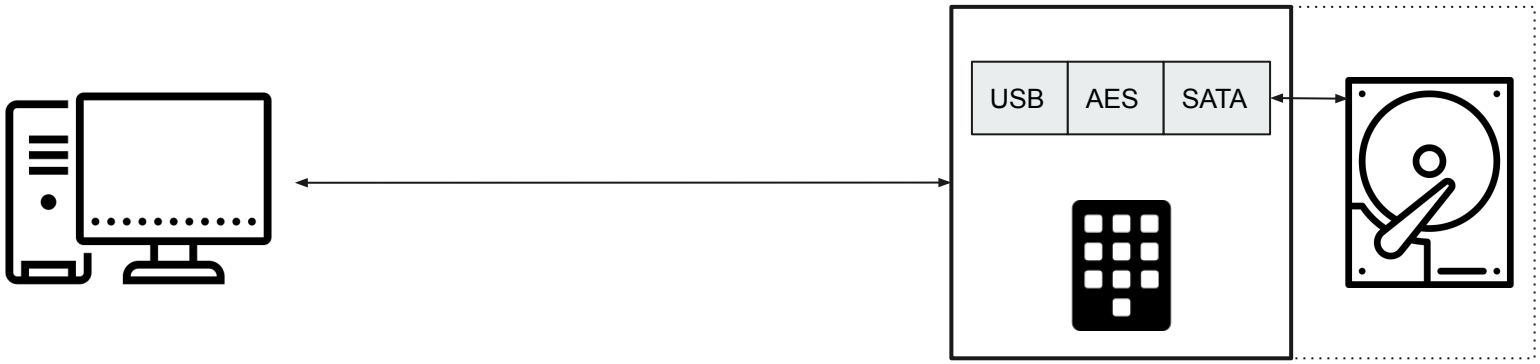
Analýza bezpečnosti externých šifrovacích obalov na disky

Autor: Adam Dej
Školiteľ: Richard Ostertág

Externý obal so schopnosťou šifrovania



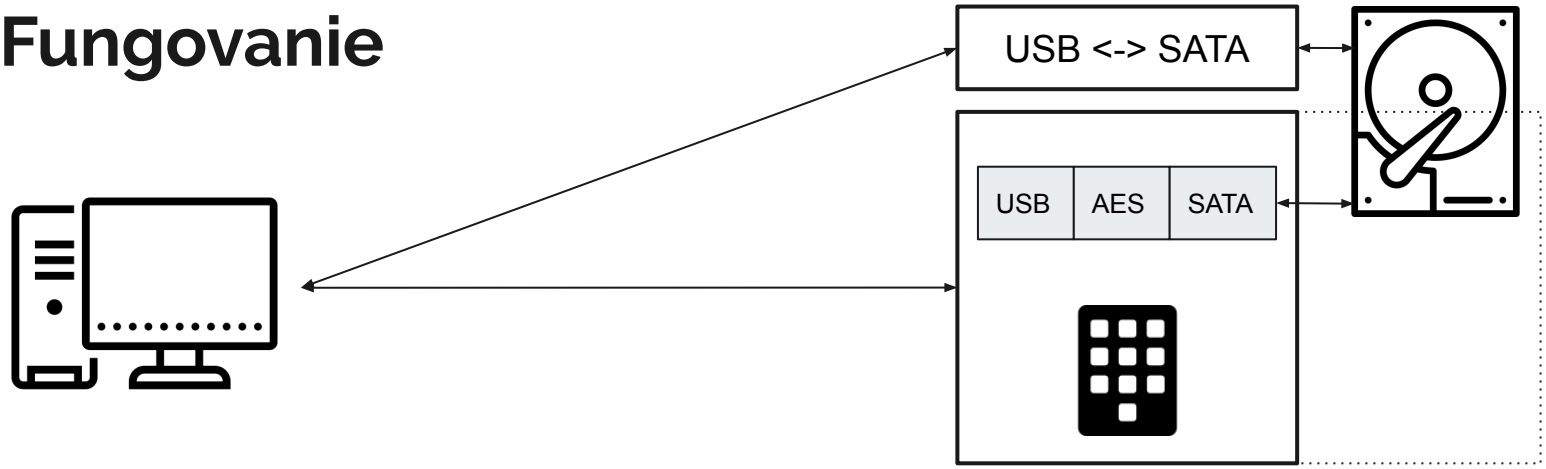
Raidsonic IB-289U3

Výrobca sľubuje:

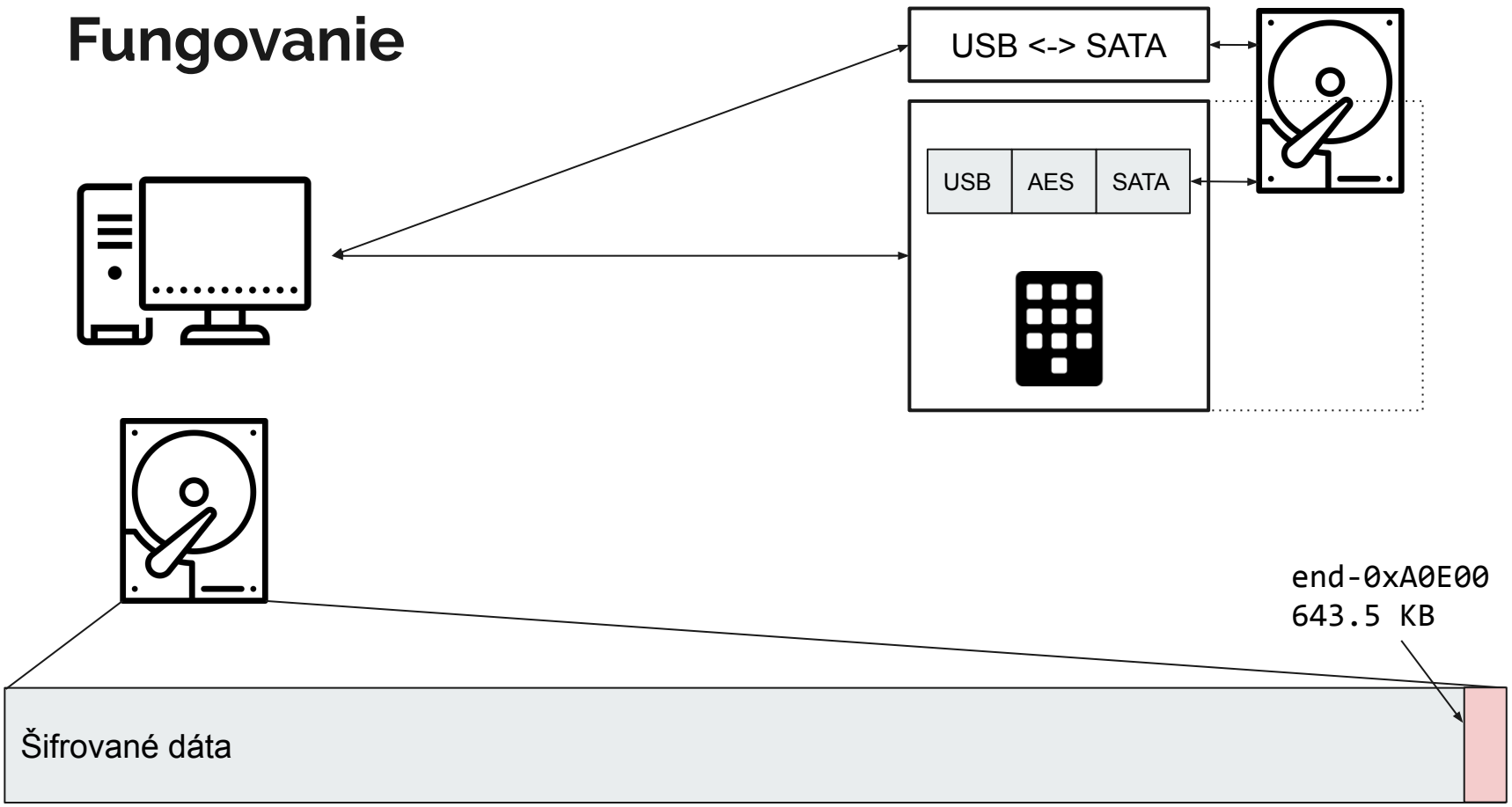
- 3 Gbit/s prenosová rýchlosť
- “Silné” AES šifrovanie
- 4-12 číselné heslo
- Možnosť zmeny hesla bez straty dát

Black-box analýza

Fungovanie



Fungovanie



Crypto blob - 512 bytov (1 sektor)

- Vytvorený pri inicializácií šifrovania
- Zmenený každou zmenou PINu
  - Šifrované dáta sa nemenia
  - Iný aj pre rovnaký pin
- Obnova pôvodného “blob”-u => Obnova pôvodného PINu a kľúča

```
000007d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000007e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000007f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000800: e331 ea0c ead7 b548 704c 6f00 bbd3 cefd  .1.....HpLo.....
00000810: 333d 0069 1ef9 0488 0cd8 ce84 204d bc93  3=.i........ M..
00000820: d573 ab35 767c 11bd 283e 0ce7 3580 2ecb  .s.5v|..(>..5...
00000830: 66e9 4682 6bb1 cc92 7b5e 1e04 4c5f a542  f.F.k...{^..L_.B
00000840: 33ba d7c7 d474 1aed 6f08 c5fa d495 297a  3....t..o.....)z
00000850: eb5e 088c cbef 6421 53fd 0f08 26e3 fc6a  .^....d!S...&..j
00000860: d76d 0fb5 933e 0c59 13de e3ed e7ae 6382  .m...>.Y......c.
00000870: bca7 3962 efcc b0d0 892d 7046 50c9 ebf8  ..9b.....-pFP...
00000880: daff d2f1 16e9 056d ce5b 318b b7b1 96dd  .......m.[1.....
00000890: 628d 6767 bc13 6fe8 7166 0bf2 cd00 3924  b.gg..o.qf....9$
000008a0: 0675 b10c 32dc f041 c789 419d 6017 4015  .u..2..A..A.`.@.
000008b0: 73b2 fc01 d00b be41 588e 3b0f 5646 17cb  s......AX.;.VF..
000008c0: 9756 a12a 7364 26a4 1201 b3ce f6d9 7e52  .V.*sd&.......~R
000008d0: d4b7 ef6f 5150 fe99 78ee 02c0 0eb7 1149  ...oQP..x......I
000008e0: 5123 b27b 14e2 c7dc 02fc 8144 e6e9 9617  Q#.{.......D....
000008f0: 8bb5 271c e8e6 d2d7 0fa7 8062 47b0 455b  ..'........bG.E[
00000900: 61a0 a61c c5b9 6f02 6213 93fd 0920 5dee  a.....o.b.... ].
00000910: 9073 cf52 f596 749b 6a7a e039 48d6 928b  .s.R..t.jz.9H...
00000920: a2e5 714a a24e 67f4 10ad 4a24 7b84 f348  ..qJ.Ng...J${..H
00000930: 894a 5250 6bf9 359b 9b13 4645 e4cb 9ce7  .JRPk.5...FE....
00000940: 7e16 825e 4be3 4608 0788 9bf4 e584 0195  ~..^K.F.........
00000950: cf61 4a87 35aa ab89 5342 705a f1ce 0a95  .aJ.5...SBpZ....
00000960: 1f5b 36a7 1df5 67ae 7281 38f4 5072 b950  .[6...g.r.8.Pr.P
00000970: b733 3f60 5af9 b8f5 d314 69c8 716a 049f  .3?`Z.....i.qj..
00000980: ce10 f1f3 05c7 ddcf 12c8 7b81 b4dd 3ded  ..........{...=.
00000990: 779c 6e55 d34b 8049 458c ea54 6071 2e25  w.nU.K.IE..T`q.%
000009a0: 90d8 2f74 9a94 fc47 621f bdd3 3a07 0726  ../t...Gb...:..&
000009b0: df23 2331 3754 d5d9 e861 3065 016e 7549  .##17T...a0e.nuI
000009c0: 9e83 7849 d9a6 6a97 d3bc 2d08 0b2e 51f3  ..xI..j...-...Q.
000009d0: 0cfe 9207 bed6 f65c 2e61 c0f6 70a8 d8bd  .......\.a..p...
000009e0: 23a0 829e 7cae 267d f7a1 6e98 cca7 ce8f  #...|.&}..n.....
000009f0: b019 fb2e 5dd3 7791 1c84 37ec 7ac7 c7f8  ....].w...7.z...
00000a00: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a10: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a20: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

Crypto blob - 512 bytov (1 sektor)

- Vytvorený pri inicializácií šifrovania
- Zmenený každou zmenou PINu
  - Šifrované dáta sa nemenia
  - Iný aj pre rovnaký pin
- Obnova pôvodného “blob”-u => Obnova pôvodného PINu a kľúča

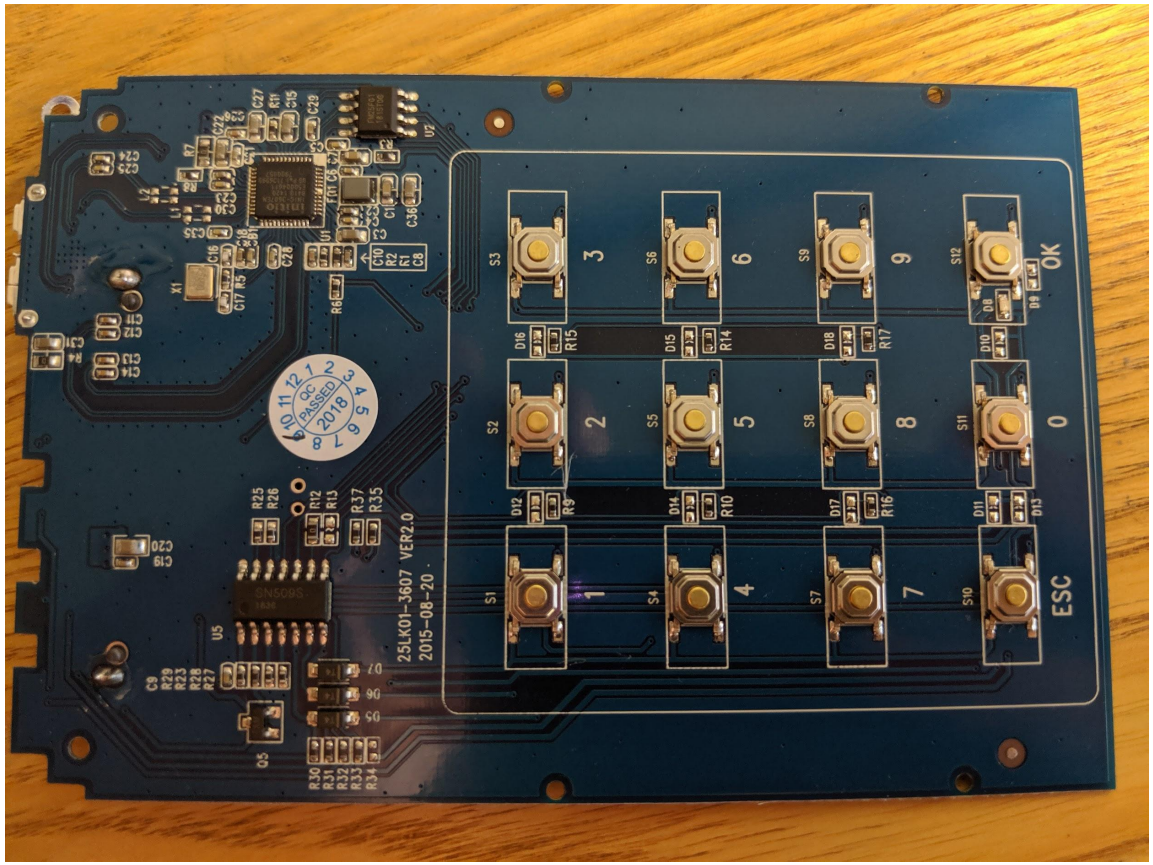
Pravdepodobne obsahuje:

- Disk Encryption Key, šifrovaný
- Misc dáta pre šifrovanie (IV, …)
- Konštantné hodnoty, pre overenie korektnosti PINu
- “salt”?

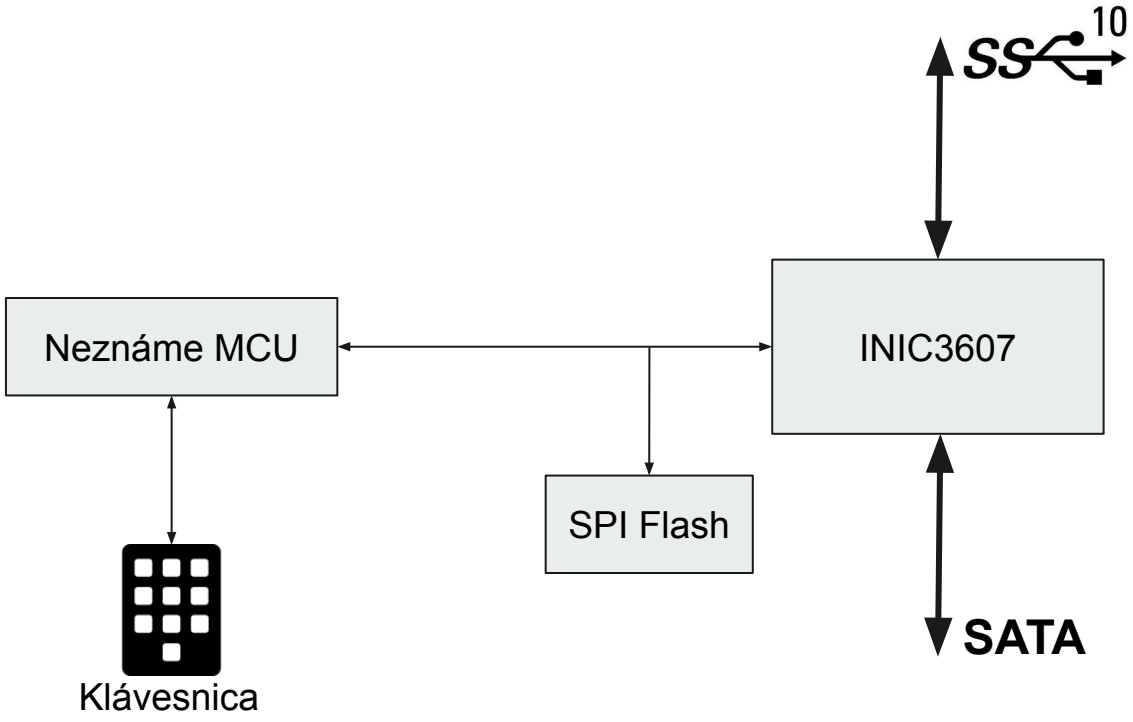
```
000007d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000007e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000007f0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000800: e331 ea0c ead7 b548 704c 6f00 bbd3 cefd  .1.....HpLo.....
00000810: 333d 0069 1ef9 0488 0cd8 ce84 204d bc93  3=.i........ M..
00000820: d573 ab35 767c 11bd 283e 0ce7 3580 2ecb  .s.5v|..(>..5...
00000830: 66e9 4682 6bb1 cc92 7b5e 1e04 4c5f a542  f.F.k...{^..L_.B
00000840: 33ba d7c7 d474 1aed 6f08 c5fa d495 297a  3....t..o.....)z
00000850: eb5e 088c cbef 6421 53fd 0f08 26e3 fc6a  .^....d!S...&..j
00000860: d76d 0fb5 933e 0c59 13de e3ed e7ae 6382  .m...>.Y......c.
00000870: bca7 3962 efcc b0d0 892d 7046 50c9 ebf8  ..9b.....-pFP...
00000880: daff d2f1 16e9 056d ce5b 318b b7b1 96dd  .......m.[1.....
00000890: 628d 6767 bc13 6fe8 7166 0bf2 cd00 3924  b.gg..o.qf....9$
000008a0: 0675 b10c 32dc f041 c789 419d 6017 4015  .u..2..A..A.`.@.
000008b0: 73b2 fc01 d00b be41 588e 3b0f 5646 17cb  s......AX.;.VF..
000008c0: 9756 a12a 7364 26a4 1201 b3ce f6d9 7e52  .V.*sd&.......~R
000008d0: d4b7 ef6f 5150 fe99 78ee 02c0 0eb7 1149  ...oQP..x......I
000008e0: 5123 b27b 14e2 c7dc 02fc 8144 e6e9 9617  Q#.{.......D....
000008f0: 8bb5 271c e8e6 d2d7 0fa7 8062 47b0 455b  ..'........bG.E[
00000900: 61a0 a61c c5b9 6f02 6213 93fd 0920 5dee  a.....o.b.... ].
00000910: 9073 cf52 f596 749b 6a7a e039 48d6 928b  .s.R..t.jz.9H...
00000920: a2e5 714a a24e 67f4 10ad 4a24 7b84 f348  ..qJ.Ng...J${..H
00000930: 894a 5250 6bf9 359b 9b13 4645 e4cb 9ce7  .JRPk.5...FE....
00000940: 7e16 825e 4be3 4608 0788 9bf4 e584 0195  ~..^K.F.........
00000950: cf61 4a87 35aa ab89 5342 705a f1ce 0a95  .aJ.5...SBpZ....
00000960: 1f5b 36a7 1df5 67ae 7281 38f4 5072 b950  .[6...g.r.8.Pr.P
00000970: b733 3f60 5af9 b8f5 d314 69c8 716a 049f  .3?`Z.....i.qj..
00000980: ce10 f1f3 05c7 ddcf 12c8 7b81 b4dd 3ded  ..........{...=.
00000990: 779c 6e55 d34b 8049 458c ea54 6071 2e25  w.nU.K.IE..T`q.%
000009a0: 90d8 2f74 9a94 fc47 621f bdd3 3a07 0726  ../t...Gb...:..&
000009b0: df23 2331 3754 d5d9 e861 3065 016e 7549  .##17T...a0e.nuI
000009c0: 9e83 7849 d9a6 6a97 d3bc 2d08 0b2e 51f3  ..xI..j...-...Q.
000009d0: 0cfe 9207 bed6 f65c 2e61 c0f6 70a8 d8bd  .......\.a..p...
000009e0: 23a0 829e 7cae 267d f7a1 6e98 cca7 ce8f  #...|.&}..n.....
000009f0: b019 fb2e 5dd3 7791 1c84 37ec 7ac7 c7f8  ....].w...7.z...
00000a00: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a10: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000a20: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

Analýza vnútorného fungovania

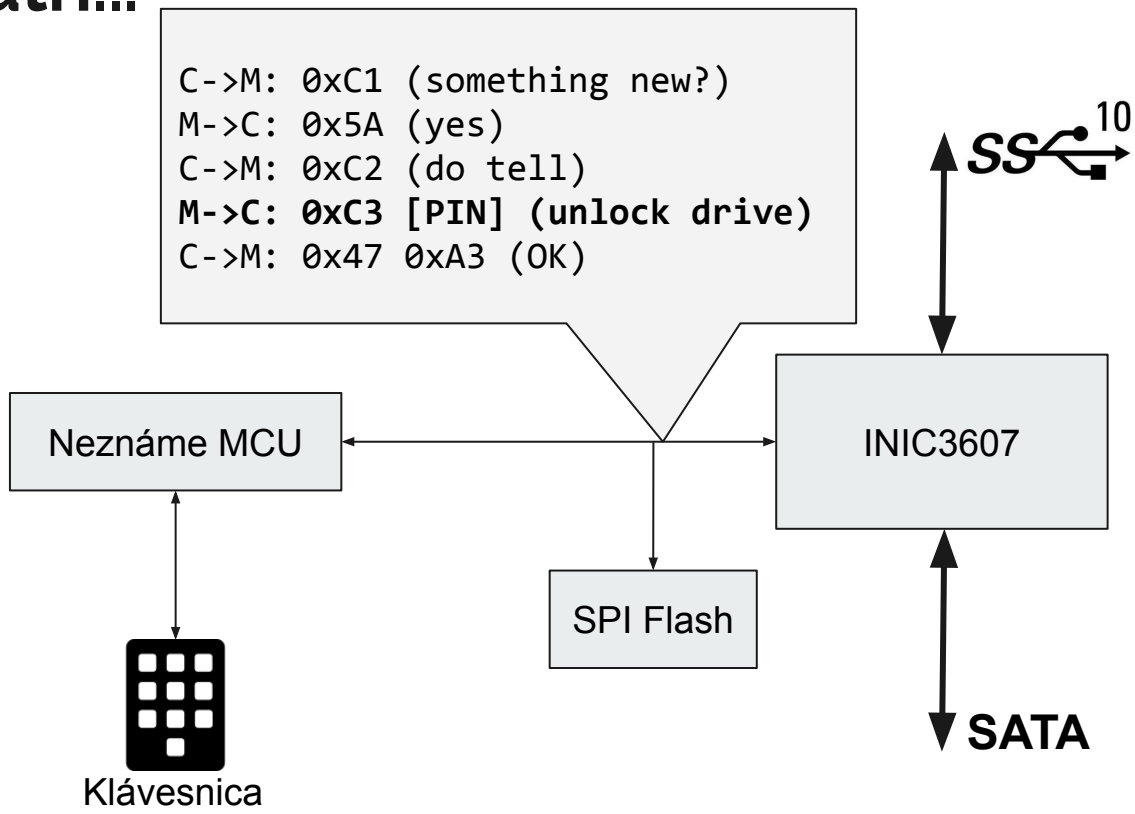
Vo vnútri...



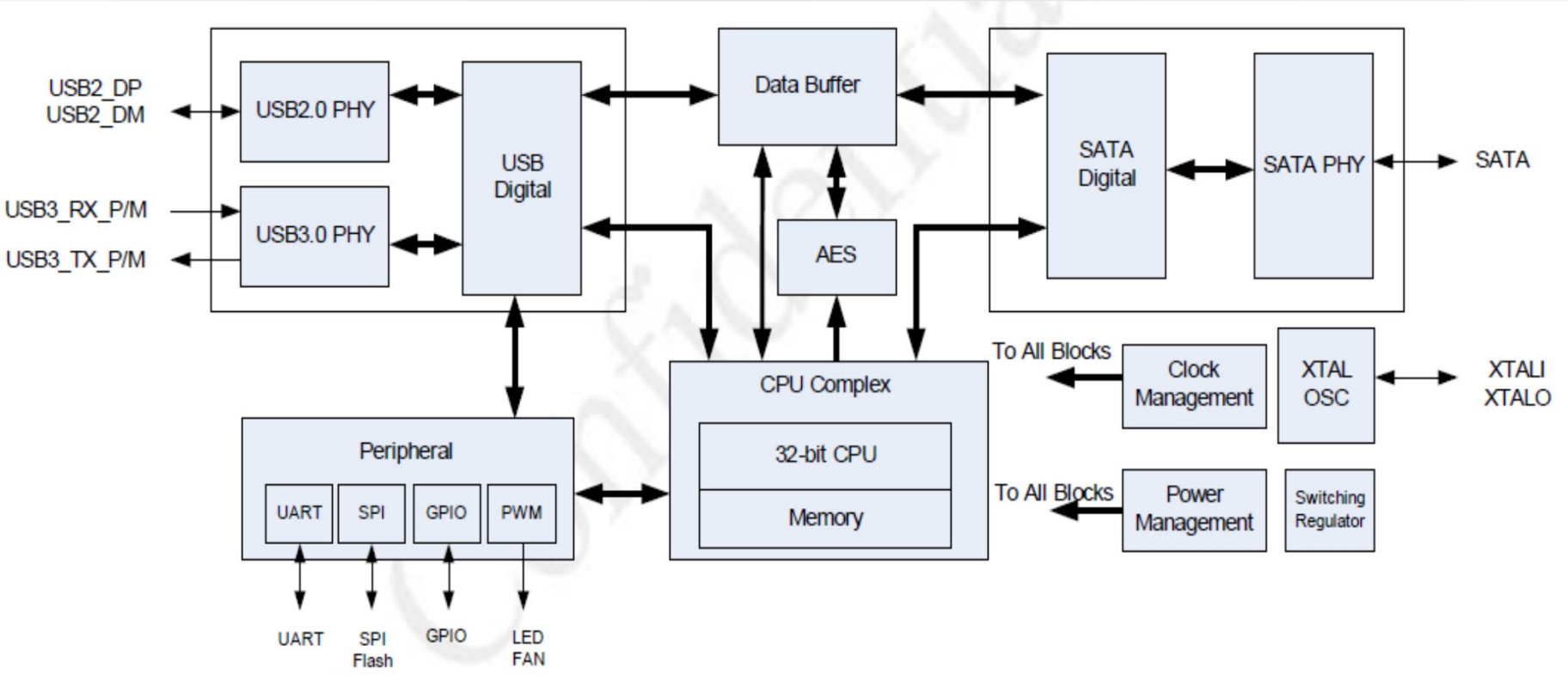
Vo vnútri...



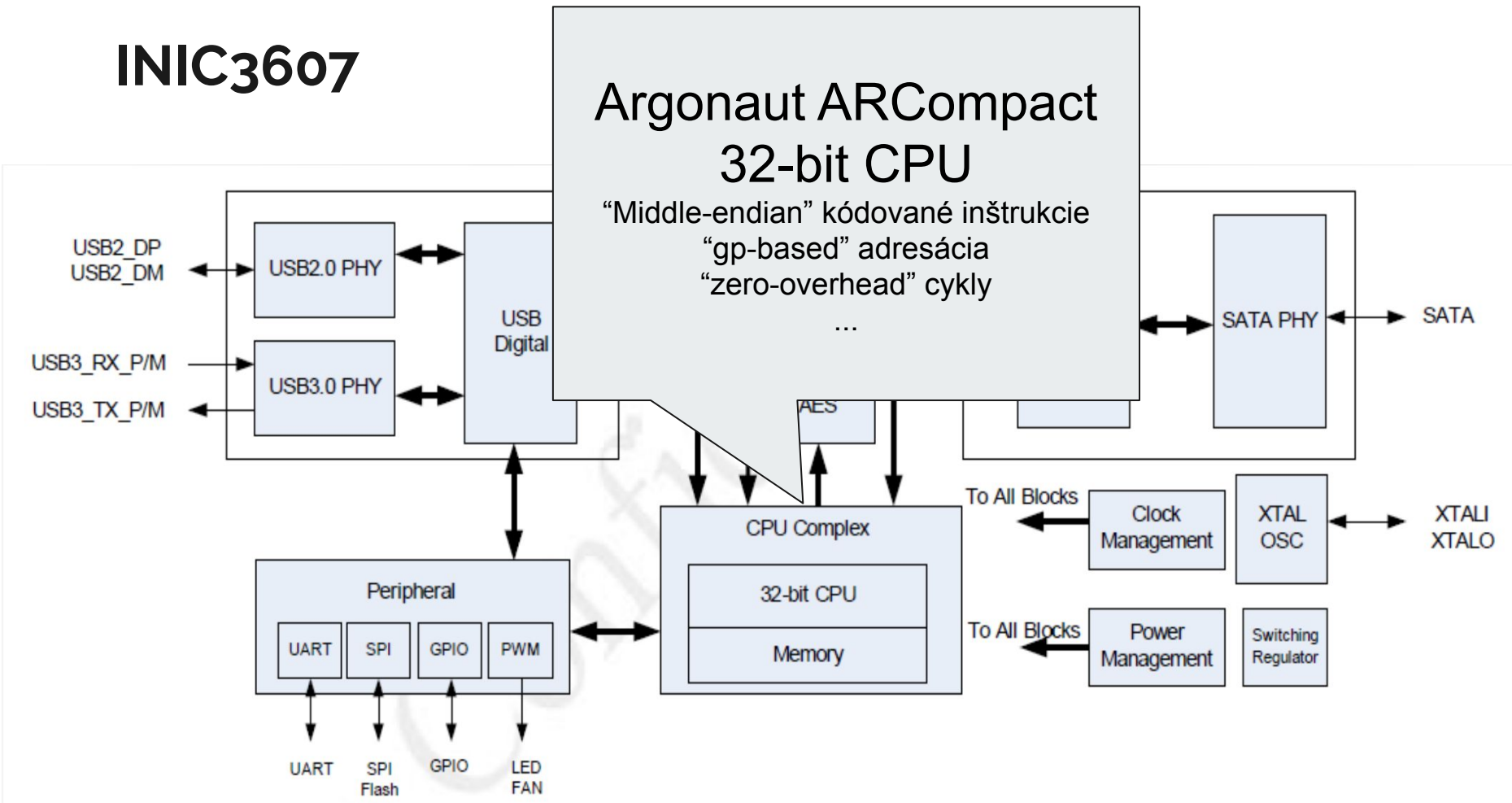
Vo vnútri...


C->M: 0xC1 (something new?)
M->C: 0x5A (yes)
C->M: 0xC2 (do tell)
M->C: 0xC3 [PIN] (unlock drive)
C->M: 0x47 0xA3 (OK)
SS 10
Neznáme MCU
INIC3607
SPI Flash
SATA
Klávesnica

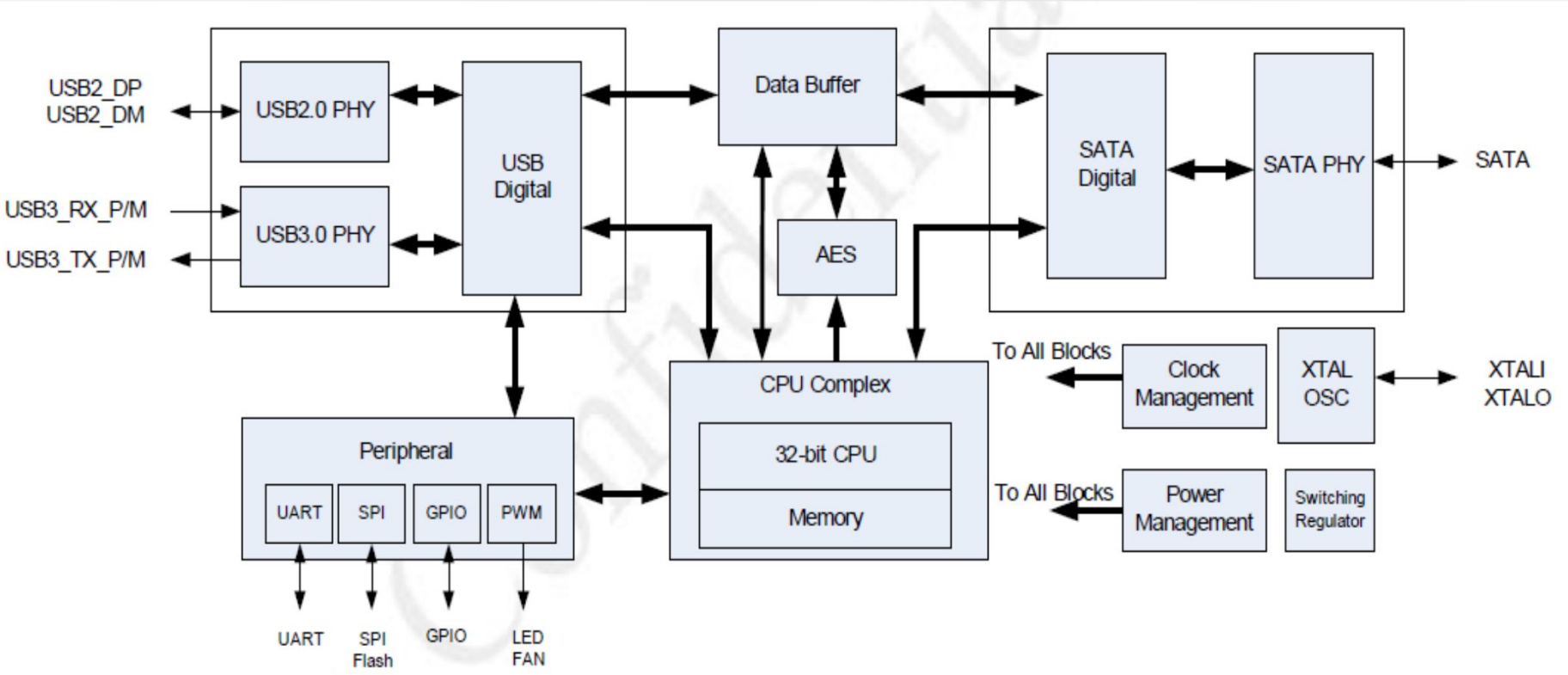
INIC-3607E

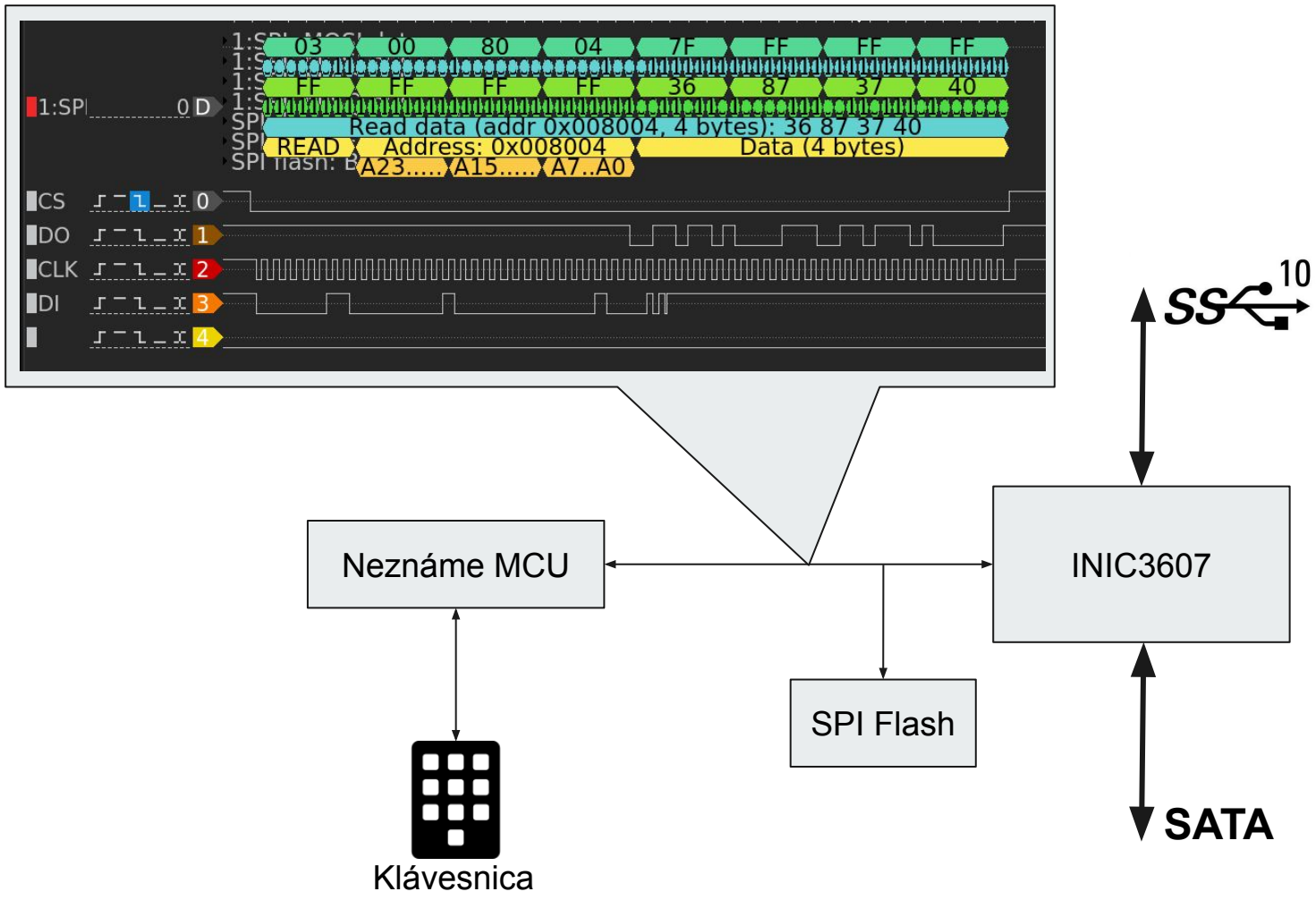

USB2_DP
USB2_DM
USB3_RX_P/M
USB3_TX_P/M
USB2.0 PHY
USB3.0 PHY
USB Digital
Data Buffer
AES
SATA Digital
SATA PHY
SATA
CPU Complex
32-bit CPU
Memory
Peripheral
UART
SPI
GPIO
PWM
UART
SPI Flash
GPIO
LED FAN
To All Blocks
Clock Management
XTAL OSC
XTALI
XTALO
To All Blocks
Power Management
Switching Regulator

INIC3607

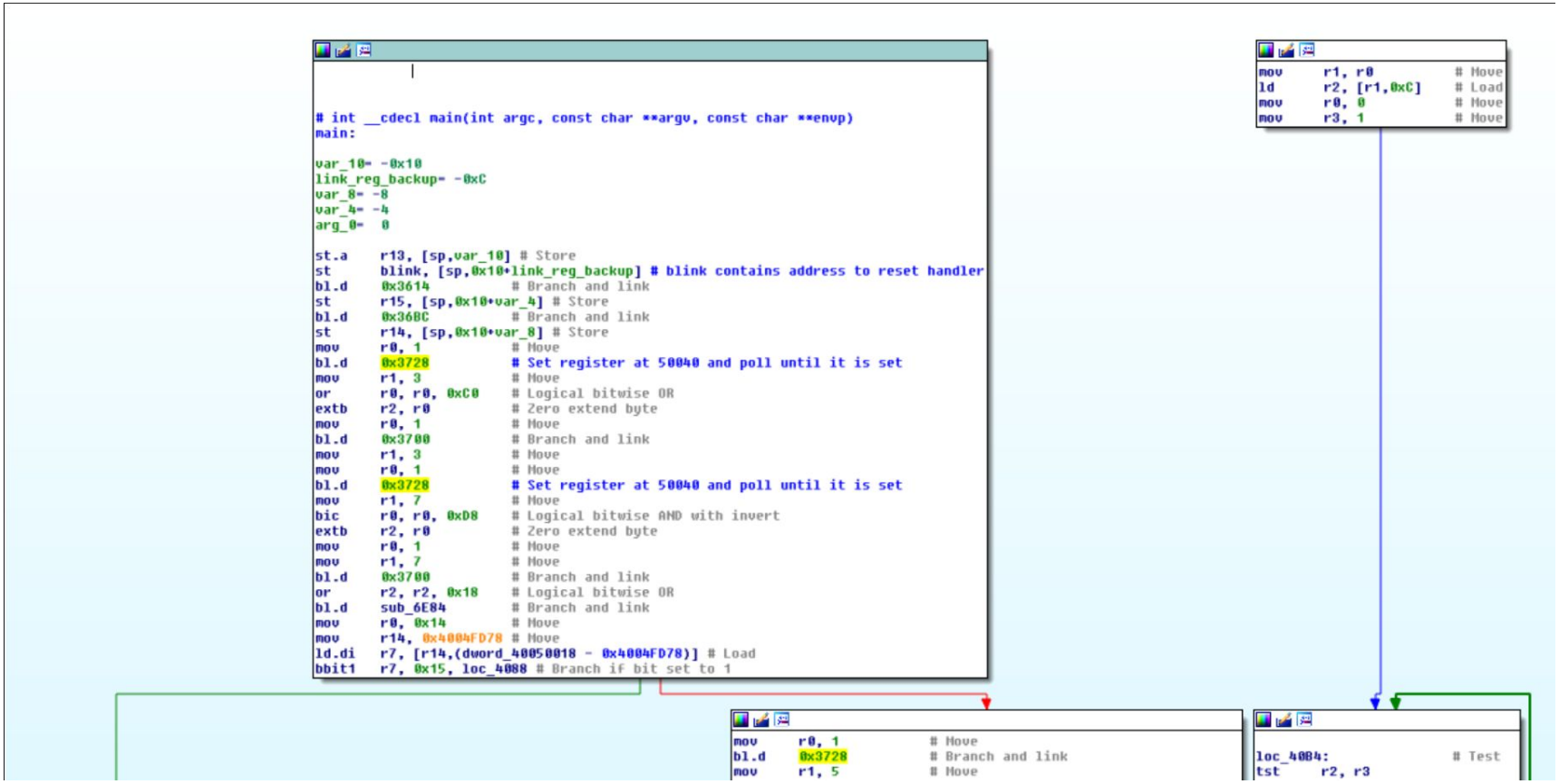

Argonaut ARCompact
32-bit CPU
“Middle-endian” kódované inštrukcie
“gp-based” adresácia
“zero-overhead” cykly
...
USB2_DP
USB2_DM
USB2.0 PHY
USB3_RX_P/M
USB3_TX_P/M
USB3.0 PHY
USB Digital
SATA PHY
SATA
AES
To All Blocks
Clock Management
XTAL OSC
XTALI
XTALO
CPU Complex
32-bit CPU
Memory
Peripheral
UART
SPI
GPIO
PWM
To All Blocks
Power Management
Switching Regulator
UART
SPI Flash
GPIO
LED FAN

INIC3607

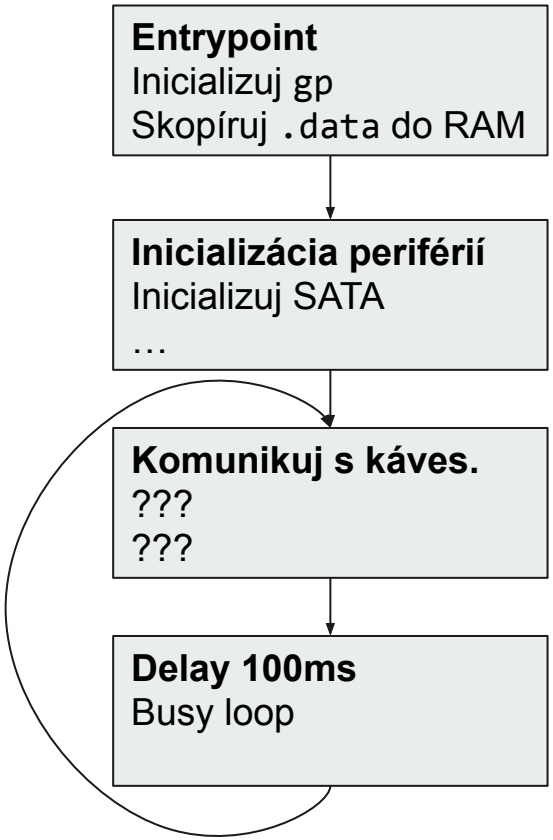

USB2_DP
USB2_DM
USB3_RX_P/M
USB3_TX_P/M
USB2.0 PHY
USB3.0 PHY
USB Digital
Data Buffer
AES
SATA Digital
SATA PHY
SATA
CPU Complex
32-bit CPU
Memory
Peripheral
UART
SPI
GPIO
PWM
UART
SPI Flash
GPIO
LED FAN
To All Blocks
Clock Management
XTAL OSC
XTALI
XTALO
To All Blocks
Power Management
Switching Regulator


03 00 80 04 7F FF FF FF
FF FF FF FF 36 87 37 40
Read data (addr 0x008004, 4 bytes): 36 87 37 40
READ
Address: 0x008004
Data (4 bytes)
A23.....
A15.....
A7..A0
CS
DO
CLK
DI
SS 10
Neznáme MCU
INIC3607
SPI Flash
SATA
Klávesnica

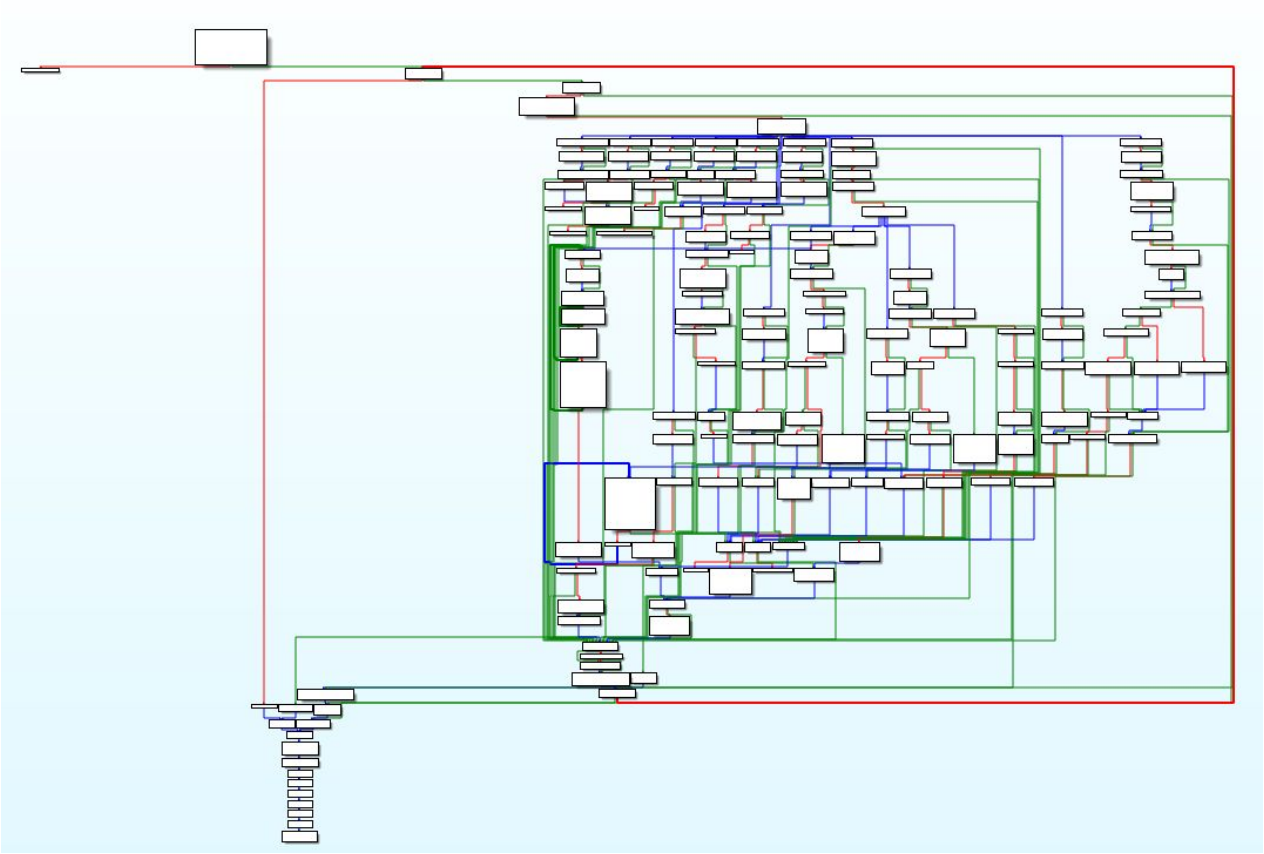
Statická analýza



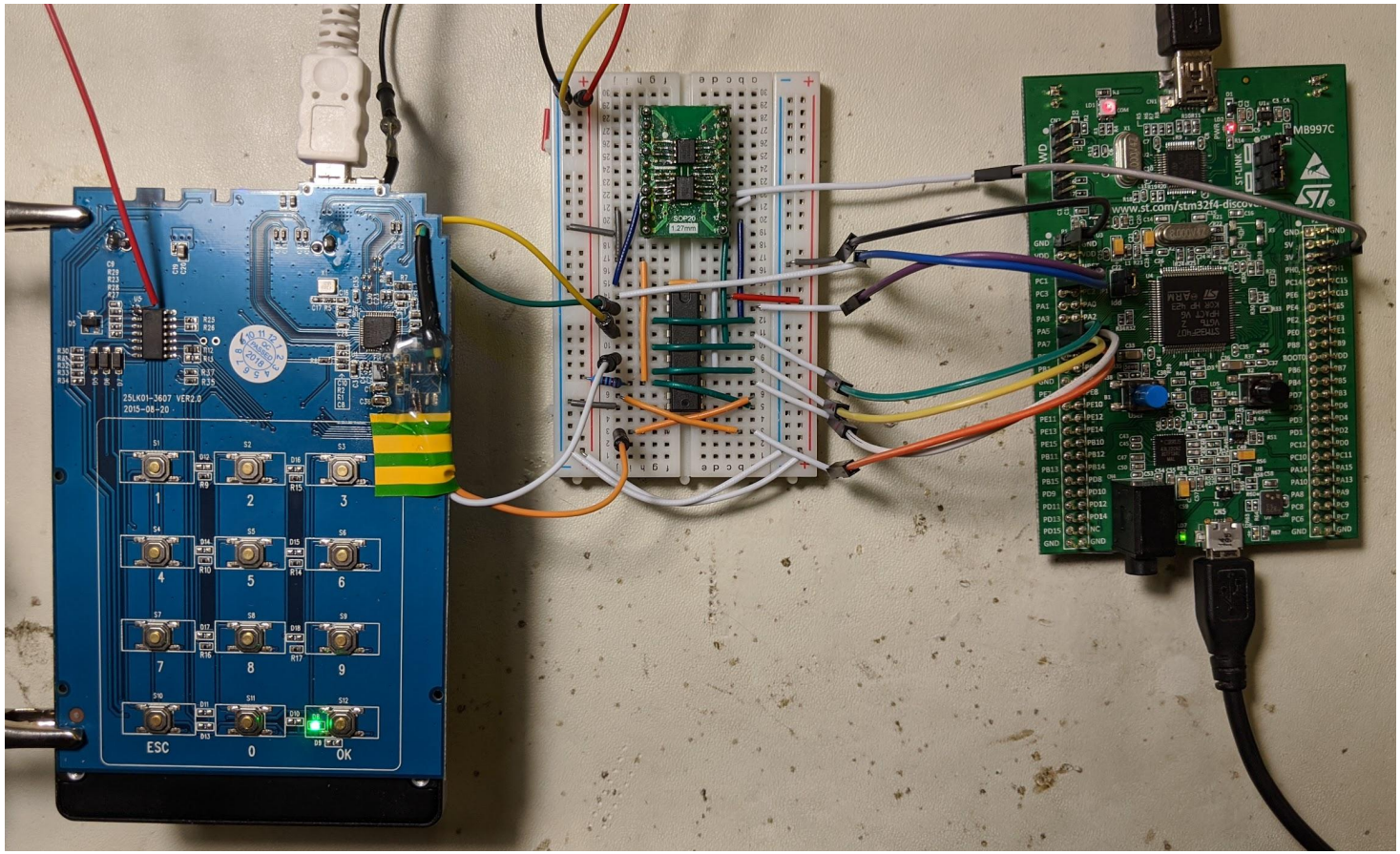
Základná štruktúra firmwareu



Stavový stroj komunikačného protokolu



“dynamická” analýza



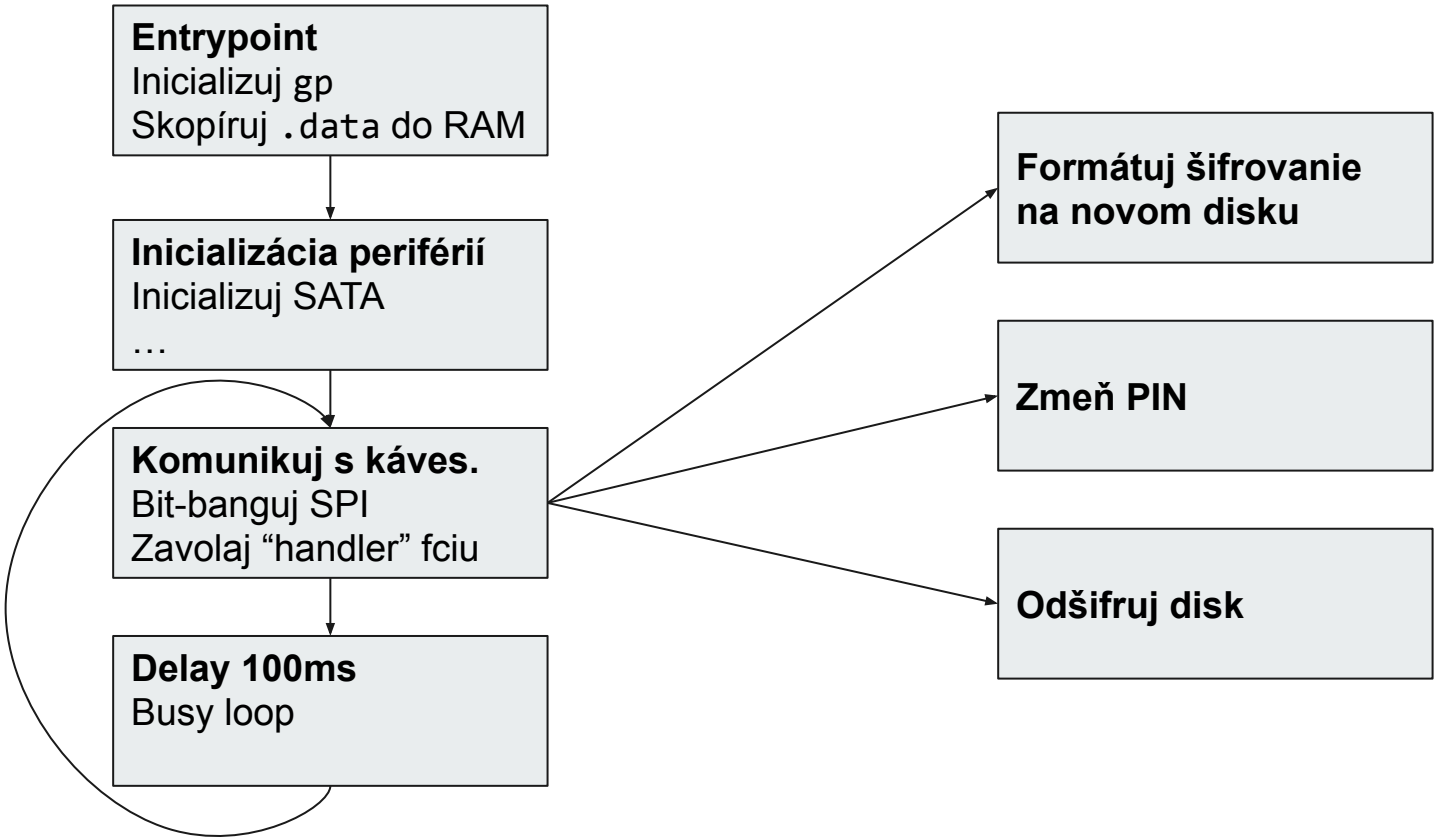
Modifikácia firmwareu

- Integrita FW zabezpečená CRC-16 na konci

Modifikácia firmwareu

- Integrita FW zabezpečená CRC-16 na konci
- Ktorúkoľvek inštrukciu viem prepísať na “branch to self” - zacyklenie

Základná štruktúra firmwareu



Nástroj `dumppoint-tool`

0x0000

```
[...]

000099C4 mov     r0, 16          # Move
000099C6 st      r0, [spi_bitbang_remaining_cycles] # Store
000099CA stb     r1, [spi_bitbang_is_first_cycle] # Store
000099CE bl.d    sub_6BFC        # does something with
000099CE                         # disabled interrupts
000099D2 stb     r1, [oh_continue_iteration_flag?] # Store
000099D6 mov     r0, 0x493E0     # Move
000099DC bl      obrovske_hovado # Branch and link
000099DE ld.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E2 bset    r0, r0, GPIO_BITS.SPI_CS # Set specified bit (to 1)
000099E4 st.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E8 bl      zeroize_protocol_statemachine # Branch and link
000099EA b.d     loc_9CC8        # Branch

[...]
```

0xA1C4

Nástroj `dumppoint-tool`

0x0000

```
[...]

000099C4 mov     r0, 16          # Move
000099C6 st      r0, [spi_bitbang_remaining_cycles] # Store
000099CA stb     r1, [spi_bitbang_is_first_cycle] # Store
000099CE bl.d    sub_6BFC        # does something with
000099CE                         # disabled interrupts
000099D2 stb     r1, [oh_continue_iteration_flag?] # Store
000099D6 mov     r0, 0x493E0     # Move
000099DC bl      obrovske_hovado # Branch and link
000099DE ld.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E2 bset    r0, r0, GPIO_BITS.SPI_CS # Set specified bit (to 1)
000099E4 st.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E8 bl      zeroize_protocol_statemachine # Branch and link
000099EA b.d     loc_9CC8        # Branch

[...]
```

0xA1C4

0xA200

dump_regs_and_ram

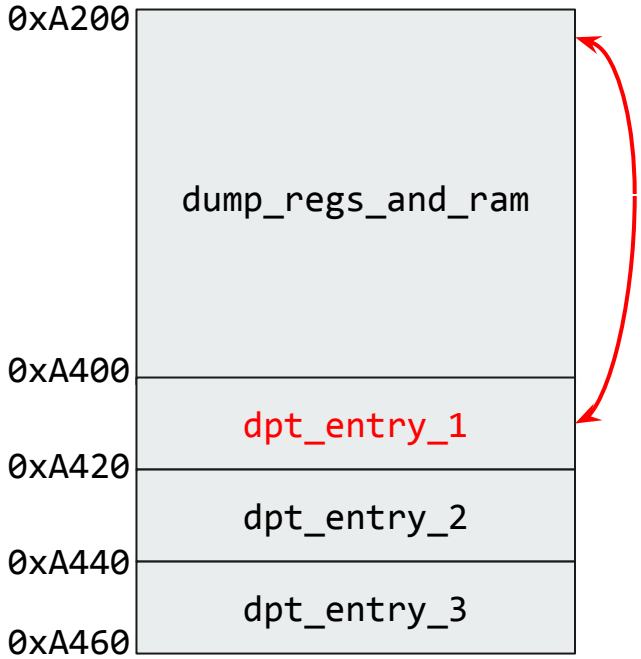
0xA400

Nástroj `dumppoint-tool`

0x0000

```
[...]

000099C4 mov     r0, 16          # Move
000099C6 st      r0, [spi_bitbang_remaining_cycles] # Store
000099CA stb     r1, [spi_bitbang_is_first_cycle] # Store
000099CE bl.d    sub_6BFC        # does something with
000099CE                         # disabled interrupts
000099D2 stb     r1, [oh_continue_iteration_flag?] # Store
000099D6 mov     r0, 0x493E0     # Move
000099DC bl      obrovske_hovado # Branch and link
000099DE ld.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E2 bset    r0, r0, GPIO_BITS.SPI_CS # Set specified bit (to 1)
000099E4 st.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E8 bl      zeroize_protocol_statemachine # Branch and link
000099EA b.d     loc_9CC8        # Branch

[...]
```

0xA1C4

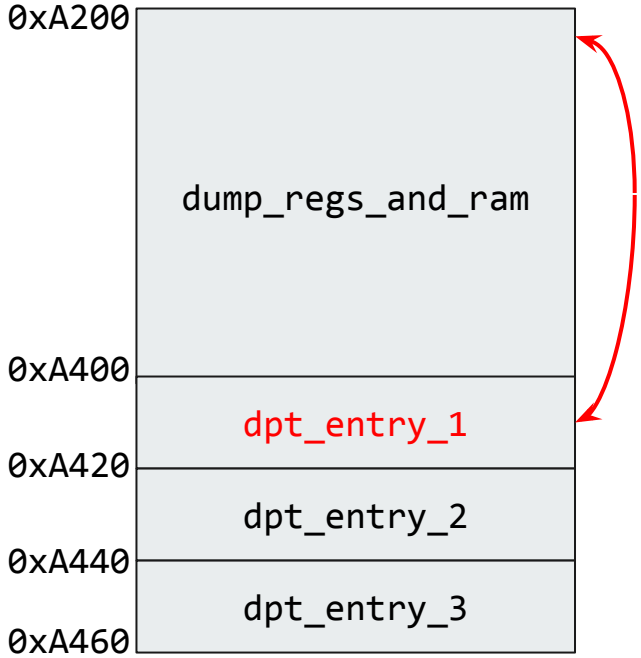


Nástroj `dumppoint-tool`

0x0000

```
[...]

000099C4 mov     r0, 16          # Move
000099C6 st      r0, [spi_bitbang_remaining_cycles] # Store
000099CA stb     r1, [spi_bitbang_is_first_cycle] # Store
000099CE bl.d    sub_6BFC        # does something with
000099CE                         # disabled interrupts
000099D2 stb     r1, [oh_continue_iteration_flag?] # Store
000099D6 mov     r0, 0x493E0     # Move
000099DC bl      obrovske_hovado # Branch and link
000099DE ld.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E2 bset    r0, r0, GPIO_BITS.SPI_CS # Set specified bit (to 1)
000099E4 st.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E8 bl      zeroize_protocol_statemachine # Branch and link
000099EA b.d     loc_9CC8        # Branch

[...]
```

0xA1C4

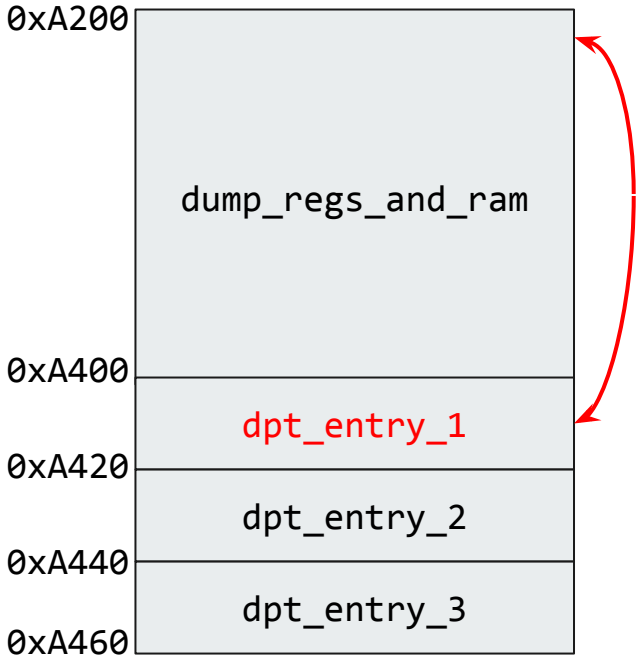


Nástroj dumppoint-tool

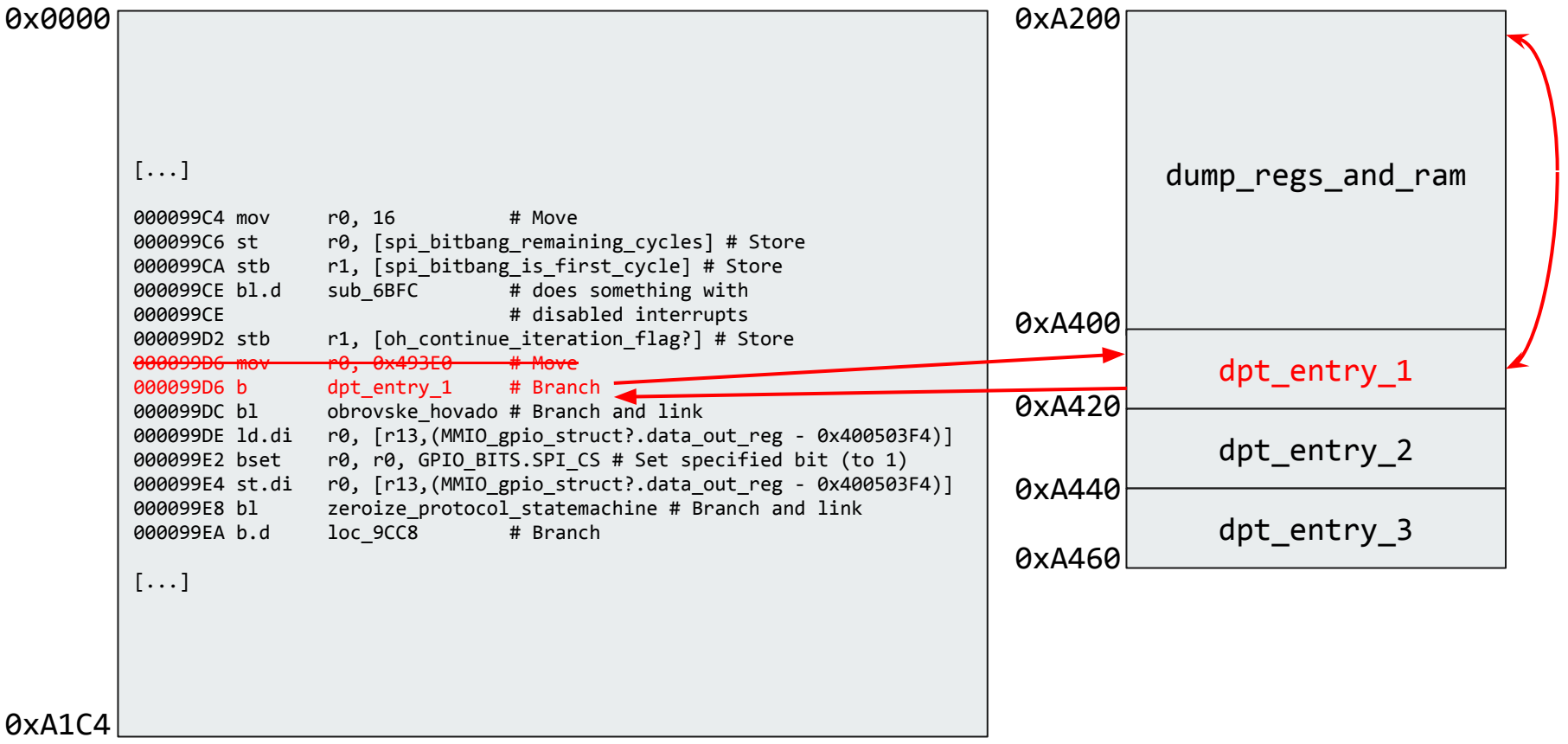
0x0000

```
[...]

000099C4 mov     r0, 16          # Move
000099C6 st      r0, [spi_bitbang_remaining_cycles] # Store
000099CA stb     r1, [spi_bitbang_is_first_cycle] # Store
000099CE bl.d    sub_6BFC        # does something with
000099CE                         # disabled interrupts
000099D2 stb     r1, [oh_continue_iteration_flag?] # Store
000099D6 mov     r0, 0x493E0     # Move
000099D6 b       dpt_entry_1     # Branch
000099DC bl      obrovske_hovado # Branch and link
000099DE ld.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E2 bset    r0, r0, GPIO_BITS.SPI_CS # Set specified bit (to 1)
000099E4 st.di   r0, [r13,(MMIO_gpio_struct?.data_out_reg - 0x400503F4)]
000099E8 bl      zeroize_protocol_statemachine # Branch and link
000099EA b.d     loc_9CC8        # Branch

[...]
```

0xA1C4



Nástroj dumppoint-tool

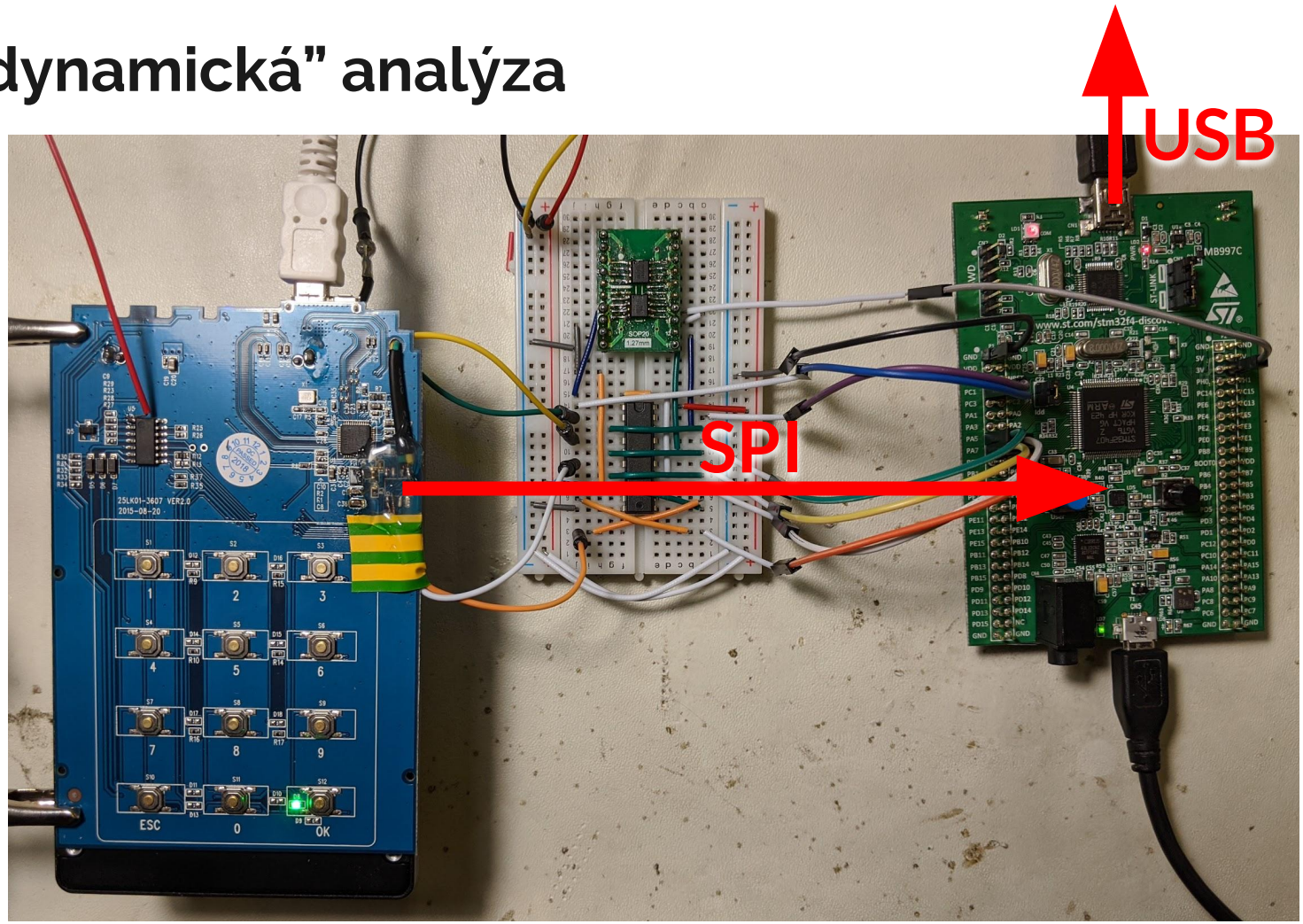


dpt_entry_*n*

- 32-bajtový kus kódu, ktorý:
  - Zavolá `dump_regs_and_ram`
  - Obnoví pôvodné registre
  - **Vykoná pôvodnú inštrukciu**
  - Skočí späť do kódu
  - Obsahuje 8-bajtový identifikačný string

```
00000000: f1c0 e1c0 4027 0075 fa0e cfff c1c0 d1c0  ....@'.u........
00000010: 4a26 0070 7d05 8fff 2068 656c 6c6f 2077  J&.p}... hello w
```

“dynamická” analýza



Zistenia

Dešifrovanie “cryptoblob”-u

- `setup_decryption` - funkcia na adrese `0x2EA4`
  - Prečíta sektor 0 hlavičky
  - Overí magické konštanty
  - Prečíta a dešifruje sektor 4 hlavičky (“cryptoblob”)
  - Overí magický string na začiatku “cryptoblob”-u

Dešifrovanie “cryptoblob”-u

- `setup_decryption` - funkcia na adrese `0x2EA4`
  - Prečíta sektor 0 hlavičky
  - Overí magické konštanty
  - Prečíta a dešifruje sektor 4 hlavičky (“cryptoblob”)
  - Overí magický string na začiatku “cryptoblob”-u

- Využíva funkciu `perform_io_on_header`
  - Užívateľsky príjemná
  - Parametre:
    - Sektor v hlavičke
    - “Flagy” - čítanie / zápis, s/bez šifrovania
    - Adresy kľúča, “bufferu” dát a číslo sektoru 0 hlavičky sú globálne premenné

Analýza `perform_io_on_disk`

- Ak šifruje, pred prečítaním sektoru volá funkcie ktoré:
  - Dva krát skopírujú 32-bajtov prijatých z klávesnice do MMIO registrov
    - PIN 1234: `0x31 0x32 0x33 0x34 0x00 0x00 0x00 [...]`
  - Skopírujú číslo čítaného sektora do MMIO registrov

Analýza `perform_io_on_disk`

- Ak šifruje, pred prečítaním sektoru volá funkcie ktoré:
  - Dva krát skopírujú 32-bajtov prijatých z klávesnice do MMIO registrov
    - PIN 1234: `0x31 0x32 0x33 0x34 0x00 0x00 0x00 [...]`
  - Skopírujú číslo čítaného sektora do MMIO registrov

- Teória: 2 kľúče a číslo sektoru - AES-256 XTS (kde číslo sektoru je tweak)

Dešifrovanie “cryptoblob”u na PC

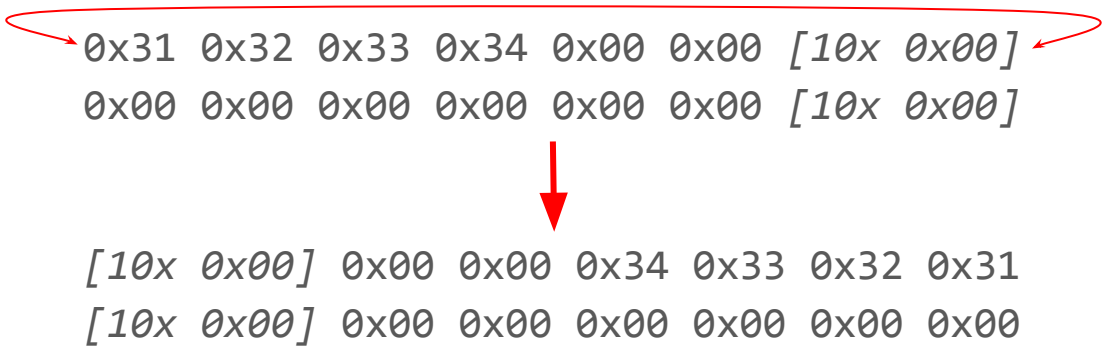
- Prvý pokus neúspešný

Dešifrovanie “cryptoblob”u na PC

- Prvý pokus neúspešný
- Zmeňme kľúč / tweak a sledujme, či výsledok dešifrovania krabičkou je identický s naším:
  - Čítanie sektoru 0 s kľúčom samých núl - identické dáta
  - Čítanie “cryptoblob”u s kľúčom samých núl - identické dáta
  - Poradie bajtov v kľúči?

Dešifrovanie “cryptoblob”u na PC

- Prvý pokus neúspešný
- Zmeňme kľúč / tweak a sledujme, čí výsledok dešifrovania krabičkou je identický s naším:
  - Čítanie sektoru 0 s kľúčom samých núl - identické dáta
  - Čítanie “cryptoblob”u s kľúčom samých núl - identické dáta
  - Poradie bajtov v kľúči?



Extrakcia kľúča

- Vieme kde sú magické bajty

```
00000000: 275d c925 4809 0000 2cfd 5e25 2cf9 244c  ']%H...,.^%,.$L
00000010: 4ac9 45f9 d549 472a 52ca 5f59 495b 2d0f  J.E..IG*R._YI[-.
00000020: 79ec 6cfc 58da 5fd7 85f3 dd7e f5db 62f2  y.l.X._....~..b.
00000030: daed ff6d 3acf f5d5 87d2 544b afac f537  ...m:.....TK...7
00000040: 7ecb 3f6b 28d8 a368 6a39 0000 0000 0000  ~.?k(..hj9......
00000050: 1363 0000 0000 0000 0000 0000 0000 0000  .c..............
00000060: 9e67 0000 0000 0000 0000 0000 0000 0000  .g..............
00000070: a967 0000 0000 0000 0000 0000 0000 0000  .g..............
00000080: 1863 0000 0000 0000 0000 0000 0000 0000  .c..............
00000090: 2367 0000 0000 0000 0000 0000 0000 0000  #g..............
000000a0: 2273 0000 0000 0000 0000 0000 0000 0000  "s..............
000000b0: 7363 0000 0000 0000 0000 0000 0000 0000  sc..............
000000c0: 7566 0000 0000 0000 0000 0000 0000 0000  uf..............
000000d0: a363 0000 0000 0000 0000 0000 0000 0000  .c..............
000000e0: 2267 0000 0000 0000 0000 0000 0000 0000  "g..............
000000f0: 7766 0000 0000 0000 0000 0000 0000 0000  wf..............
00000100: 7567 0000 0000 0000 0000 0000 0000 0000  ug..............
00000110: 2366 0000 0000 0000 0000 0000 0000 0000  #f..............
00000120: a266 0000 0000 0000 0000 0000 0000 0000  .f..............
00000130: b366 0000 0000 0000 0000 0000 0000 0000  .f..............
00000140: 17e6 0000 0000 0000 0000 0000 0000 0000  ................
00000150: 13c6 0000 0000 0000 0000 0000 0000 0000  ................
00000160: 8ae6 0000 0000 0000 0000 0000 0000 0000  ................
00000170: 89ce 0000 0000 0000 0000 0000 0000 0000  ................
00000180: 5cce 0000 0000 0000 0000 0000 0000 0000  \...............
00000190: 2acc 0000 0000 0000 0000 0000 0000 0000  *...............
000001a0: 73cc 0000 0000 0000 0000 0000 0000 0000  s...............
000001b0: 55cc 0000 0000 0000 0000 0000 0000 0000  U...............
000001c0: ab8c 0000 0000 0000 0000 0000 0000 0000  ................
000001d0: 3a99 0000 0000 0000 0000 0000 0000 0000  :...............
000001e0: c299 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 6a31 0000 0000 0000 0000 0000 0000 0000  j1..............
```

Extrakcia kľúča

- Vieme kde sú magické bajty

```
00000000: 275d c925 4809 0000 2cfd 5e25 2cf9 244c  ']%H...,.^%,.$L
00000010: 4ac9 45f9 d549 472a 52ca 5f59 495b 2d0f  J.E..IG*R._YI[-.
00000020: 79ec 6cfc 58da 5fd7 85f3 dd7e f5db 62f2  y.l.X._....~..b.
00000030: daed ff6d 3acf f5d5 87d2 544b afac f537  ...m:.....TK...7
00000040: 7ecb 3f6b 28d8 a368 6a39 0000 0000 0000  ~.?k(..hj9......
00000050: 1363 0000 0000 0000 0000 0000 0000 0000  .c..............
00000060: 9e67 0000 0000 0000 0000 0000 0000 0000  .g..............
00000070: a967 0000 0000 0000 0000 0000 0000 0000  .g..............
00000080: 1863 0000 0000 0000 0000 0000 0000 0000  .c..............
00000090: 2367 0000 0000 0000 0000 0000 0000 0000  #g..............
000000a0: 2273 0000 0000 0000 0000 0000 0000 0000  "s..............
000000b0: 7363 0000 0000 0000 0000 0000 0000 0000  sc..............
000000c0: 7566 0000 0000 0000 0000 0000 0000 0000  uf..............
000000d0: a363 0000 0000 0000 0000 0000 0000 0000  .c..............
000000e0: 2267 0000 0000 0000 0000 0000 0000 0000  "g..............
000000f0: 7766 0000 0000 0000 0000 0000 0000 0000  wf..............
00000100: 7567 0000 0000 0000 0000 0000 0000 0000  ug..............
00000110: 2366 0000 0000 0000 0000 0000 0000 0000  #f..............
00000120: a266 0000 0000 0000 0000 0000 0000 0000  .f..............
00000130: b366 0000 0000 0000 0000 0000 0000 0000  .f..............
00000140: 17e6 0000 0000 0000 0000 0000 0000 0000  ................
00000150: 13c6 0000 0000 0000 0000 0000 0000 0000  ................
00000160: 8ae6 0000 0000 0000 0000 0000 0000 0000  ................
00000170: 89ce 0000 0000 0000 0000 0000 0000 0000  ................
00000180: 5cce 0000 0000 0000 0000 0000 0000 0000  \...............
00000190: 2acc 0000 0000 0000 0000 0000 0000 0000  *...............
000001a0: 73cc 0000 0000 0000 0000 0000 0000 0000  s...............
000001b0: 55cc 0000 0000 0000 0000 0000 0000 0000  U...............
000001c0: ab8c 0000 0000 0000 0000 0000 0000 0000  ................
000001d0: 3a99 0000 0000 0000 0000 0000 0000 0000  :...............
000001e0: c299 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 6a31 0000 0000 0000 0000 0000 0000 0000  j1..............
```

Extrakcia kľúča

- Vieme kde sú magické bajty
- Metódou pokus-omyl sme našli kľúče key1, key2

```
00000000: 275d c925 4809 0000 2cfd 5e25 2cf9 244c  ']%H...,.^%,.$L
00000010: 4ac9 45f9 d549 472a 52ca 5f59 495b 2d0f  J.E..IG*R._YI[-.
00000020: 79ec 6cfc 58da 5fd7 85f3 dd7e f5db 62f2  y.l.X._....~..b.
00000030: daed ff6d 3acf f5d5 87d2 544b afac f537  ...m:.....TK...7
00000040: 7ecb 3f6b 28d8 a368 6a39 0000 0000 0000  ~.?k(..hj9......
00000050: 1363 0000 0000 0000 0000 0000 0000 0000  .c..............
00000060: 9e67 0000 0000 0000 0000 0000 0000 0000  .g..............
00000070: a967 0000 0000 0000 0000 0000 0000 0000  .g..............
00000080: 1863 0000 0000 0000 0000 0000 0000 0000  .c..............
00000090: 2367 0000 0000 0000 0000 0000 0000 0000  #g..............
000000a0: 2273 0000 0000 0000 0000 0000 0000 0000  "s..............
000000b0: 7363 0000 0000 0000 0000 0000 0000 0000  sc..............
000000c0: 7566 0000 0000 0000 0000 0000 0000 0000  uf..............
000000d0: a363 0000 0000 0000 0000 0000 0000 0000  .c..............
000000e0: 2267 0000 0000 0000 0000 0000 0000 0000  "g..............
000000f0: 7766 0000 0000 0000 0000 0000 0000 0000  wf..............
00000100: 7567 0000 0000 0000 0000 0000 0000 0000  ug..............
00000110: 2366 0000 0000 0000 0000 0000 0000 0000  #f..............
00000120: a266 0000 0000 0000 0000 0000 0000 0000  .f..............
00000130: b366 0000 0000 0000 0000 0000 0000 0000  .f..............
00000140: 17e6 0000 0000 0000 0000 0000 0000 0000  ................
00000150: 13c6 0000 0000 0000 0000 0000 0000 0000  ................
00000160: 8ae6 0000 0000 0000 0000 0000 0000 0000  ................
00000170: 89ce 0000 0000 0000 0000 0000 0000 0000  ................
00000180: 5cce 0000 0000 0000 0000 0000 0000 0000  \...............
00000190: 2acc 0000 0000 0000 0000 0000 0000 0000  *...............
000001a0: 73cc 0000 0000 0000 0000 0000 0000 0000  s...............
000001b0: 55cc 0000 0000 0000 0000 0000 0000 0000  U...............
000001c0: ab8c 0000 0000 0000 0000 0000 0000 0000  ................
000001d0: 3a99 0000 0000 0000 0000 0000 0000 0000  :...............
000001e0: c299 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 6a31 0000 0000 0000 0000 0000 0000 0000  j1..............
```

Extrakcia kľúča

- Vieme kde sú magické bajty
- Metódou pokus-omyl sme našli kľúče key1, key2
- Význam zvyšných bajtov nepoznáme

```
00000000: 275d c925 4809 0000 2cfd 5e25 2cf9 244c  '].%H...,.^%,.$L
00000010: 4ac9 45f9 d549 472a 52ca 5f59 495b 2d0f  J.E..IG*R._YI[-.
00000020: 79ec 6cfc 58da 5fd7 85f3 dd7e f5db 62f2  y.l.X._....~..b.
00000030: daed ff6d 3acf f5d5 87d2 544b afac f537  ...m:.....TK...7
00000040: 7ecb 3f6b 28d8 a368 6a39 0000 0000 0000  ~.?k(..hj9......
00000050: 1363 0000 0000 0000 0000 0000 0000 0000  .c..............
00000060: 9e67 0000 0000 0000 0000 0000 0000 0000  .g..............
00000070: a967 0000 0000 0000 0000 0000 0000 0000  .g..............
00000080: 1863 0000 0000 0000 0000 0000 0000 0000  .c..............
00000090: 2367 0000 0000 0000 0000 0000 0000 0000  #g..............
000000a0: 2273 0000 0000 0000 0000 0000 0000 0000  "s..............
000000b0: 7363 0000 0000 0000 0000 0000 0000 0000  sc..............
000000c0: 7566 0000 0000 0000 0000 0000 0000 0000  uf..............
000000d0: a363 0000 0000 0000 0000 0000 0000 0000  .c..............
000000e0: 2267 0000 0000 0000 0000 0000 0000 0000  "g..............
000000f0: 7766 0000 0000 0000 0000 0000 0000 0000  wf..............
00000100: 7567 0000 0000 0000 0000 0000 0000 0000  ug..............
00000110: 2366 0000 0000 0000 0000 0000 0000 0000  #f..............
00000120: a266 0000 0000 0000 0000 0000 0000 0000  .f..............
00000130: b366 0000 0000 0000 0000 0000 0000 0000  .f..............
00000140: 17e6 0000 0000 0000 0000 0000 0000 0000  ................
00000150: 13c6 0000 0000 0000 0000 0000 0000 0000  ................
00000160: 8ae6 0000 0000 0000 0000 0000 0000 0000  ................
00000170: 89ce 0000 0000 0000 0000 0000 0000 0000  ................
00000180: 5cce 0000 0000 0000 0000 0000 0000 0000  \...............
00000190: 2acc 0000 0000 0000 0000 0000 0000 0000  *...............
000001a0: 73cc 0000 0000 0000 0000 0000 0000 0000  s...............
000001b0: 55cc 0000 0000 0000 0000 0000 0000 0000  U...............
000001c0: ab8c 0000 0000 0000 0000 0000 0000 0000  ................
000001d0: 3a99 0000 0000 0000 0000 0000 0000 0000  :...............
000001e0: c299 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 6a31 0000 0000 0000 0000 0000 0000 0000  j1..............
```

Dešifrovanie disku na Linuxe

- Extrahujeme kľúče do súboru
- Využijeme dm-crypt

Dešifrovanie disku na Linuxe

- Extrahujeme kľúče do súboru
- Využijeme dm-crypt

```
cryptsetup --cipher=aes-xts-plain64 --key-size=512 \
--key-file=extracted.key open --type plain /dev/sdb enc

mount /dev/mapper/enc /mnt
```

Bruteforce

- Z “cryptoblob”u nám stačí dešifrovať prvý AES blok
  - Magické bajty sú prvé štyri
- Vieme vyskúšať všetky 12-miestne PINy
  - “embarrassingly parallel” úloha

Bruteforce

- Z “cryptoblob”u nám stačí dešifrovať prvý AES blok
  - Magické bajty sú prvé štyri
- Vieme vyskúšať všetky 12-miestne PINy
  - “embarrassingly parallel” úloha

- Náš proof-of-concept bruteforce: **2 dni**
- Paralelne na Google Cloud Platform: **5€ - 7€**

Efekt použitia PBKDF2

- Upravili sme firmvér, pridali sme do neho PBKDF2 (s SHA1-HMAC).
  - C implementácia z OpenBSD + vlastný linker skript

Efekt použitia PBKDF2

- Upravili sme firmvér, pridali sme do neho PBKDF2 (s SHA1-HMAC).
  - C implementácia z OpenBSD + vlastný linker skript

Počet iterácií	Čas behu na MCU	Čas útoku na 5-miestny PIN
0 (originálny firmvér)	59 ms	0.109 s
100	68 ms	6.3 s
1000	190 ms	1 min
10 000	**1 421 ms**	**10 min**

Ako rýchly je bruteforce teraz?

- Problém s PBKDF2 - dá sa efektívne implementovať na GPU a ASICoch
  - Citovaná práca uvádza 40x zrýchlenie voči CPU

Ako rýchly je bruteforce teraz?

- Problém s PBKDF2 - dá sa efektívne implementovať na GPU a ASICoch
  - Citovaná práca uvádza 40x zrýchlenie voči CPU

- Veľmi **hrubý** odhad:
  - Čistý čas: ~~ **4 roky**
  - Náklady v cloude (VM + GPU): **~~ 6400€**

- Zhruba 1000x zvýšenie ceny útoku hrubou silou

Aktualizácia firmvéru

- Neexistuje nástroj pre naše zariadenie.
- Existuje pre Zalman HE-130 ktoré tiež využíva INIC-3607E.

Aktualizácia firmvéru

- Neexistuje nástroj pre naše zariadenie.
- Existuje pre Zalman HE-130 ktoré tiež využíva INIC-3607E.

- Naše zariadenie nedokáže aktualizovať.
- Ak do nášho zariadenia nahráme firmvér HE-130, aktualizuje ho.

Aktualizácia firmvéru

- Neexistuje nástroj pre naše zariadenie.
- Existuje pre Zalman HE-130 ktoré tiež využíva INIC-3607E.

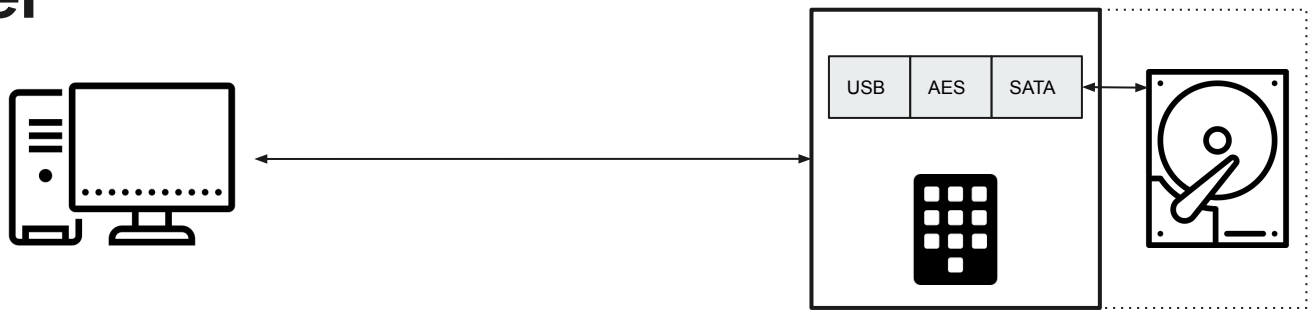
- Naše zariadenie nedokáže aktualizovať.
- Ak do nášho zariadenia nahráme firmvér HE-130, aktualizuje ho.

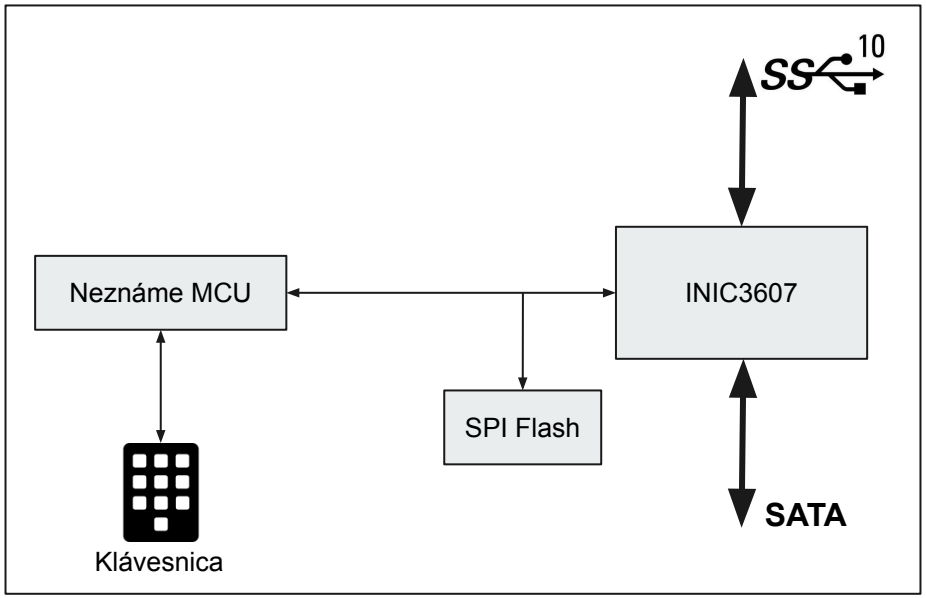
- V našom prípade asi vedľajší efekt zapojenia ovládača klávesnice - používa rovnaké PINy.
  - Ak je update funkcia implementovaná na úrovni IC, update mechanizmus si toho nemusí byť vedomý a update zlyhá.

Záver

Na začiatku to bola “čierna krabička”

Záver


USB
AES
SATA


SS 10
Neznáme MCU
INIC3607
SPI Flash
SATA
Klávesnica

Dosiahnuté výsledky

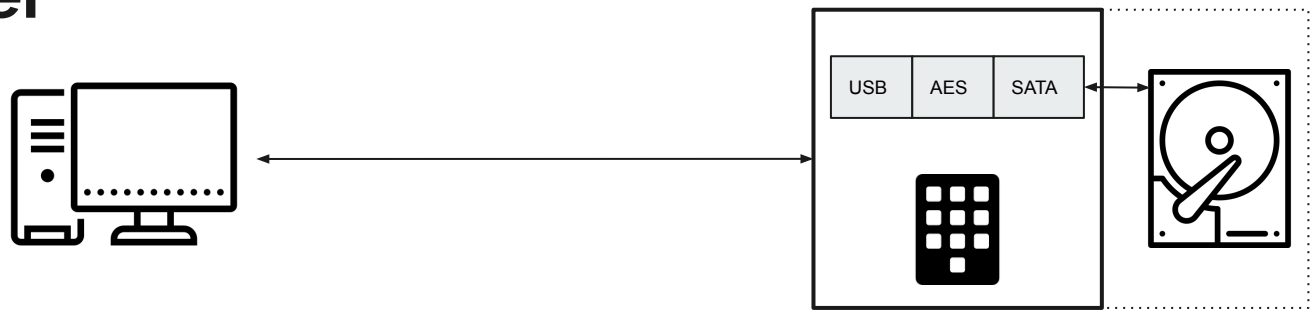
- Vieme dešiforvať disk pod Linuxom ak poznáme PIN
- Vieme dešifrovať disk ak **nepoznáme** PIN
  - Praktický bruteforce útok
  - Situáciu vieme cca 1000x zlepšiť softvérovou aktualizáciou
- Nevieme bez autorizácie aktualizovať firmvér
  - Ale to je možno len náhoda, a vieme to urobiť u iných zariadení.

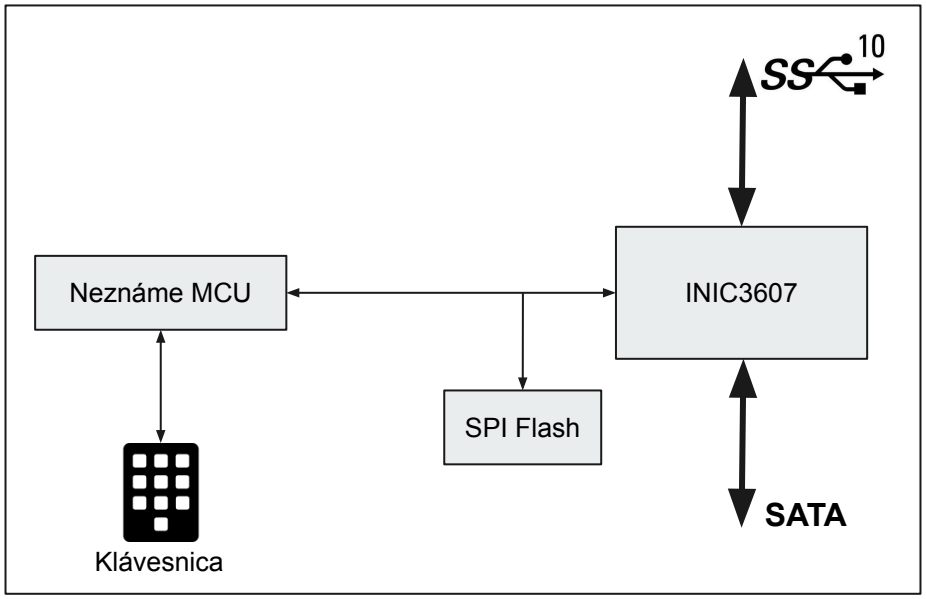
Dosiahnuté výsledky

- Vieme dešiforvať disk pod Linuxom ak poznáme PIN
- Vieme dešifrovať disk ak **nepoznáme** PIN
  - Praktický bruteforce útok
  - Situáciu vieme cca 1000x zlepšiť softvérovou aktualizáciou
- Nevieme bez autorizácie aktualizovať firmvér
  - Ale to je možno len náhoda, a vieme to urobiť u iných zariadení.

- Detailne spísané techniky analýzy aplikovateľné na iné MCU architektúry ARCompact
- Vlastný nástroj `dumppoint-tool`

Záver


USB
AES
SATA


10
Neznáme MCU
INIC3607
SPI Flash
SATA
Klávesnica