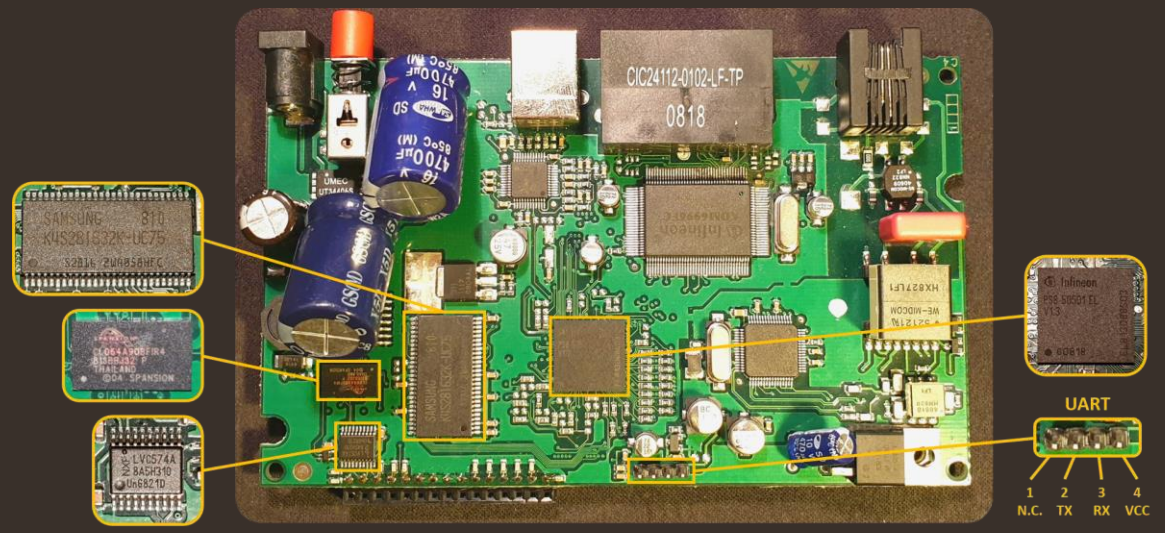
Alice Gate 2 Plus

1 Raccolta delle informazioni

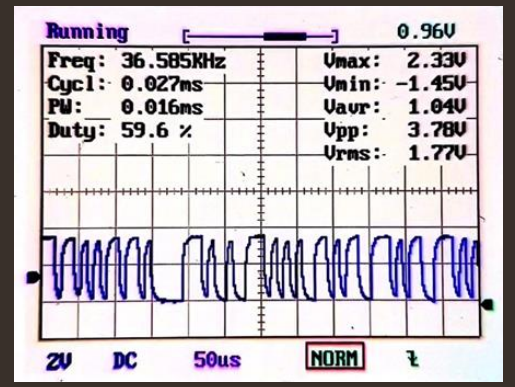
- ✗ Nessuna pagina di download aggiornamenti
- ✗ Impossibile intercettare un aggiornamento
- ✗ Nessuna pagina informativa
- ✓ Pin allineati buoni candidati ad essere la UART

2 Individuazione UART

- Per ogni pin si misura la sua resistenza con GND e Vcc, e la sua tensione
- Si individua il pin di trasmissione grazie l'ausilio di un oscilloscopio (o logic analyzer)



Pin	R_{GND} (Ω)	R_{Vcc} (Ω)	V (V)	Note
1	∞	∞	0	N.C.
2	1.39K	1.52K	3.36	Sospetto TX
3	1.37K	1.48K	3.33	
4	104.5	0	3.37	V_{CC}



3 Estrazione del firmware

- Ci si connette all'interfaccia seriale individuando la corretta velocità di trasmissione (l'unica che restituisce un output leggibile)
- Si analizza il processo di boot per recuperare maggiori informazioni sul dispositivo

```
Version 1.0.1
Read EEPROM
Jump to Flash
Head : Amazon Version 1.0.0
DRAM:  16 MB

 Head : relocate_code start
Head: relocate code finish.
   Image Name:   u-boot image
   Image Type:   MIPS Linux Firmware (lzma compressed)
   Data Size:    40672 Bytes = 39.7 kB
   Load Address: 80100000
   Entry Point:  80100000
Disabling all the interrupts
   Uncompressing UBoot Image ...
   Uncompression completed successfully with destLen 124144.
 Head: Jumping to u-boot in the ram at 0x80100000
Infineon Amazon
U-Boot 2.0.16-16 (Jun 19 2008 - 17:51:23)
In env_init : env_ptr = 0xb37c0000
For enviornment CRC32 is OK
Board: AMAZON Yangtse Version, Chip V1.3, CPU Speed 235 MHz
IDF LED fix ... done
DRAM:  16 MB
USB support: 48Mhz clock enabled

 relocate_code start
 relocate code finish

Entering flash_init()
detected SPANSION S29GL064A

IDF-FLASH fix...done
Flash:  8 MB
env_relocate[228] malloced ENV at 80aa0008
```

```
AMAZON-DIALFACE # flinfo

Bank # 1: AMD S29GL064A (64 Mbit)
  Size: 8 MB in 135 Sectors
  Sector Start Addresses:
    B3000000      B3002000      B3004000      B3006000      B3008000
    B300A000      B300C000      B300E000      B3010000      B3020000
    B3030000      B3040000      B3050000      B3060000      B3070000
    B3080000      B3090000      B30A0000      B30B0000      B30C0000
    B30D0000      B30E0000      B30F0000      B3100000      B3110000
    B3120000      B3130000      B3140000      B3150000      B3160000
    B3170000      B3180000      B3190000      B31A0000      B31B0000
    B31C0000      B31D0000      B31E0000      B31F0000      B3200000
    B3210000      B3220000      B3230000      B3240000      B3250000
    B3260000      B3270000      B3280000      B3290000      B32A0000
    B32B0000      B32C0000      B32D0000      B32E0000      B32F0000
    B3300000      B3310000      B3320000      B3330000      B3340000
    B3350000      B3360000      B3370000      B3380000      B3390000
    B33A0000      B33B0000      B33C0000      B33D0000      B33E0000
    B33F0000      B3400000      B3410000      B3420000      B3430000
    B3440000      B3450000      B3460000      B3470000      B3480000
    B3490000      B34A0000      B34B0000      B34C0000      B34D0000
    B34E0000      B34F0000      B3500000      B3510000      B3520000
    B3530000      B3540000      B3550000      B3560000      B3570000
    B3580000      B3590000      B35A0000      B35B0000      B35C0000
    B35D0000      B35E0000      B35F0000      B3600000      B3610000
    B3620000      B3630000      B3640000      B3650000      B3660000
    B3670000      B3680000      B3690000      B36A0000      B36B0000
    B36C0000      B36D0000      B36E0000      B36F0000      B3700000
    B3710000      B3720000      B3730000      B3740000      B3750000
    B3760000      B3770000      B3780000      B3790000      B37A0000
    B37B0000      B37C0000      B37D0000      B37E0000      B37F0000
```

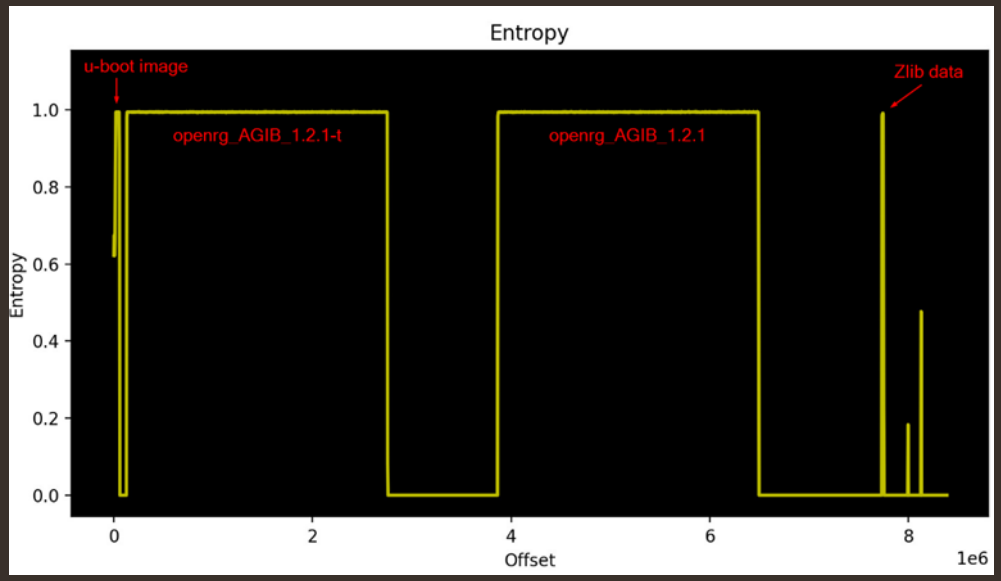
- ✗ Nessun prompt di accesso al termine del processo di boot
- ✓ Possibilità di interrompere il boot e di accedere al bootloader
  - Si controlla la lista dei comandi eseguibili

```
b3000000: 10 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00    ................
b3000010: 68 8c 68 8c 00 00 00 00 00 00 00 00 00 00 00 00    h.h.............
b3000020: 40 80 90 00 40 80 98 00 40 1a 60 00 24 1b ff fe    @...@...@.`.$...
b3000030: 03 5b d0 24 40 9a 60 00 40 80 68 00 40 80 48 00    .[.$@.`.@.h.@.H.
b3000040: 40 80 58 00 24 08 00 02 40 88 80 00 04 11 00 02    @.X.$...@.......
b3000050: 00 00 00 00 00 00 4c 3c 03 e0 e0 21 8f e9 00 00    ......L<...!....
b3000060: 03 89 e0 20 8f 99 00 94 00 00 00 00 03 20 f8 09    ... ......... ..
b3000070: 00 00 00 00 8f 99 00 f4 00 00 00 00 03 20 f8 09    ............. ..
b3000080: 00 00 00 00 24 08 00 03 40 88 80 00 8f 99 00 98    ....$...@.......
b3000090: 03 20 f8 09 00 00 00 00 3c 08 9f c0 35 08 10 00    . ......<...5...
b30000a0: 25 1d 00 00 8f 99 01 04 03 20 00 08 00 00 00 00    %........ ......
b30000b0: 8f 99 00 44 03 20 f8 09 00 00 00 00 03 e0 00 08    ...D. ..........
b30000c0: 00 80 c8 21 03 20 00 08 00 00 00 00 00 80 40 21    ...!. ........@!
b30000d0: 00 a0 48 21 3c 01 00 02 01 01 50 20 8d 0b 00 00    ..H!<.....P ....
b30000e0: ad 2b 00 00 25 08 00 04 01 48 08 2a 10 20 ff fb    .+..%....H.*. ..
b30000f0: 25 29 00 04 00 00 00 00 03 e0 00 08 00 00 00 00    %).............
b3000100: 00 80 e8 21 03 80 70 21 3c 01 b3 00 03 81 e0 22    ...!..p!<......"
b3000110: 03 86 e0 20 03 8e 70 22 3c 08 b3 00 21 0a 4d e0    ... ..p"<...!.M.
b3000120: 00 c0 48 21 8d 0b 00 00 ad 2b 00 00 25 08 00 04    ..H!.....+..%...
b3000130: 01 48 08 2a 10 20 ff fb 25 29 00 04 20 c8 01 54    .H.*. ..%).. ..T
b3000140: 01 00 00 08 00 00 00 00 b3 00 4d c0 b3 00 4d f0    ..........M...M.
b3000150: 00 00 00 4c 8d 0b ff fc 23 8c 00 08 24 0a 00 02    ...L....#...$...
b3000160: 8d 89 00 00 11 20 00 02 01 2e 48 20 ad 89 00 00    ..... ....H ....
b3000170: 21 4a 00 01 01 4b 08 2a 14 20 ff f9 21 8c 00 04    !J...K.*. ..!...
b3000180: 8d 09 ff f4 8d 0a ff f8 01 2e 48 20 01 4e 50 20    ..........H .NP
b3000190: 21 29 ff fc 21 29 00 04 01 2a 08 2a 54 20 ff fd    !)..!)...*.*T ..
b30001a0: ad 20 00 00 00 a0 20 21 8f 99 00 24 03 20 00 08    . .... !...$. ..
b30001b0: 00 c0 28 21 10 00 ff ff 10 00 ff ff 00 00 00 00    ..(!............
b30001c0: 3c 08 b0 10 35 08 53 00 3c 09 13 00 35 29 00 31    <...5.S.<...5).1
b30001d0: ad 09 00 20 3c 09 14 00 35 29 00 31 ad 09 00 24    ... <...5).1...$
b30001e0: 3c 09 18 00 35 29 00 30 ad 09 00 28 3c 09 1c 00    <...5).0...(<...
b30001f0: 35 29 00 60 ad 09 00 2c 3c 09 00 01 35 29 d7 ff    5).`...,<...5)..
b3000200: ad 09 00 60 ad 09 00 64 3c 08 bf 80 24 09 00 02    ...`...d<...$...
```

4 Analisi del firmware

```
bongio  PC-LUCA  ../firmware dump  binwalk alice.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
16368         0x3FF0          U-Boot version string, "U-Boot 2.0.16-16 (Jun 19 2008 - 17:51:45)"
17632         0x44E0          CRC32 polynomial table, big endian
19936         0x4DE0          uImage header, header size: 64 bytes, header CRC: 0x25BFFA15, created: 2008-06-19 15:51:45, image size: 4
0672 bytes, Data Address: 0x80100000, Entry Point: 0x80100000, data CRC: 0x65DE756C, OS: Linux, CPU: MIPS, image type: Firmware Image,
compression type: lzma, image name: "u-boot image" 1
20000         0x4E20          LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 124144 bytes13
1220        0x20094         uImage header, header size: 64 bytes, header CRC: 0xE90E64B, created: 2008-03-28 11:28:55, image size: 2625
539 bytes, Data Address: 0x80002000, Entry Point: 0x80003D50, data CRC: 0xE43A00E6, OS: Linux, CPU: MIPS, image type: OS Kernel Image,
compression type: lzma, image name: "openrg_AGIB_1.2.1-t" 2
131284        0x200D4         LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 4083712 bytes
3866772       0x3B0094        uImage header, header size: 64 bytes, header CRC: 0x58A60386, created: 2008-03-26 17:48:43, image size: 2
626643 bytes, Data Address: 0x80002000, Entry Point: 0x80003D50, data CRC: 0x51D75F52, OS: Linux, CPU: MIPS, image type: OS Kernel Imag
e, compression type: lzma, image name: "openrg_AGIB_1.2.1" 3
3866836       0x3B00D4        LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 4083712 bytes
7733400       0x760098        Zlib compressed data, default compression
```



Dal firmware estratto si nota che:

- Sono presenti tre immagini di boot
- È presente una partizione di dati compressa
- Il firmware non pare essere stato cifrato

All'interno della partizione compressa vi è una file di configurazione contenente:

- Certificati
- Una chiave privata RSA
- Delle password cablate che sono state offuscate

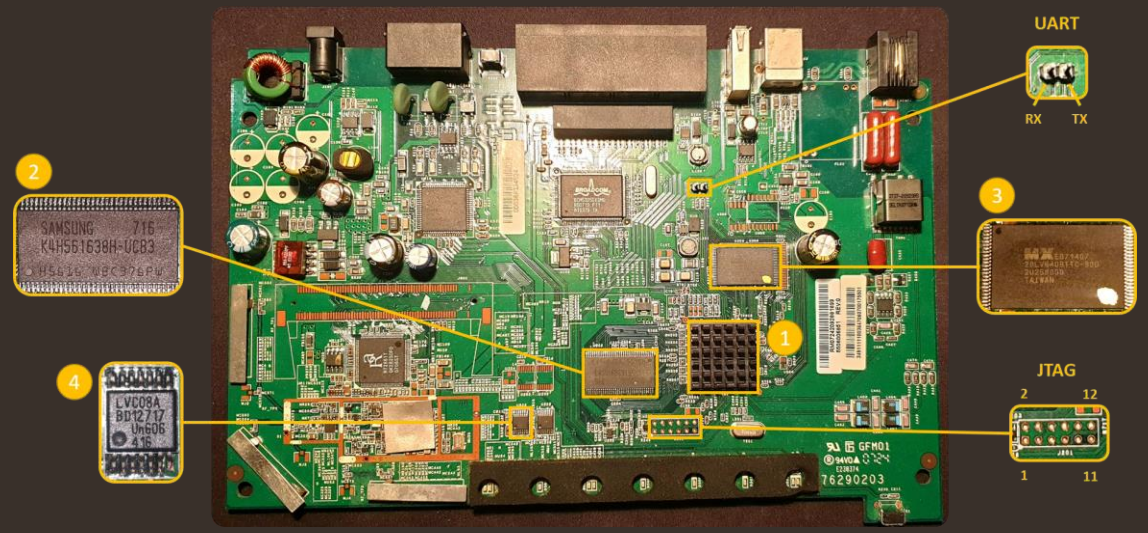
```
bongio  PC-LUCA  ../_760000.bin.extracted  grep password 98
        (password(&b7;`X&b3;&99;&18;T&e2;&b6;&b2;))
          (password(&b7;X&5c;&b9;&a2;))
      (password(&9f;+#&b6;&a6;&df;c&9d;&be;&ba;u&a0;&05;8&ae;&28;F&07;t&0c;&ff;&0c;&fe;&cf;))
      (conn_req_password())
```

```
bongio  PC-LUCA  ../_760000.bin.extracted  cat private_key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA8RXUWwdDD5yx4iq3bcfVz5gB8wPudE6X7NxgN+/0dSm5/fGt
eoeTQAO9t9qhZmqoe/1w9SwRSzdAzS2T9+K0SbXou1jl2N8xWCThymQOgO+shPyt
2NeegBgLIhQkmJ/NKWICeyoDJumvSiloaAexmaE0Id/KfgJDt0hv34lB8Ly4Lt2O
2Ak6QTW5PH1vvWWySE+8fd5KB1MrQIqdchYq8L5oOpI5f4iIRBnRIyLejcSYzOKi
W5b4gPwhw+RWkGEL1xgLiW6dVlVl+fr7kvqllJjN+mtezrtz+rRpoumM7NqFwosT
aN1NfUal8uakhQzyZx0WTwvH/xWyWsUUtcYo8wIDAQABAoIBABB4Gkqho14kqS43
FtLEDQIiczejtB1z5QMERvprRPrf/9muMdil/FQqLUKrB82USbA2rwnAmenWe3HI
xEvxy7khWSW7O/BlxtwroNUPosICHXn0PPgMOsKrYc9RKvLWL9C85kh9pTt6SUQ6
sewxYluJXKNXw2B6TR/vLd1KZhvI1qO0XMrO02ck40G/Amk4JDYgmTRbRaFHcjMZ
4Qd6rF0QldZnWFl0QUh50nipBssxoyUserwznz7B5HCFhs1NAjCNSBarIsJFiteL
+/wU2mksk9khntMKzAT8Qu2YAX/kGpqRzBKCMeUjlIgyks5BKQ7RHVrJkjmA7U3/
GhXFpckCgYEA/1FzvL9LnL11EUXIbfI/vRhhWtKw766Ql5ywWqDdMW5w0VAzREzS
gxKbmoBlp0uLC0eOIG6edD9ck+lSixOWOL267sTaKKuUeHoE9dCLyM5Qc6JbpymF
BTUBLQfjidvrqefIdNAODiWsSrZMyh5XzD3/mdi0sWWVMq+8UZRduL8CgYEA8bql
qTPPKGjNukhYtShhDvXnNwOb8Si5OpPlAOySeN3LvJk4boxHgRAmgCSgUDv3qSZu
TSprih/SQzVuqsorUX6axjLP9PVM9TbWFcQ3BoPlXv4IDsBlNA9Gtjz22ofV16RN
BLR4TxroFZpQmpjM3IM5CaXrTRbG9PN1oWacyM0CgYAczjHCn8qGGpH0quzcCrLK
QM/rEU5JHGbP1CvJbdDG3PD5jJTcJdayVw0bN1VAtLMxSJdubUyPTP7C6VYYvtL5
/93xRmBeqk0L8qhQm4DJ3Q0SnsS8bWDGn55MWFGBokBKYQ4qr7aGPhXcMAkl3JqH
Po9x6hMo2I8mstEKWzTfvQKBgQCSO1VIHJ1vVqdNz8JKJRlCEaRD9Zz6sKYNN7bL
blHVaGd9ujsXNSl0fC6uSnnoz74sx6DmcYkIz+NE4SgHjbHS5QIAcHC5QUPC+99a
345iFJxHcOmy8tTGP4+JYyv6Wz4T68Lj28EEKcTIfMfSHimgJIn2uja0Ndk6CaXZ
c9fY6QKBgBTeeCMPknEX2YPlyT5fMbc5U44G8ZkWUbdBxqOxdxeKLNJ0zgmtRGQg
Gf2gij+Kt99TqmAOSH134NQY+mjddgUpDxdH3tHKFewR6UPeJJen4uMaWmktpDdY
qiJ8lupzIrYLx8U67GYL9ZE6/qLiC/zax7XCurHnC+3YQLAcuwRi
-----END RSA PRIVATE KEY-----
```

Fastweb Home Access Gateway

1 Raccolta delle informazioni

- ✗ Nessuna pagina di download aggiornamenti
- ✗ Impossibile intercettare un aggiornamento
- ✓ Presenza di una pagina informativa che ci indica componenti e posizione dell'interfaccia UART
- ✓ Pin allineati buoni candidati ad essere la JTAG



2 Analisi del bootloader

- ✗ Nessun comando permette di visualizzare la memoria

```
CFE> help
Available commands:

w                   Write the whole image start from beginning of the flash
e                   Erase [n]vram or [a]ll flash except bootrom
r                   Run program from flash image or from host depend on [f/h] flag
p                   Print boot line and board parameter info
c                   Change booline parameters
f                   Write image to the flash
m                   test mac client
i                   Erase persistent storage data
b                   Change board parameters
d                   Set default mac address
reset               Reset the board
flashimage          Flashes a compressed image after the bootloader.
help                Obtain help for CFE commands

For more information about a command, enter 'help command-name'
*** command status = 0
```

3 Individuazione e connessione all'interfaccia JTAG

- Col medesimo metodo della UART si individuano i pin dell'interfaccia JTAG

Pin	RGND (Ω)	RVcc (Ω)	V (V)	Note	Pin	RGND (Ω)	RVcc (Ω)	V (V)	Note
1	1.78K	1.71K	3.28		2	0	74.6	0	GND
3	1.83K	1.76K	3.38		4	0	74.6	0	GND
5	1.85K	1.78K	0		6	0	74.6	0	GND
7	1.83K	1.76K	3.38		8	0	74.6	0	GND
9	1.82K	1.75K	2.90		10	0	74.6	0	GND
11	10K	9.98K	3.36		12	0	74.6	0	GND

- Ci si connette all'interfaccia JTAG grazie ad un apposito debugger
- ✗ JTAG disabilitata

```
pi@raspberrypi:~ $ sudo jtag

UrJTAG 0.10 #2007
Copyright (C) 2002, 2003 ETC s.r.o.
Copyright (C) 2007, 2008, 2009 Kolja Waschk and the respective authors

UrJTAG is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
There is absolutely no warranty for UrJTAG.

warning: UrJTAG may damage your hardware!
Type "quit" to exit, "help" for help.

jtag> cable gpio tdi=23 tdo=24 tck=25 tms=18
Initializing GPIO JTAG Chain
jtag> detect
error: not found: queue is empty
```

Le contromisure

- Proteggersi dall'estrazione del firmware:
  - Aggiornamenti remoti sicuri (uso di connessioni sicure, controllo del numero di versione, ecc.)
  - Disabilitare le interfacce di debug
- Secure boot: solo software autenticato può essere eseguito sul dispositivo
- Cifratura del firmware

Conclusioni

- Sono state descritte ed analizzate le prime fasi di estrazione e analisi statica di un firmware di un dispositivo IoT
- Sono state attuate tali fasi analizzando due dispositivi dimostrando la difficoltà e allo stesso tempo la semplicità con cui è possibile minacciare la sicurezza di un dispositivo
- Si sono forniti due punti di vista: sia quello dell'analista (colui che minaccia il dispositivo), sia quello dello sviluppatore (colui che deve proteggere il dispositivo)