RETRO-new: **HELLENA-51**

(Crack by: O. Kowalczuk & Hannibal, 2012)

Tento malý grécky mikropočítač sa objavil v podobe stavebnice ešte v roku 2001. Bol nástupcom svojho času populárneho jednodeskáča EMA-51 a jeho rework, (podobne, ako napr. rework japonského Gakkenu-GMC4) sa objavil ešte raz v roku 2009/10 v podaní mladých študentov s podtitulom „Children of TROY". Žiaľ kríza a politická situácia v grécku spôsobila, že sa táto stavebnica akosi „vyparila"...

Poliak **O.Kowalczuk**, ktorý napálený procesor do Helleny-51 a aj predlohu dosky pre EAGLE zohnal od Eniklesa Myrthiu, jedného z autorov Helleny – s ním hodil aj reč o tom, **„ako je to vyriešené"**. Sebavedomý Enikles pokojne všetko opísal:MCU používaný v reworkovej Hellene-51 je ATMEL89C51AC2 a pre jeho napálenie je nutný nielen **SW**, ktorým je **„RAOS_v0.15b"** (32kB), ale aj **bootovacia náhrada** namiesto pôvodného „BOOTLoadera_v1.4.1", ktorý napaľuje do procesorov firma Atmel. Ide o tzv: **„RAOS-uboot_v1.0"** (1kB), ktorý do lokácie od 0xF800 (bank FM1 v MCU) dostanete jedine **drahým paralelným programátorom** týchto čipov.

Prečo je to takto komlikované?

Gréci si totiž vymysleli **„ochranu" SW**. Po zostavení stavebnice bolo nutné spustiť Hellenu na dvakrát: Prvým zapnutím sa vynútila **aktivita „RAOS-ubootu"**, ktorý mal jedinú úlohu: poprepisovať a poupravovať niektoré cfg-registre a bajty v rôznych miestach SW „RAOSu", napáleného v banku FM0 procesora. Po doporučovanej dobe čakania – 3sec. mal užívateľ mikropočítač vypnúť a po opätovnom zapnutí už Hellena vždy normálne nabiehala. Pravdaže dotyčný „RAOS" si vždy po štarte, či resete procesora kontroluje práve zmeny, ktoré prvým zapnutím previedol „RAOS-uboot".

Ako nápad to nebolo zlé, lenže... ☺

Napálený MCU do Helleny som si vtedy (ne)legálne zakúpil aj ja, mikropočítač som „zadrátoval" na univerzálke podľa schémy a predošlým postupom úspešne rozchodil. **Podľa očakávania – dotyčný „RAOS-uboot"** sa postaral o to, aby **procesor zostal chránený voči čítaniu obsahu pamäte** cez ISP...
Mal som však hexový výpis z EPROM predchodcu Helleny: mikropočítača EMA-51 (SW bol „RAOS v0.10b") a práve **vtedy ma napadla jedna vec:** Pri náhodnom prezeraní si hexa výpisu „RAOSu" z EMY-51 mi náhle pred očami skrsol hneď na začiatku tento riadok, v ktorom som si všimol malej časti kódu:

```
:1000800001677914E49311D9A3D9F92279082323BC
:10009000234440115911840167E9B49400400224BB
:1000A0002C11D4E493227D0078FE7B037AFE7C0839
:1000B0007900E8F323F80909E344F0006A60080DC9
:1000C000DCEEEA23FADBE722E493FF740193F58286
```

Ide o sekvenciu z konca nejakého podprogramu – **CLR A, MOVC A, @A+PC, RET.** Tak – to vzbudilo nádej, či nie je náhodou „RAOS" Helleny a EMY v tom mieste zhodný, pretože Hellena má svojimi vlastnými editormi **znemožnený prístup ku svojmu „RAOSu" v lokácii FM0 (0x0 - 0x7FFFh)**. Tak som Hellenu pripojil cez RS232 na PC a napísal v CHARONe krátky program, ktorý odkazoval volanie na tú adresu:

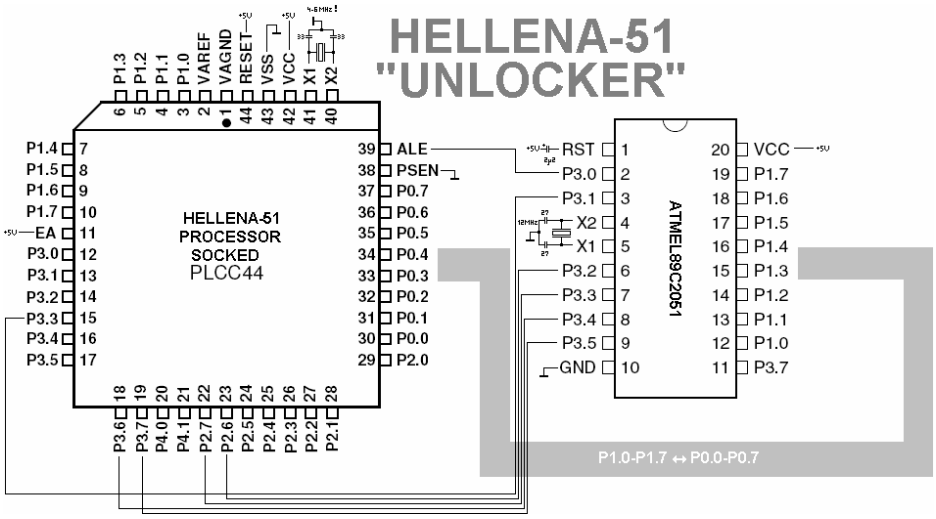
```
;----TXD-FM0-----          inc DPTR          !break stop!
        acall serialinit  acall transmit    ;----CALLS-----
        mov DPTR, #0      mov A, DPTh       …
loop:   lcall $0x00A3h    cjne A, #80, loop …
```

Spustením v exe-RAM Helleny tá následne "vypľula" celý svoj "RAOS" na sériový port! Takže úsek 0x00A3-0x00A5h sedel! Na porte ho už odchytil CHARON a vytvoril z neho Intel-hexový formát. Pre zaujímavosť som si ho porovnal s "RAOSom" EMY-51: má kvantum rozdielov…

Takže "RAOS_v0.15b", upravený **už teraz nepotrebnou náhradou "RAOSu-uboot_v1.0"** bol na svete! **Vypálil som ho** pomocou programu "FLIP" **do ďalšieho procesora** a zastrčil do pätice Helleny. **Šlapalo to okamžite, až na jeden zádrhel:** nešla exekutíva z užívateľskej RAM, začínajúcej od 0x8000h. Mohlo za to defaultné nastavenie HW bytu výrobcom, ktoré má level 4:

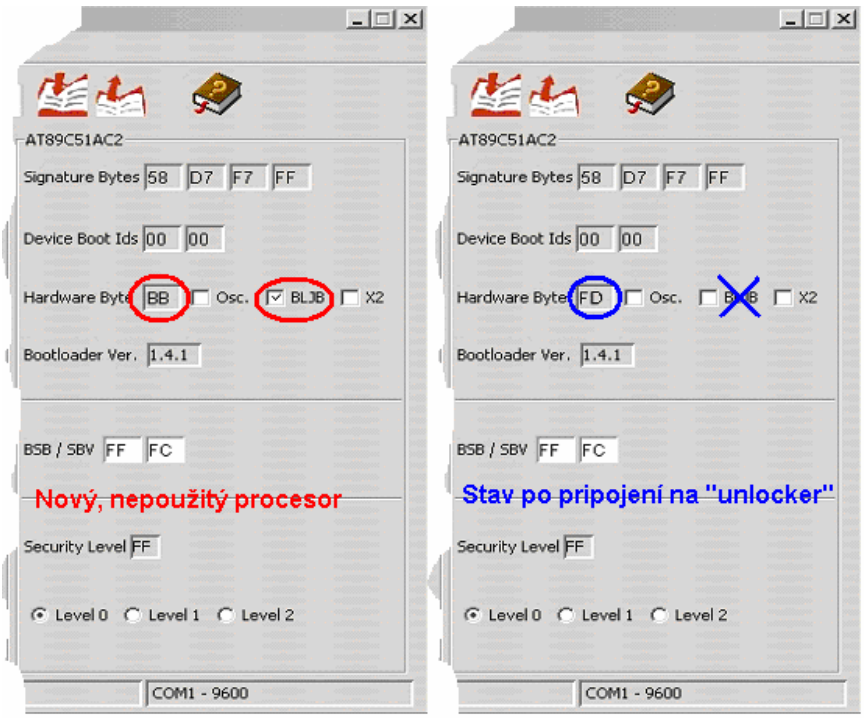
Program Lock Bits				Program Lock bits U: unprogrammed P: programmed
Security Level	LB0	LB1	LB2	Protection Description
1	U	U	U	No program lock features enabled. MOVC instruction executed from external program memory returns non coded data.
2	P	U	U	MOVC instructions executed from external program memory are barred to return code bytes from internal memory, $\overline{EA}$ is sampled and latched on reset, and further parallel programming of the Flash is disabled.
3	U	P	U	Same as 2, also verify through parallel programming interface is disabled.
4	U	U	P	Same as 3, also external execution is disabled if code roll over beyond 7FFFh

Žiaľ – hardwarový lock bit procesora nie je možné pomocou ISP meniť, jediná možnosť je použiť drahý paralelný programátor tohoto obvodu. Preto som o všetkom napísal Kowalczukovi a ten mi pomohol: problém vyriešil primitívnou aplikáciou, ktorú nazval: **Hellena-51"unlocker"**.



Ako teda na to…

1. Vložte procesor pre Hellenu-51 do "unlockeru", zapnite napájanie a počkate cca.1-2 sec.
2. Pripojte procesor pre Hellenu-51 cez ISP na PC a spustite program "FLIP". Vyvolajte BOOTLoader (/PSEN na GND pred zapnutím napájania!) cez ktorý sa s procesorom spojíte a skontrolujete status HW registra podľa tohoto obrázku:



3. Nakoniec napálte cracknutý program RAOS_v0.15b/L (LITE verzia) a procesor je možné zasunúť do pätice mikropočítača. Týmto pádom by už malo všetko pracovať správne a jednoduchý mikrokomp z pouhých 4-roch IO je pripravený pre používanie…

Takže – pre všetkých fanúšikov RETRO noviniek: HELLENA-51. ☺