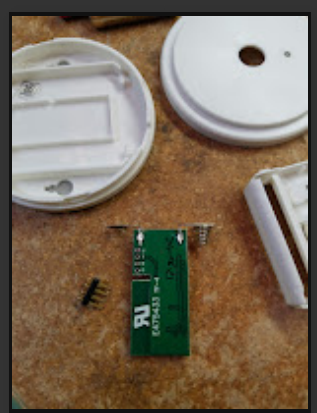
# Anything Goes

Saturday, January 12, 2019

## Ikea Ansluta Hacking - target control via TI's lunchpad

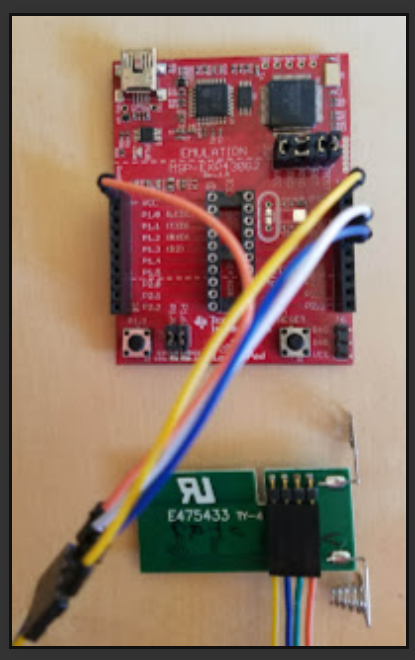
Notes of hacking Ikea Ansluta LED lighting.



*Notably, this is less important now as Ikea's own smart home gateway TRÅDFRI solves the problem of controlling Ansluta lights via home automation. Although, the system is very hack-able likely for other purposes.*

### Hardware

Both the remote and power supplies are based on TI's MSP430 G2231 and CC2500 RF transciver. The Ansluta's PCBs have programming/debugging headers ready for hacking.



The 4 Pin Header by the Bat+ label (top) has the following pins: Vcc, T, R, Gnd (clearly labeled).

I connected these to LP EXP430 Spy-Bi-Wire

```
Vcc --> VCC (1)
T   --> TEST(17)
R   --> RST (18)
Gnd --> GND (20)
```

The LunchPad Exp439G2 will power up the remote, no need for batteries. Just remove the actual MPU from the socket. And...do not try this with transformer! this is dangerous as it's directly powered from power line.

IKEA ANSLUTA - Remote and LED power supply connections

| MSP430 G2231 | | Remote | Transformer |
|---|---|---|---|
| Pin | Function | Connection | Connection |
| 1 | Vcc | Bat+ | Vcc |
| 2 | p1.0 | LED | LED |
| 3 | p1.1 | ? | ? |
| 4 | p1.2 | CC2500 CSn | CC2500 CSn |
| 5 | p1.3 | CC2500 GDO0 | CC2500 GDO0 |
| 6 | p1.4 | CC2500 GDO2 | CC2500 GDO2 |
| 7 | p1.5 | CC2500 SCLK | CC2500 SCLK |
| 8 | p1.6 | CC2500 SI | CC2500 SI |
| 9 | p1.6 | CC2500 SO | CC2500 SO |
| 10 | SBWTDIO | Hdr R | Hdr R |
| 11 | SBWTCK | Hdr T | Hdr T |
| 12 | P2.7 | Key | Key |
| 13 | P2.6 | ? | N-FET Gate |
| 14 | Vss | Bat- | Gnd |

### Software

#### Debugging the target

I am using lubuntu 18.04 and mspdebug (0.25/compiled locally). and I am able to connect and break into the running code.

Invoke (may need sudo):

```
mspdebug rf2500
```

Here is output (parts removed - there are complains about FET interface not working...)

```
Using Olimex identification procedure
Device ID: 0xf201
  Code start address: 0xf800
  Code size         : 2048 byte = 2 kb
  RAM  start address: 0x200
  RAM  end   address: 0x27f
  RAM  size         : 128 byte = 0 kb
Device: F20x2_G2x2x_G2x3x
Number of breakpoints: 2
fet: FET returned NAK
warning: device does not support power profiling
Chip ID data:
  ver_id:         01f2
  ver_sub_id:     0000
  revision:       40
  fab:            40
  self:           0000
  config:         02
  fuses:          00
Device: F20x2_G2x2x_G2x3x
```

run & break

```
(mspdebug) run
Running. Press Ctrl+C to interrupt...
^C
    ( PC: 0fc9e)  ( R4: 077fd)  ( R8: 0ff17)  (R12: 00000)
    ( SP: 0027a)  ( R5: 0bf96)  ( R9: 09ff6)  (R13: 00006)
    ( SR: 000da)  ( R6: 0fffc)  (R10: 0ff7f)  (R14: 00006)
    ( R3: 00000)  ( R7: 0efcd)  (R11: 00200)  (R15: 00008)
0xfc9e:
    0fc9e: 30 41                    RET
    0fca0: 0e 43                    CLR     R14
    0fca2: 3e 90 2f 00              CMP     #0x002f, R14
    0fca6: 09 2c                    JC      0xfcba
    0fca8: 4c 4e                    MOV.B   R14,    R12
    0fcaa: 5d 4e 8a fd              MOV.B   0xfd8a(R14), R13
(mspdebug)
```

Next? Replace it with my own fw...when I have more time.

**Arduino with CC2250**
Here is my version of Arduino+CC2500 that is based on a great work done here.

It works!

## References

**spreasheet with MPC pin connections**

https://github.com/NDBCK/Ansluta-Remote-Controller

https://tildeslash.dk
/Hacking%20IKEA%20Ansluta%20remote%20switch%20to%20work%20with%20Alexa.html

TI Spy-by-wire

mspdebug+lunchpad

mspdebug+gdb

Posted by Unknown at 12:01 PM

## No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Simple theme. Powered by Blogger.