Enalbe monitor mode for the Nexus 5

{dwegemer, mschulz} @ seemoo.de
nexmon.org

32c3

Disclaimer

nexmon

Please don’t sue us!

Monitor what?

nexmon

We need:

802.11 **Management**, **Control** and Data frames

Promisc Mode: get all frames on the ether, not only the ones which are addressed to us

Why monitor mode on mobile phones?

nexmon

Move from this …

… to that

Image Source: icanhas.cheezburger.com

Related Work

nexmon

BCMON: bcm4329 + bcm4330

monmob: bcm4325 + bcm4329

nexmon: bcm4339

Image Source: ifixit.com

DIY: 384 easy steps to enable monitor mode

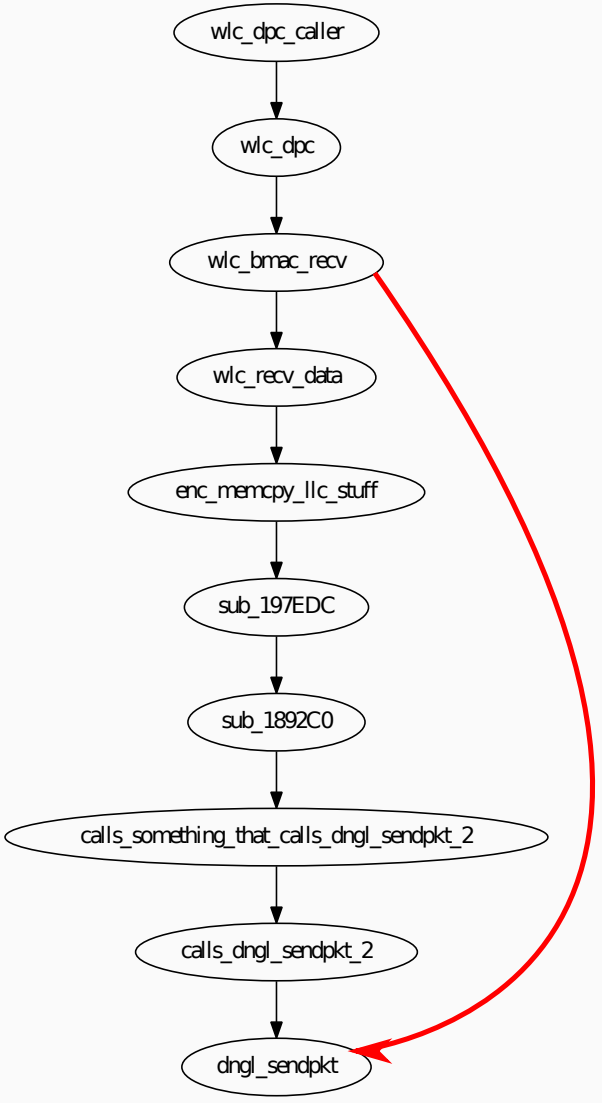
nexmon

1. Extract ROM + RAM

DIY: 384 easy steps to enable monitor mode

nexmon

2. Find the RX path



DIY: 384 easy steps to enable monitor mode

nexmon

3. Patch necessary parts:

Frame handler: wlc_bmac_recv()

```
RAM:001AAD98
RAM:001AAD98                ; =============== S U B R O U T I N E =======================================
RAM:001AAD98
RAM:001AAD98
RAM:001AAD98                ; int __fastcall wlc_bmac_recv(wlc_hw_info *wlc_hw_info_ptr, int fifo, int bound,
RAM:001AAD98                wlc_bmac_recv                           ; CODE XREF: j_wlc_bmac_recv↑j
RAM:001AAD98
RAM:001AAD98                var_40          = -0x40
RAM:001AAD98                fifo_local      = -0x3C
RAM:001AAD98                p               = -0x34
RAM:001AAD98                tsf_h           = -0x30
RAM:001AAD98                tsf_l           = -0x2C
RAM:001AAD98
RAM:001AAD98 2D E9 F0 4F                    PUSH.W          {R4-R11,LR} ; Push registers
RAM:001AAD9C 99 46                          MOV             R9, R3  ; Rd = Op2
RAM:001AAD9E 03 68                          LDR             R3, [R0] ; Load from Memory
RAM:001AADA0 87 B0                          SUB             SP, SP, #0x1C ; Rd = Op1 - Op2
RAM:001AADA2 04 46                          MOV             R4, R0  ; Rd = Op2
RAM:001AADA4 01 91                          STR             R1, [SP,#0x40+fifo_local] ; Store to Memory
RAM:001AADA6 1B 68                          LDR             R3, [R3] ; Load from Memory
RAM:001AADA8 93 F8 E7 A0                    LDRB.W          R10, [R3,#0xE7] ; Load from Memory
RAM:001AADAC 1A B1                          CBZ             R2, loc_1AADB6 ; Compare and Branch on Zero
RAM:001AADAE 9B 6A                          LDR             R3, [R3,#0x28] ; Load from Memory
RAM:001AADB0 D3 F8 40 B0                    LDR.W           R11, [R3,#0x40] ; Load from Memory
RAM:001AADB4 01 E0                          B               loc_1AADBA ; Branch
RAM:001AADB6                ; ---------------------------------------------------------------------------
RAM:001AADB6
RAM:001AADB6                loc_1AADB6                              ; CODE XREF: wlc_bmac_recv+14↑j
RAM:001AADB6 4F F0 FF 3B                    MOV.W           R11, #0xFFFFFFFF ; Rd = Op2
001AAD98 001AAD98: wlc_bmac_recv
```

MAC control flags: wlc_coreinit()

```
RAM:001AB66C                ; =============== S U B R O U T I N E =======================================
RAM:001AB66C
RAM:001AB66C                ; d11 core init
RAM:001AB66C                ;    reset PSM
RAM:001AB66C                ;    download ucode/PSM
RAM:001AB66C                ;    let ucode run to suspend
RAM:001AB66C                ;    download ucode inits
RAM:001AB66C                ;    config other core registers
RAM:001AB66C                ;    init dma
RAM:001AB66C
RAM:001AB66C                ; void __fastcall wlc_coreinit(wlc_hw_info *wlc_hw)
RAM:001AB66C                wlc_coreinit                            ; CODE XREF: wlc_bmac_init+4E↓p
RAM:001AB66C                                                        ; DATA XREF: RAM:off_180D78↑o
RAM:001AB66C
RAM:001AB66C                var_28          = -0x28
RAM:001AB66C
RAM:001AB66C 2D E9 F7 43                    PUSH.W          {R0-R2,R4-R9,LR} ; Push registers
RAM:001AB670 04 46                          MOV             R4, R0  ; Rd = Op2
RAM:001AB672 4F F0 FF 31                    MOV.W           R1, #0xFFFFFFFF ; Rd = Op2
RAM:001AB676 0A 4A                          LDR             R2, =0x4000404 ; Load from Memory
RAM:001AB678 01 27                          MOVS            R7, #1  ; Rd = Op2
RAM:001AB67A D0 F8 84 50                    LDR.W           R5, [R0,#0x84] ; Load from Memory
RAM:001AB67E 06 68                          LDR             R6, [R0] ; Load from Memory
RAM:001AB680 A3 F6 FE FC                    BL              wlc_bmac_mctrl ; Branch with Link
RAM:001AB684 20 46                          MOV             R0, R4  ; wlc_hw_info_ptr
RAM:001AB686 A1 F6 89 FF                    BL              wlc_coreinit_ucode_download ; Branch with Link
RAM:001AB68A 20 46                          MOV             R0, R4  ; wlc_info_ptr
RAM:001AB68C A4 F6 78 FE                    BL              wlc_coreinit_wait_ucode_selfsuspend ; Branch with Link
RAM:001AB690 20 46                          MOV             R0, R4  ; wlc_info_ptr
001AB66C 001AB66C: wlc_coreinit
```

DIY: 384 easy steps to enable monitor mode

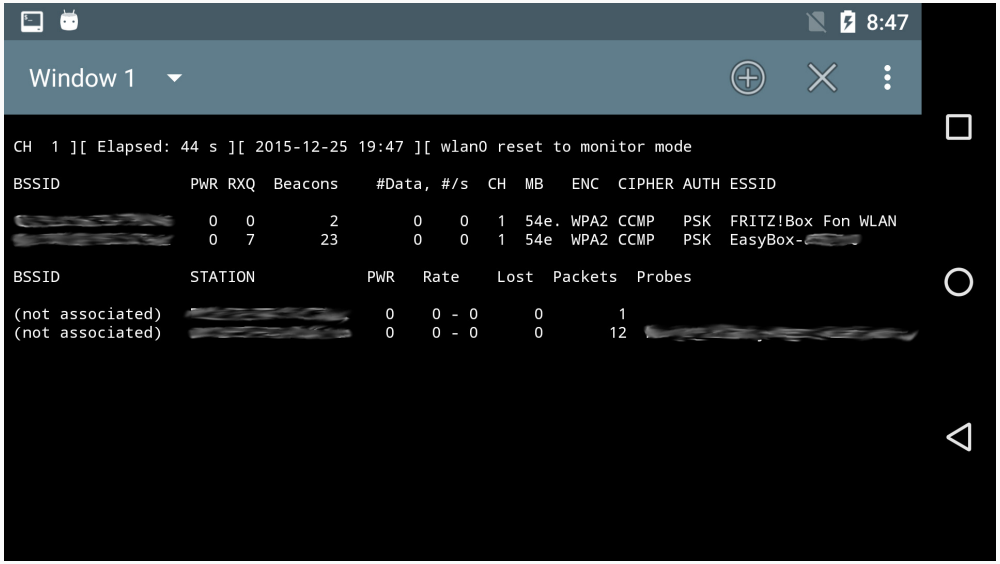
nexmon

379. Write binary patches in C:

```
int wlc_bmac_recv(struct wlc_hw_info *wlc_hw, uint fifo, bool bound, int *cnt) {
    struct sk_buff *p;
    while( (p = dma_rx (wlc_hw->di[fifo])) ) {
      dngl_sendpkt(SDIO_INFO_ADDR, p, 0xF);
    }
    dma_rxfill(wlc_hw->di[fifo]);
    return 0;
}
```

Future Work

nexmon



TX path: **injection support**

Fix Radiotap header: set RSSI / channel information

Improve stability

More information

nexmon

Code + Android boot ROM:
nexmon.org

Read our technical report:
NexMon: A Cookbook for Firmware Modifications on Smartphones to Enable Monitor Mode (available at nexmon.org)

Contact:

Daniel Wegemer:
dwegemer@seemoo.de; talk to me;
call me via DECT/GSM (2412/2414)
Matthias Schulz:
mschulz@seemoo.de