RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SBX1-W4

IOT HARDWARE HACKING - DEMOING FIRMWARE EXTRACTION AND PROTECTION METHODS

Deral Heiland

Research Lead (IoT)
Rapid7
@percent_x

Nathan Sevier

Senior Security Consultant
Rapid7
@__r4ge__

Agenda

- Why is hardware security important?
- How is hardware security compromised?
- What security methods are available for prevention?

WHY

Hardware security is important

Protecting intellectual property

```
00001AD0   00 00 30 43  6C 61 73 73  69 63 20 41  36 30 20 52  47 42 57 00  00 00 30 32  ..0Classic A60 RGBW...02
00001AE8   30 31 34 30  33 33 31 49  54 4F 53 2A  2A 2A 2A 00  00 00 FF 28  09 D0 41 F2  0140331ITOS****....(..A.
00001B00   10 01 DF F8  F4 2A 12 68  8A 5C 90 42  89 41 C9 0F  00 E0 00 21  08 46 70 47  .....*.h.\.B.A.....!.FpG
00001B18   01 70 C0 F8  01 20 70 47  0C B5 01 70  40 1C 00 A9  05 22 02 F7  06 FD 03 BD  .p... pG...p@....".......
00001B30   01 22 00 F0  1F 03 9A 40  80 28 0F D2  40 11 DF F8  B8 3A 1B 68  03 EB 80 00  ."....@.(..@....:.h....
00001B48   4F F4 80 53  00 29 19 58  02 D0 11 43  19 50 70 47  91 43 19 50  70 47 80 28  O..S.).X...C.PpG.C.PpG.(
00001B60   01 D3 00 20  70 47 01 21  00 F0 1F 02  91 40 40 11  DF F8 88 2A  12 68 02 EB  ... pG.!.....@@....*.h..
00001B78   80 00 00 F5  80 50 00 68  08 40 40 1E  80 41 C0 0F  70 47 2D E9  F8 43 DF F8  .....P.h.@@..A..pG-...C..
00001B90   68 4A 10 22  00 21 20 68  00 F5 80 50  06 F7 7B FC  00 25 05 E0  01 21 28 46  hJ.".! h...P..{..%....!(F
00001BA8   C0 B2 FF F7  C1 FF 6D 1C  04 2D F7 D3  00 25 41 F2  8B 17 0C E0  01 21 20 68  ......m..-...%A......! h
00001BC0   30 18 38 5C  40 44 C0 B2  FF F7 B2 FF  08 F1 01 08  C8 45 F3 D3  6D 1C 20 68  0.8\@D...........E..m. h
00001BD8   41 F2 10 01  09 5C 8D 42  18 D2 05 EB  45 01 4E 00  30 18 39 5C  FF 29 F1 D0  A....\.B....E.N.0.9\.)..
00001BF0   41 F2 8D 11  0A 58 00 2A  02 D1 4F F0  01 09 06 E0  10 46 00 1D  00 0B 00 F1  A....X.*..O......F......
00001C08   01 09 5F FA  89 F9 4F F0  00 08 DD E7  BD E8 F1 83  41 F2 12 00  DF F8 DC 19  .._...O..........A......
00001C20   09 68 40 5C  70 47 02 28  01 D0 03 28  04 D1 B1 F5  00 5F 80 41  C0 0F 70 47  .h@\pG.(...(......_.A..pG
00001C38   52 28 01 D1  01 20 70 47  40 06 FB D5  40 F6 F4 70  81 42 80 41  C0 0F 70 47  R(... pG@...@..p.B.A..pG
00001C50   FF 28 01 D1  00 20 70 47  41 06 01 D5  01 20 70 47  01 28 FB D0  3E 28 F9 D0  .(... pGA.... pG.(..>(..
00001C68   3F 28 [illegible]  (...(...(...(...(..
00001C80   80 28 [illegible]  (...(...(.......!..I...
00001C98   D4 2A 12 68  41 F2 10 03  9D 5C 99 42  0B D2 41 F2  8C 13 01 EB  41 04 02 EB  .*.hA....\.B..A.....A...
00001CB0   44 02 9A 5C  82 42 ED D1  08 46 C0 B2  00 E0 FF 20  10 BC 70 47  2D E9 F6 47  D..\.B...F..... ..pG-..G
00001CC8   82 B0 80 46  1D 46 0C 9C  DD F8 09 90  09 F1 08 00  80 08 4F EA  80 0A BA F5  ...F.F............O......
00001CE0   80 5F 02 D9  DF F8 8C 0A  8D E0 08 F6  F8 76 04 23  01 AA 31 46  00 20 05 F7  ._..........v.#..1F. ..
00001CF8   D4 F9 00 28  F2 D1 01 21  14 20 01 F0  99 F8 DF F8  F0 78 00 2C  17 D1 03 21  ...(...!. .......x.,...!
00001D10   AA F1 01 00  03 F7 6F FA  01 20 05 F0  9E F9 53 46  3A 68 41 46  00 20 05 F7  ......o.. ....SF:hAF. ..
00001D28   BC F9 04 46  00 20 05 F0  94 F9 00 2C  D6 D1 03 F7  79 FA 00 90  0F E0 AA EB  ...F. .....,.....y.......
00001D40   09 00 42 1F  FF 21 38 68  48 44 40 1D  06 F7 A3 FB  52 46 92 B2  39 68 03 20  ..B..!8hHD@.....RF..9h.
00001D58   03 F7 7C FA  00 90 01 98  10 F1 01 0F  36 D1 ED B2  00 2D 02 D0  DF F8 14 0A  ..|.........6....-......
00001D70   49 E0 04 23  00 AA 31 46  00 20 05 F7  2D F9 00 28  02 D0 DF F8  F0 49 3D E0  I..#..1F. ..-..(.....I=.
00001D88   04 23 01 AA  31 46 00 20  05 F7 87 F9  00 28 10 D1  01 98 00 99  88 42 0C D1  .#..1F. .....(.......B..
00001DA0   DF F8 D8 49  9D F8 08 00  39 68 40 18  90 F8 D3 1F  41 F0 01 01  80 F8 D3 1F  ...I....9h@.....A.......
00001DB8   24 E0 DF F8  B8 49 9D F8  08 00 39 68  40 18 90 F8  D3 1F 01 F0  FE 01 80 F8  $....I....9h@...........
00001DD0   D3 1F 17 E0  9D F8 08 00  39 68 40 18  00 99 01 9A  91 42 08 D0  DF F8 98 49  ........9h@......B.....I
00001DE8   90 F8 D3 1F  01 F0 FE 01  80 F8 D3 1F  06 E0 00 24  90 F8 D3 1F  41 F0 01 01  ..............$....A...
00001E00   80 F8 D3 1F  20 46 04 B0  BD E8 F0 87  38 B5 0C 46  00 F6 FC 75  04 23 00 AA  .... F......8..F...u.#..
00001E18   29 46 00 20  05 F7 41 F9  00 28 02 D0  DF F8 4C 0B  32 BD DF F8  48 1B 00 9A  )F. ..A..(....L.2...H...
00001E30   8A 42 23 D0  10 46 C0 43  1E D1 00 2C  02 D0 DF F8  38 0B 32 BD  00 91 04 23  .B#..F.C...,....8.2....#
```

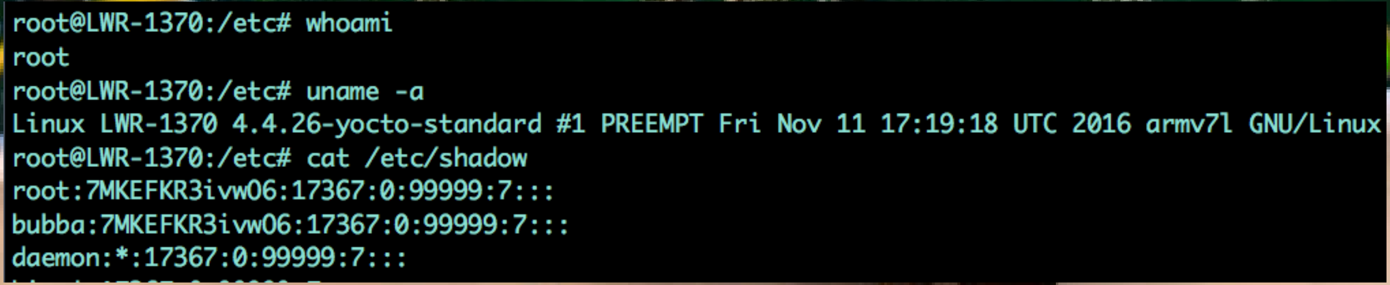
Why

Mitigate and protecting brand reputation

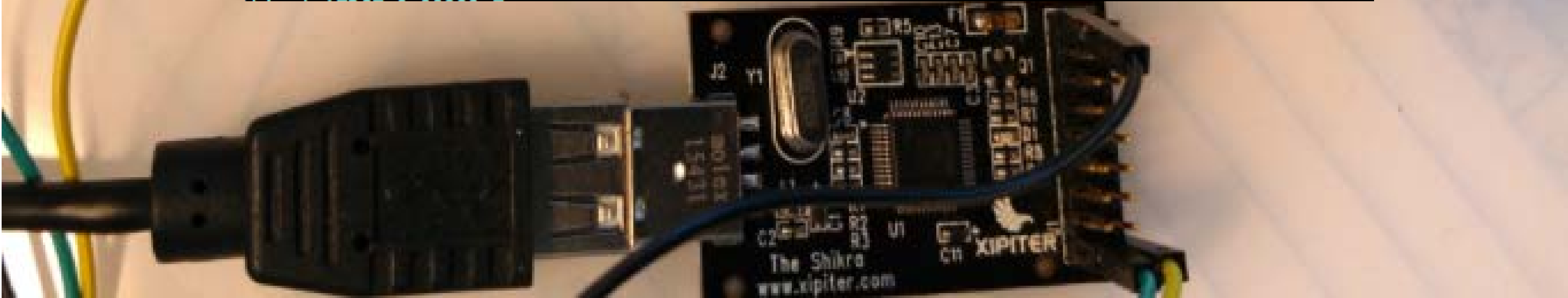
“It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.”

--Warren Buffett--

Protect against device compromise



```
root@LWR-1370:/etc# whoami
root
root@LWR-1370:/etc# uname -a
Linux LWR-1370 4.4.26-yocto-standard #1 PREEMPT Fri Nov 11 17:19:18 UTC 2016 armv7l GNU/Linux
root@LWR-1370:/etc# cat /etc/shadow
root:7MKEFKR3ivw06:17367:0:99999:7:::
bubba:7MKEFKR3ivw06:17367:0:99999:7:::
daemon:*:17367:0:99999:7:::
```

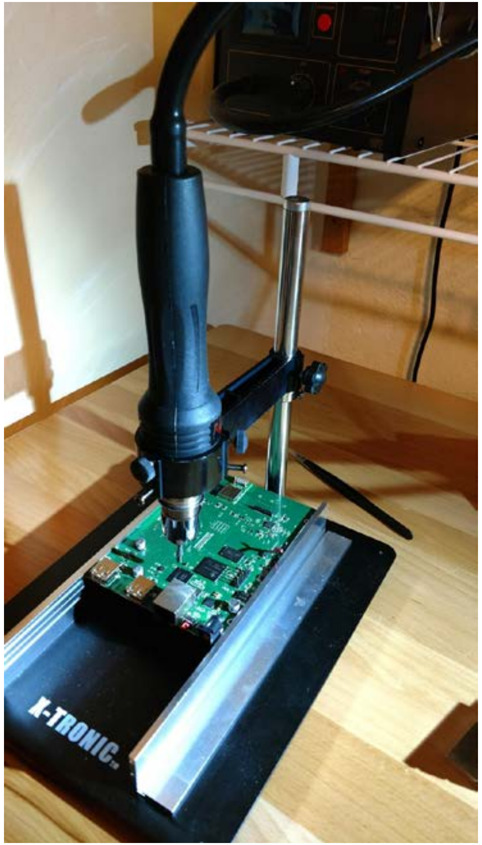


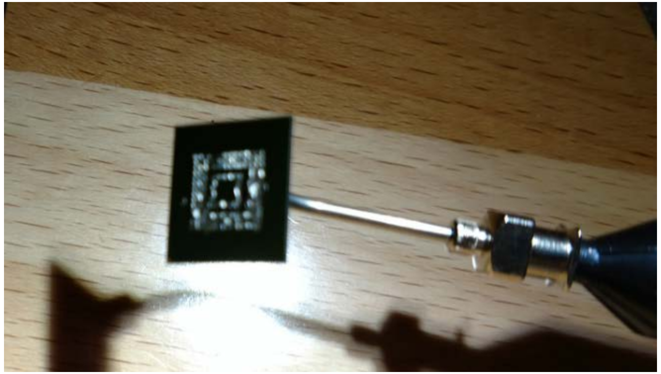
HOW

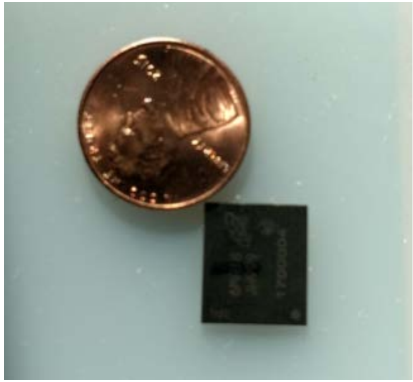
Demo examples of device compromise and firmware extraction

Extracting Memory Chips

- Destructive
- Flash
  - SPI
  - NAND/NOR
  - eMMC
- Demo

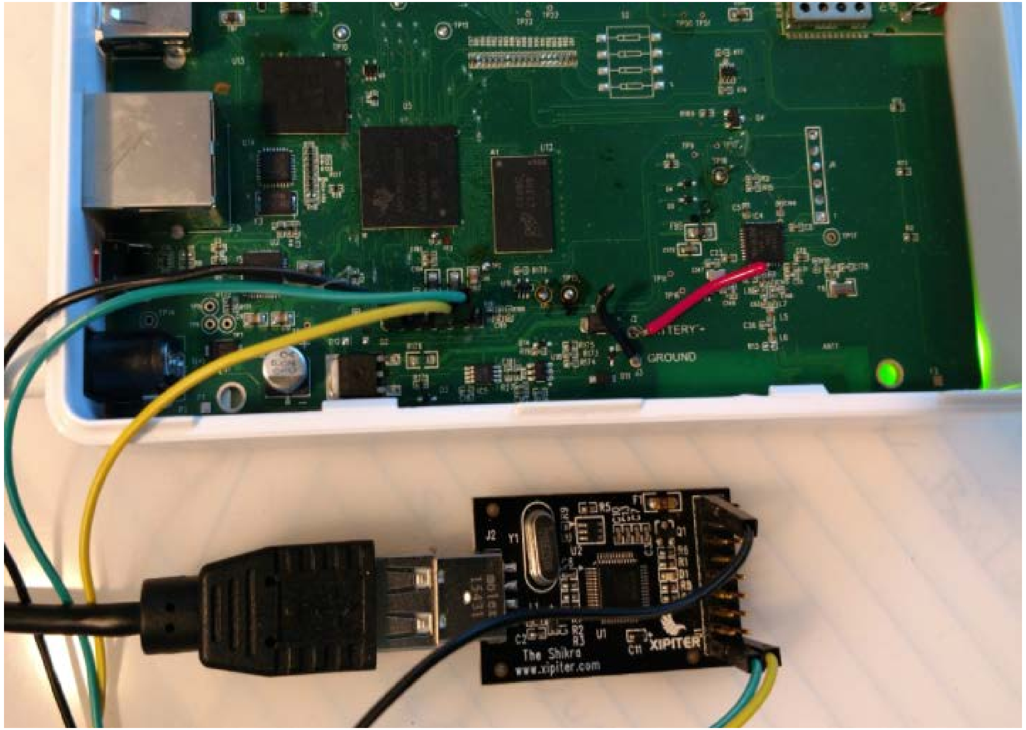






Gaining Root Access Via UART

- Bypass authentication
- U-Boot console
  - Interrupt boot cycle
  - Alter boot arguments
- Live Demo

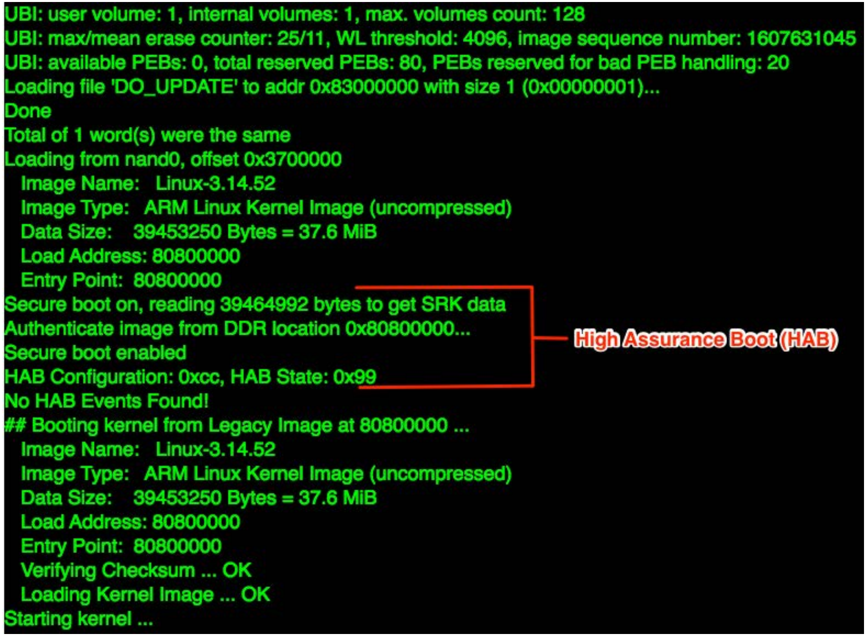


WHAT

Methods available for improving security

What

- Secure boot
  - Authenticated against the hardware
  - Required signing to execute on MCU
  - Prevent tampering

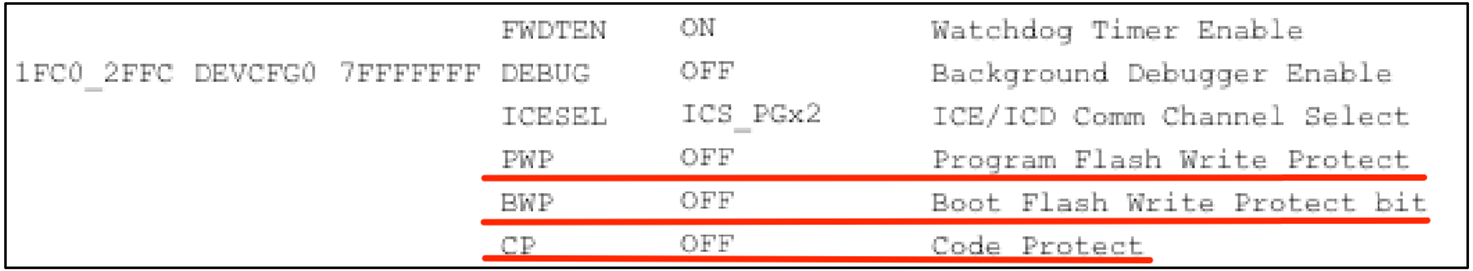


```
UBI: user volume: 1, internal volumes: 1, max. volumes count: 128
UBI: max/mean erase counter: 25/11, WL threshold: 4096, image sequence number: 1607631045
UBI: available PEBs: 0, total reserved PEBs: 80, PEBs reserved for bad PEB handling: 20
Loading file 'DO_UPDATE' to addr 0x83000000 with size 1 (0x00000001)...
Done
Total of 1 word(s) were the same
Loading from nand0, offset 0x3700000
   Image Name:   Linux-3.14.52
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    39453250 Bytes = 37.6 MiB
   Load Address: 80800000
   Entry Point:  80800000
Secure boot on, reading 39464992 bytes to get SRK data
Authenticate image from DDR location 0x80800000...
Secure boot enabled
HAB Configuration: 0xcc, HAB State: 0x99
No HAB Events Found!
## Booting kernel from Legacy Image at 80800000 ...
   Image Name:   Linux-3.14.52
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    39453250 Bytes = 37.6 MiB
   Load Address: 80800000
   Entry Point:  80800000
   Verifying Checksum ... OK
   Loading Kernel Image ... OK
Starting kernel ...
```

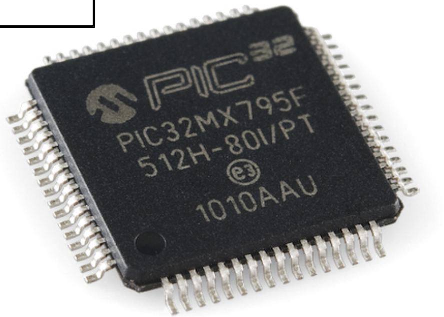
High Assurance Boot (HAB)

What

- Built in processor flash protections

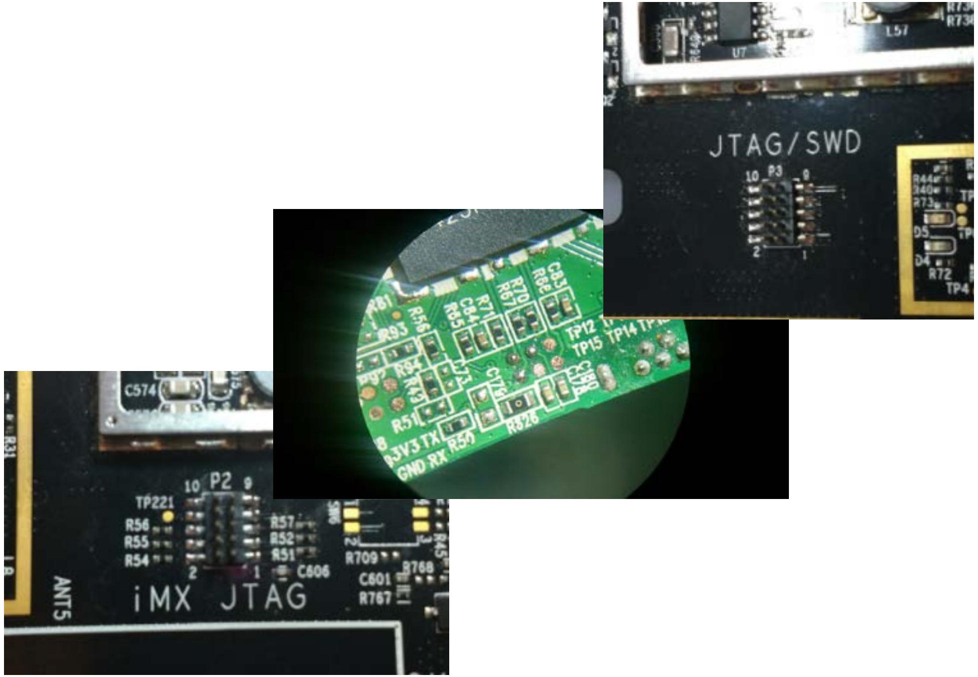


```
                            FWDTEN      ON          Watchdog Timer Enable
1FC0_2FFC DEVCFG0 7FFFFFFF  DEBUG       OFF         Background Debugger Enable
                            ICESEL      ICS_PGx2    ICE/ICD Comm Channel Select
                            PWP         OFF         Program Flash Write Protect
                            BWP         OFF         Boot Flash Write Protect bit
                            CP          OFF         Code Protect
```



What

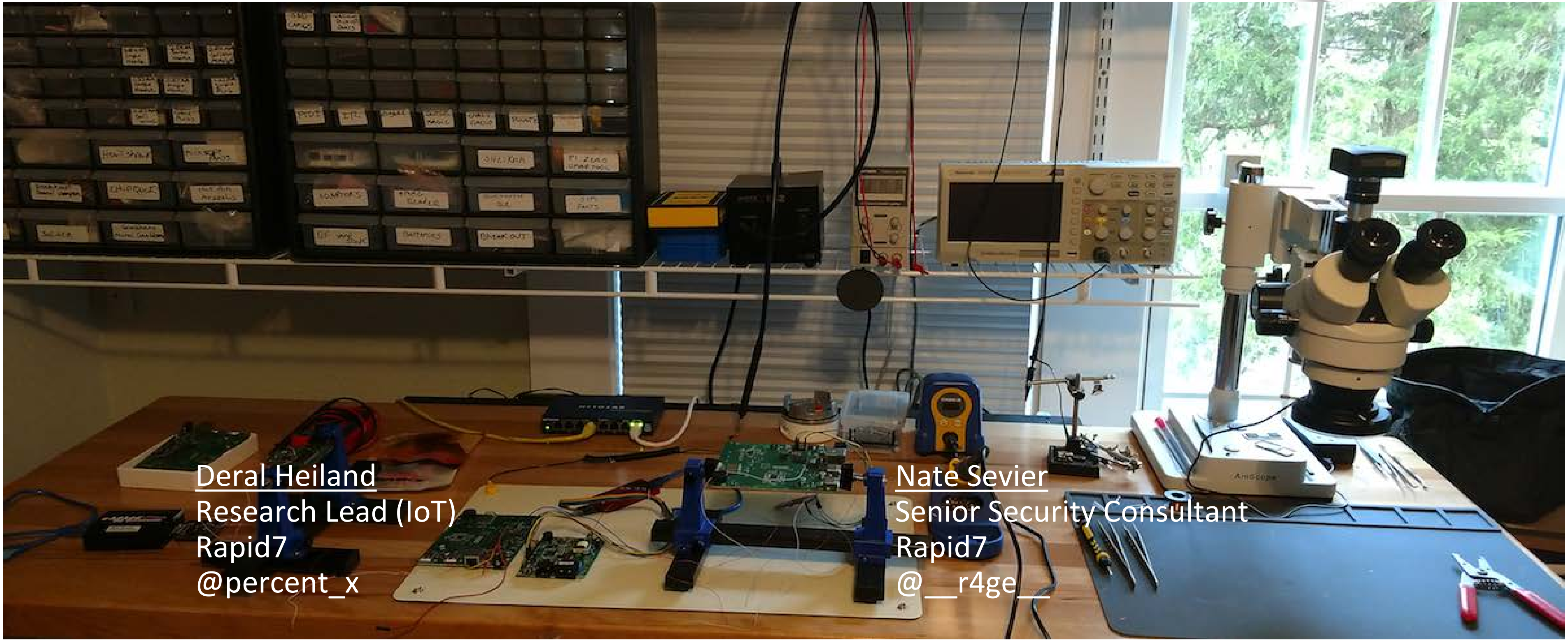
- Disable
  - UART
    - Disabled in production
  - JTAG
    - Disable in Production
      - Electronic fuse
      - Physical fuse



What

- Encryption firmware & data
  - Storage
  - Transmission
  - Trusted Platform Module (TPM)

Questions



Deral Heiland
Research Lead (IoT)
Rapid7
@percent_x

Nate Sevier
Senior Security Consultant
Rapid7
@__r4ge__