Anything Goes

Sunday, January 13, 2019

Ikea Ansluta Hacking - reverse engineering the firmware

Since acquiring target control via Spy-Bi-Wire and LaunchPad I am able to inspect and dump flash, disassemble and program back the flash to original stage

The extracted files are in git here:
https://github.com/michkrom/msp430-ansluta/tree/master/original

Dumping Flash

In .hex intell format that is usable to programming it back:

```
mspdebug rf2500 "hexout 0xf800 2048 flash.hex"
```

In .raw binary format

```
mspdebug rf2500 "save_raw 0xf800 2048 flash.raw"
```

Reprogramming back to original

Use .hex Intel format

```
mspdebug rf2500 "prog flash.hex"
```

Disassembling flash

```
mspdebug rf2500 "dis 0xf800 2048 flash.dis"
```

Things learned from the disassembly:

- Operating mode is low power state LM3 and waking on interrupt from key press (connected to P2.7). However, LM1 is also entered after key press, perhaps to await for another key press before going LM3. Does this save energy?
- Apparently, the randomization of remote's ID is done via...an ADC reads which ends up as middle 4 bytes of the message (each ADC read uses only lowest bit). That likely saves mfg time instead of individually programming each remote with ID - this is smart!
- The SPI communication with CC2500 is bit-banged (not using build-in MSP's SPI engine). This is likely due to messed up hw design - the MOSI/MISO lines are switched from their default pins:

```
MSP430       Device
--------------------------------------
     P1.0    LED
RXD  P1.1    unused?
TXD  P1.2    CC2500 CS
     P1.3    CC2500 GDO0
     P1.4    CC2500 GDO2
SCLK P1.5    CC2500 SCLK
SOMI P1.6    CC2500 SI
SIMO P1.7    CC2500 SO
     P2.6    unused (N-FET's Gate in transformer)
     P2.7    Key (switch)
```

Posted by Unknown at 3:59 PM

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)