Sau **Phần 1 mô tả APPROTECT Bypass** , bài đăng mới này trình bày cách:

- khai thác sản phẩm thật dựa trên nRF52840 để bung Firmware và kích hoạt lại giao diện SWD.
- tái tạo cuộc tấn công vào các SoC nRF52 khác để xác nhận lỗ hổng trong tất cả các phiên bản nRF52.

Khai thác xác thực trên sản phẩm thật

Hãy bắt đầu bằng một tình huống cổ điển, trong đó hacker cần truy cập vào Firmware của sản phẩm. Nếu sản phẩm này dựa trên nRF52, nó có thể được bảo vệ để tránh việc đọc chương trình cơ sở nhằm ngăn chặn kỹ thuật đảo ngược.

Mục tiêu: Logitech G Pro

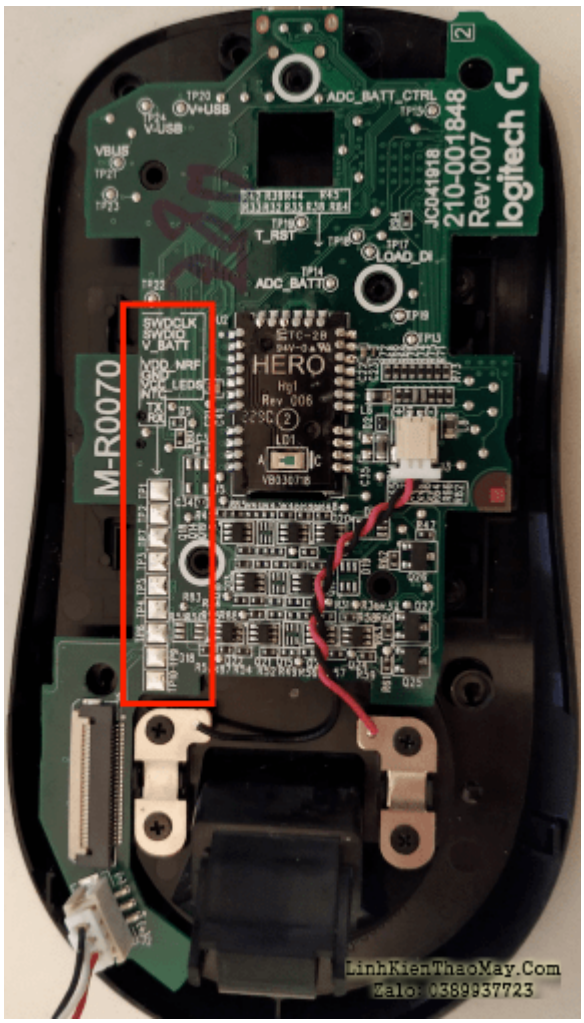
Để xác thực khai thác, mình đã chọn thiết bị đầu tiên mình có trong tay. Đó là **Chuột Logitech G Pro của mình dựa trên nRF52840** .

Lưu ý: Mục đích của mình không phải là tấn công sản phẩm Logitech ở đây .

Nhận quyền truy cập

mình bỏ qua phần giới thiệu nhưng đối với những người quan tâm, **đây là một video hay trên YouTube** .

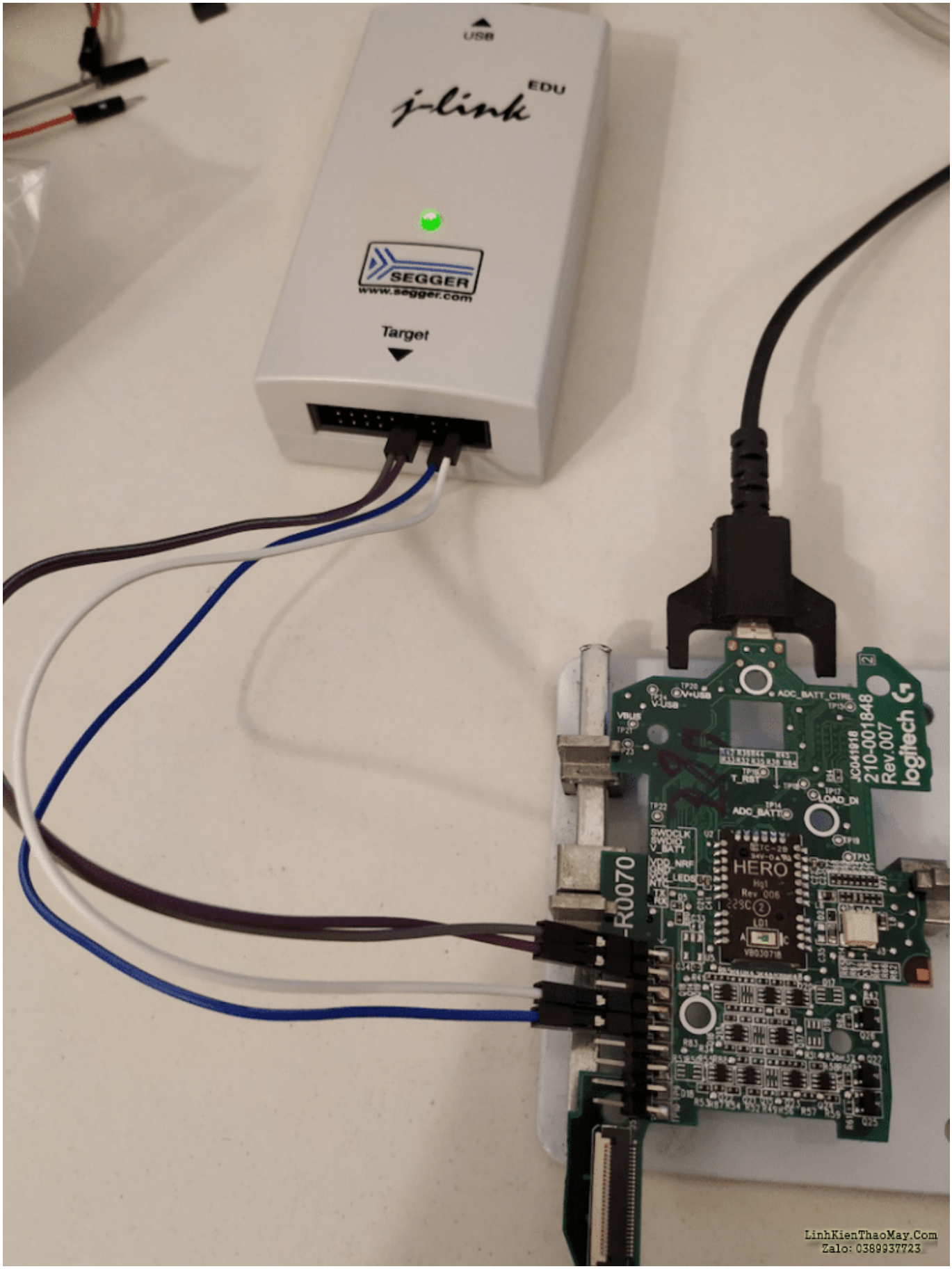
Thiết bị được tháo dỡ để truy cập vào bo mạch chính:



PCB mặt trước của Logitech PRO G. Nhìn cảm biến HERO đẹp quá.

Các chân SWD (SWDCLK, SWDIO) được in lụa nên rất dễ nhận biết (khung màu đỏ).

Sau đó, một số tiêu đề pin được hàn để kết nối mục tiêu với đầu dò Gỡ lỗi Segger J-Link:



Dây nhảy SWDCLK, SWDIO, VDD_NRF và GND giữa mục tiêu và đầu dò JTAG. Cáp USB cũng bị cắm do chưa kết nối pin..

Mọi nỗ lực kết nối qua OpenOcd và GDB đều bị từ chối:

```
$ openocd -f /usr/local/share/openocd/scripts/interface/jlink.cfg -c "transport select swd" -f /usr/local/share/openocd/scripts/target/nrf52.cfg

$ arm-none-eabi-gdb
```

PHÊ DUYỆT được bật. Và kết nối với SWD bị từ chối.

Tất nhiên, tính năng APPROTECT được bật trên thiết bị này.

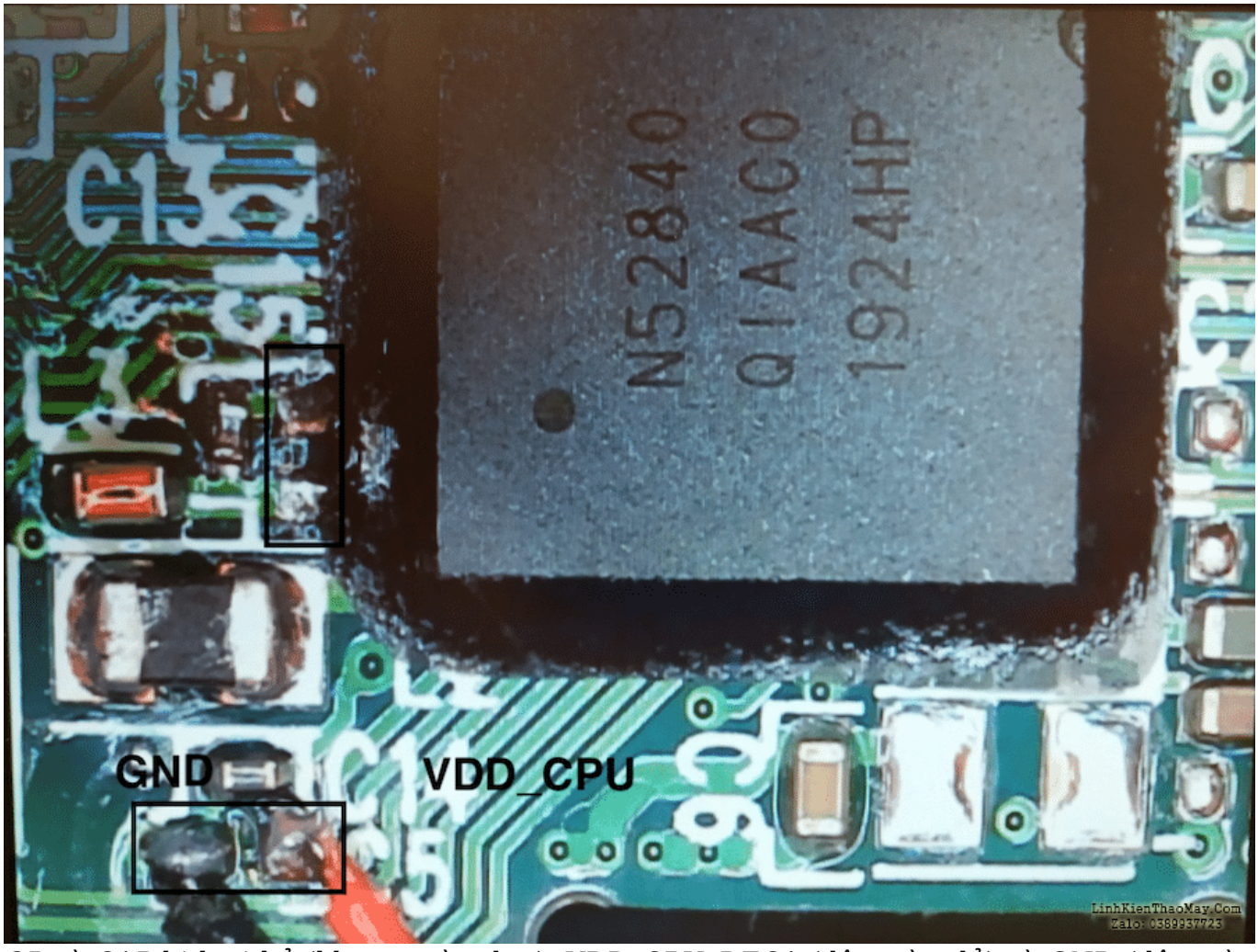
Tái tạo đường vòng APPROTECT

Sự chuẩn bị

NRF52840 nằm ở mặt sau PCB và đóng vai trò là bộ xử lý chính của hệ thống.

Thiết kế PCB hoàn toàn phù hợp với thiết kế tham chiếu nRF52840 (có trong Bảng dữ liệu Bắc Âu). Nó giống như một thiết kế sao chép-dán.

Các tụ tách C5 và C15 được loại bỏ và đầu ra debug được kết nối với VDD_CPU (DEC1):



C5 và C15 bị loại bỏ (khung màu đen). VDD_CPU_DEC1 (dây màu đỏ) và GND (dây màu đen).

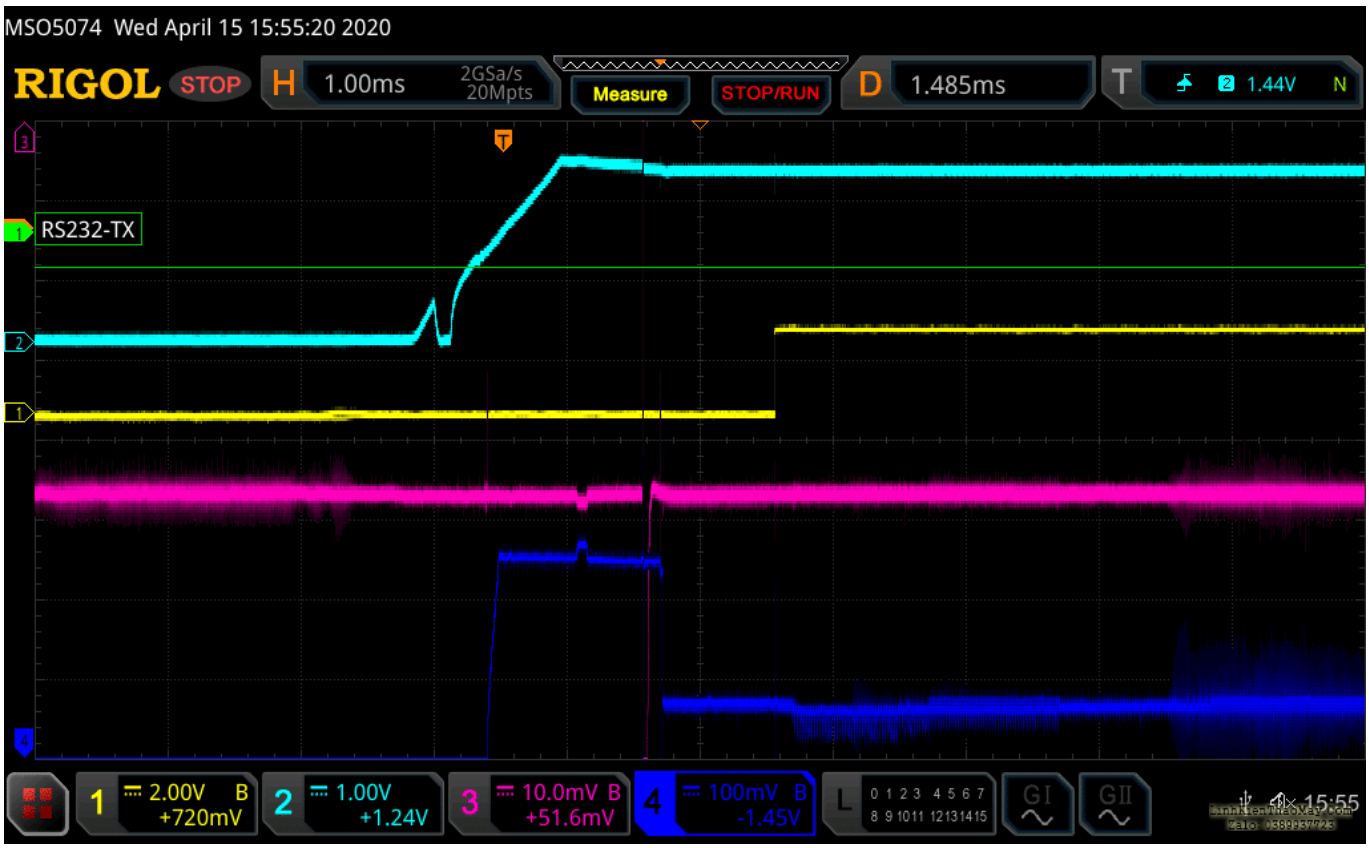
VDD_CPU (DEC1) được kết nối với debug thông qua đầu nối SMA. Dưới đây là hình ảnh của thiết lập tấn công đầy đủ:

Thiết lập nhanh trên Logitech PRO G

Lỗi tấn công Thời gian

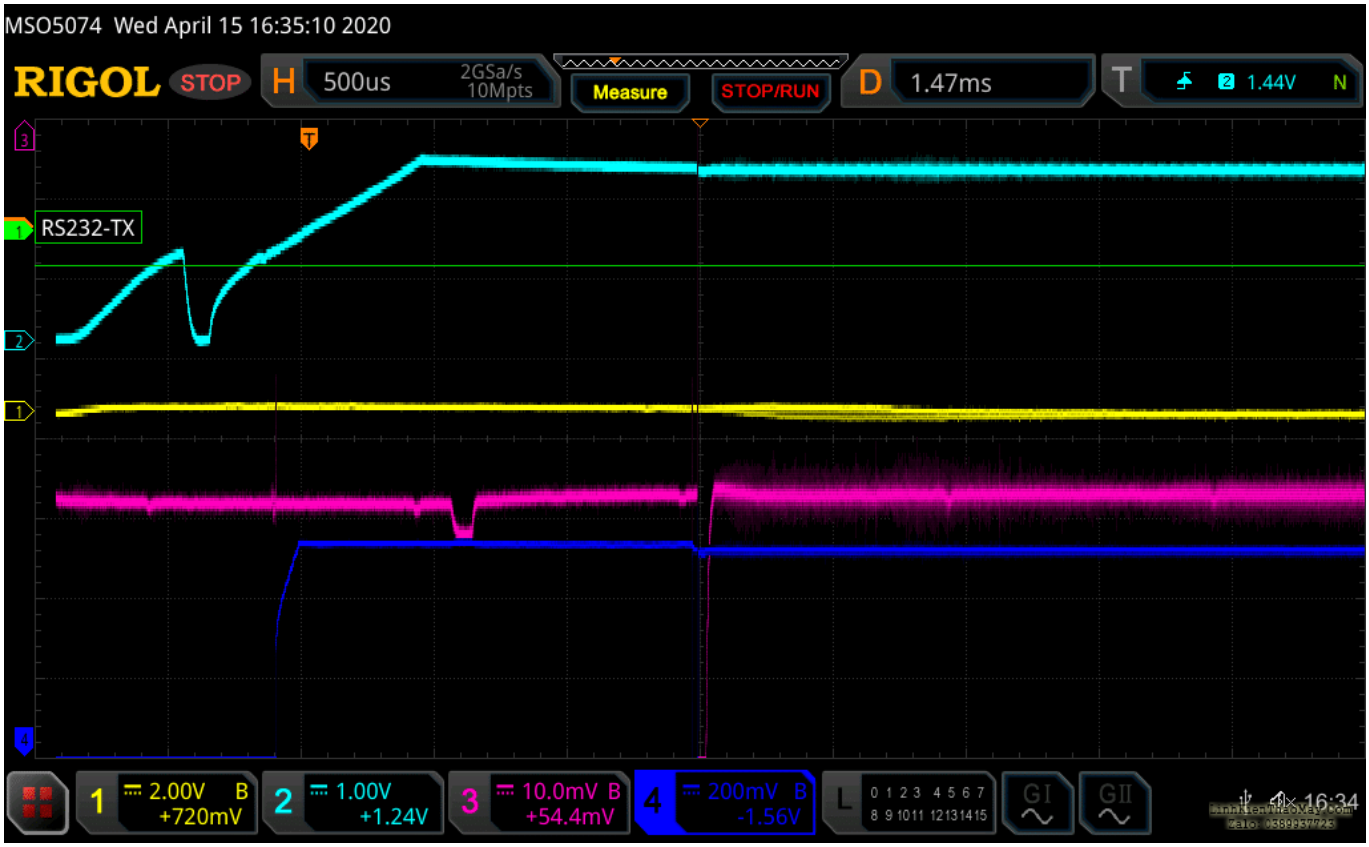
Cuộc tấn công lỗi được thực hiện bằng cách chạy tập lệnh python, tập lệnh này chịu trách nhiệm đồng bộ hóa hệ thống debug, máy hiện sóng và đặt lại thiết bị sau mỗi lần thử lỗi.

Ảnh chụp màn hình này hiển thị quá trình khởi động bình thường (hành vi cổ điển của thiết bị):



Hoạt động bình thường (không có hiệu ứng debug). CH1=UART, CH2= VDD_nRF (Kích hoạt phạm vi), CH3 = mức tiêu thụ dòng điện của CPU, CH4= VDD_CPU.

Sau đó, kết quả bạn muốn thấy sau khi thực hiện lỗi thành công:



Tấn công thành công. CH1=UART, CH2= VDD_nRF (Kích hoạt phạm vi), CH3 = mức tiêu thụ dòng điện của CPU, CH4= VDD_CPU.

Tín hiệu VDD_nRF trên bo mạch được sử dụng làm tham chiếu kích hoạt phạm vi. Sau một khoảng thời gian trễ cụ thể, lỗi được đưa vào sẽ làm gián đoạn quá trình khởi tạo bình thường của nRF52840.

Từ quan điểm của shell, trình gỡ lỗi bên ngoài giờ đây có thể kết nối với chuột:

```
 ----- APPROTECT BYPASS 13 -----
#### OpenOcd test ####
xPack OpenOCD, 64-bit Open On-Chip Debugger 0.10.0+dev (2019-07-17-11:25)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.org/doc/doxygen/bugs.html
swd
Info : J-Link V10 compiled Jan  7 2020 16:51:47
Info : Hardware version: 10.10
Info : VTarget = 2.161 V
Info : clock speed 1000 kHz
Info : SWD DPIDR 0x2ba01477
Info : nrf52.cpu: hardware has 6 breakpoints, 4 watchpoints
Info : nrf52.cpu: external reset detected
Info : Listening on port 3333 for gdb connections
```

Trình gỡ lỗi được kết nối với nRF52840

Trích xuất phần mềm

Sau khi kết nối, bước tiếp theo là kết xuất Firmware và UICR:

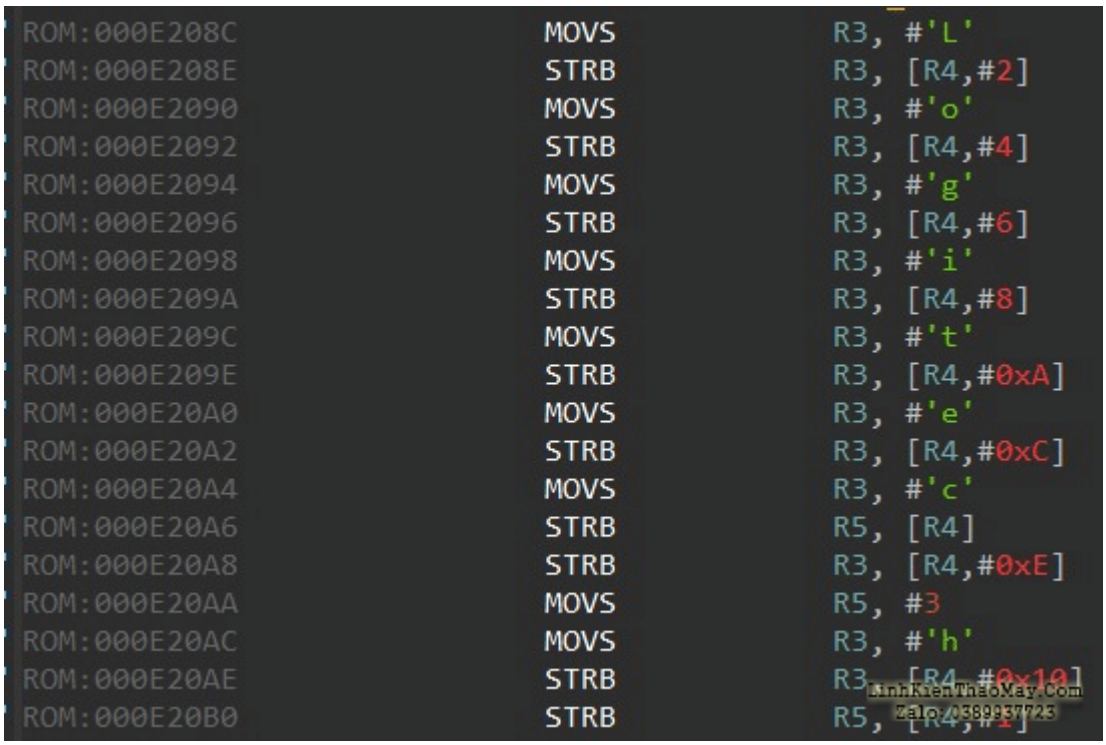
```
#openocd via telnet
dump_image FLASH.bin 0x0 0x100000
dump_image UICR.bin 0x10001000 0x1000
#optional
dump_image FICR.bin 0x10000000 0x1000
```

Dưới đây là phiên bản bộ tải khởi động và Tên thiết bị ở 0xE5CD8 trong bộ nhớ flash:

```
000e5cd0  00 aa df 85 ee 71 4a 00  4d 50 4d 31 35 5f 44 30  |.....qJ.MPM15_D0|
000e5ce0  00 42 4f 54 37 34 2e 30  32 5f 42 30 30 32 36 00  |.BOT74.02_B0026.|
000e5cf0  47 20 50 72 6f 20 57 69  72 65 6c 65 73 73 20 47  |G Pro Wireless G|
000e5d00  61 6d 69 6e 67 20 4d 6f  75 73 65 00 19 22 0e 00  |aming Mouse.."..|
000e5d10  20 34 00 20 44 60 0e 00  01 00 01 03 81 00 00 00  | 4. D`..........|
000e5d20  60 5d 0e 00 19 00 00 00  79 5d 0e 00 36 00 00 00  |`]......y]..6...|
000e5d30  34 34 00 20 44 5d 0e 00  54 39 00 20 45 22 0e 00  |44. D]..T9. E"..|
000e5d40  4c 5d 0e 00 3c 34 00 20  15 00 00 00 64 34 00 20  |L]..<4. ....d4. |
000e5d50  54 34 00 20 01 00 00 00  08 00 00 00 00 00 00 00  |T4. ............|
```

Phiên bản bộ nạp khởi động

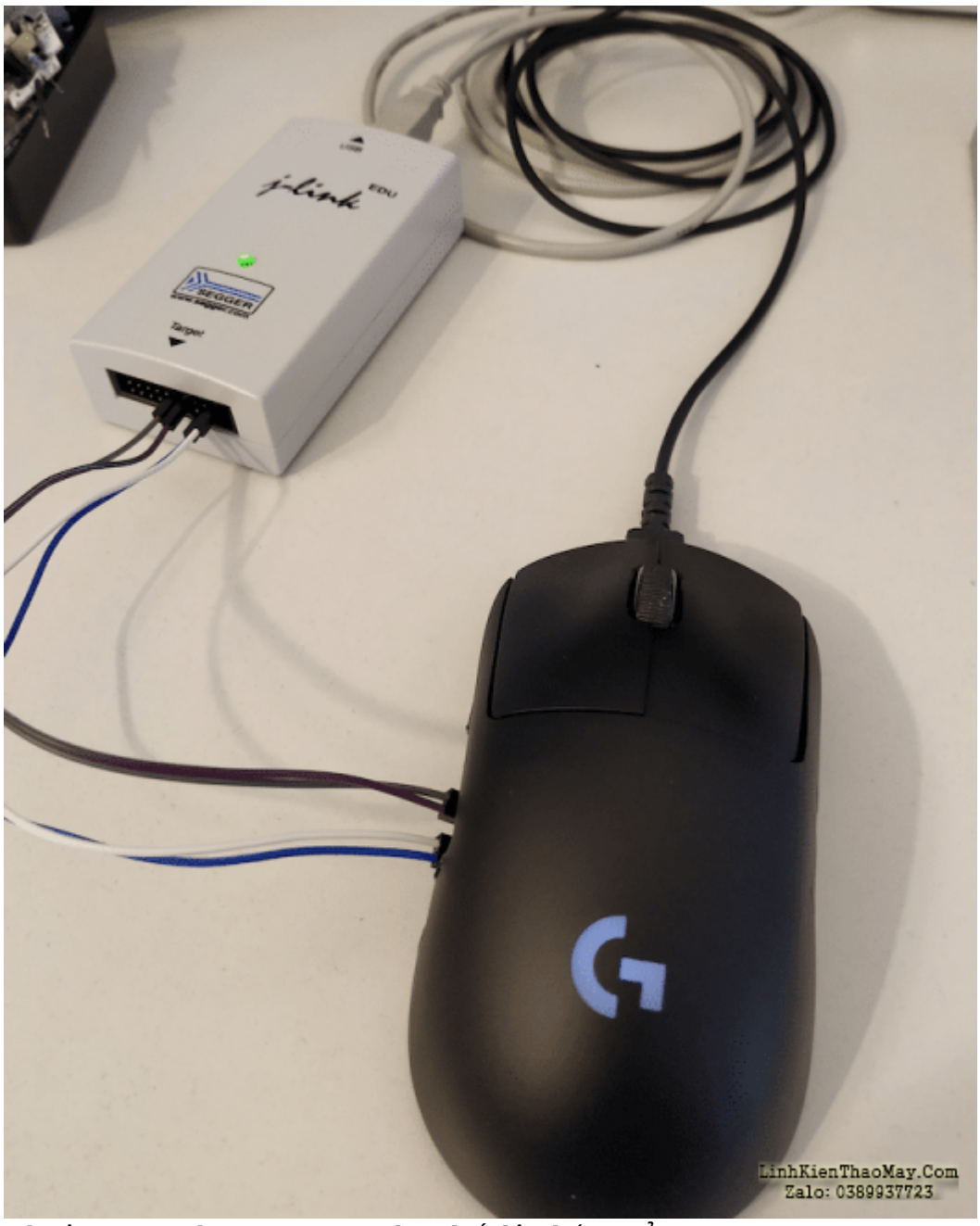
Sau đó, Phân tích mã tĩnh có thể được thực hiện để tìm các lỗ hổng (hoặc chỉ để hiểu cách thức hoạt động của nó).



Kỹ năng Big C

Kích hoạt lại gỡ lỗi vĩnh viễn

Để kích hoạt lại liên tục giao diện gỡ lỗi, APPROTECT bị vô hiệu hóa **(xem Phần 1)** và flash lại với FLASH.bin và UICR.bin đã được trích xuất (tất nhiên là có APPROTECT được vá thành 0xFFFFFFFF):



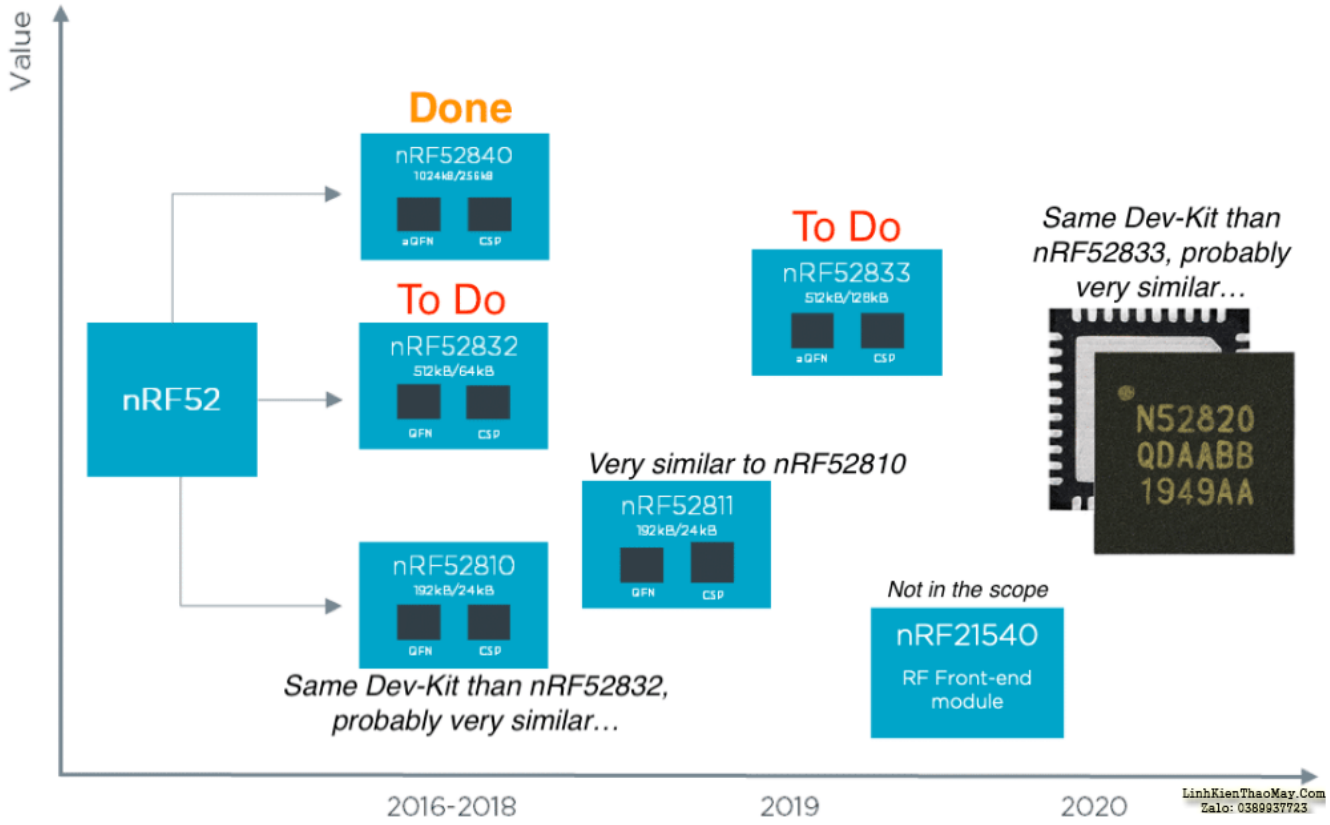
Chuột Logitech PRO-G quay lại chế độ phát triển...

Chuột quay trở lại ***"Chế độ phát triển"*** , trong đó Phân tích mã động là một lợi thế to lớn (đặc biệt là trong quá trình phát triển khai thác).

Gánh nặng gia đình

Cho đến nay, tất cả các kết quả đã thu được trên nRF52840.

Các SoC nRF52 dùng chung CPU Cortex-M4, cùng Cổng gỡ lỗi, cùng Bộ nhớ Flash (ngoại trừ mảng bộ nhớ) và cùng NVMC. Trong bối cảnh này, có khả năng lỗ hổng này phổ biến đối với toàn bộ dòng SoC dòng nRF52. Đây là tầm nhìn của mình về hệ sinh thái nRF52:



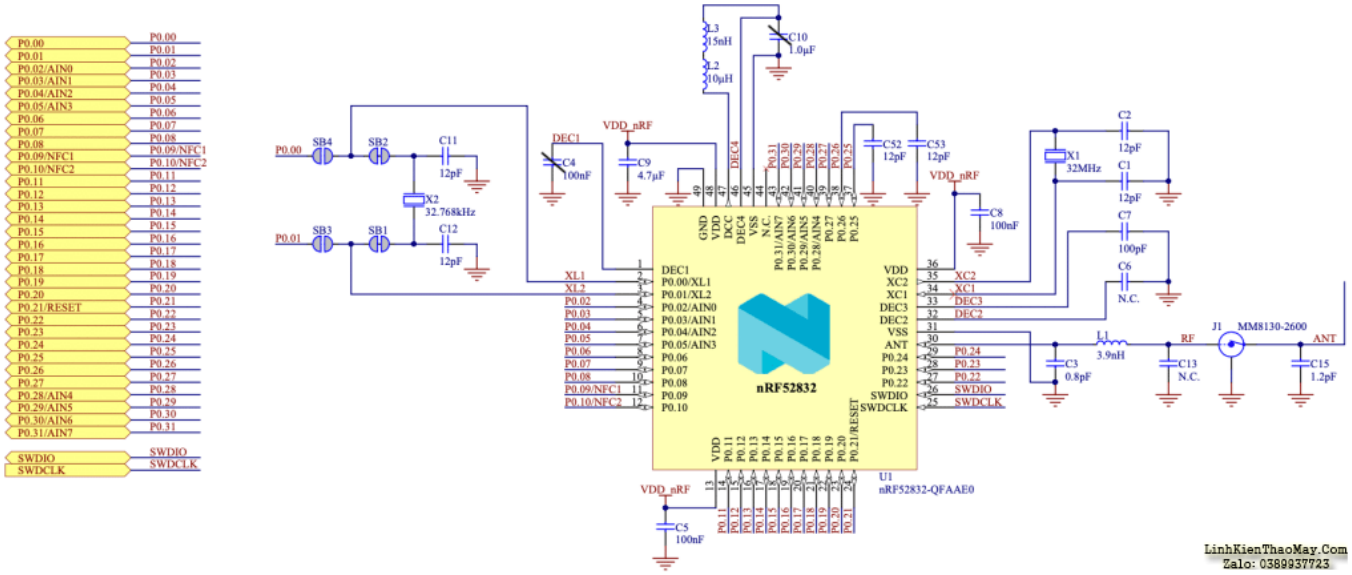
Đánh giá các nền tảng nRF52 hiện có

Sau lần xem xét nhỏ này, mình quyết định tập trung vào nRF52832 và nRF52833. Nordic cung cấp bộ công cụ phát triển cho hai nền tảng này.

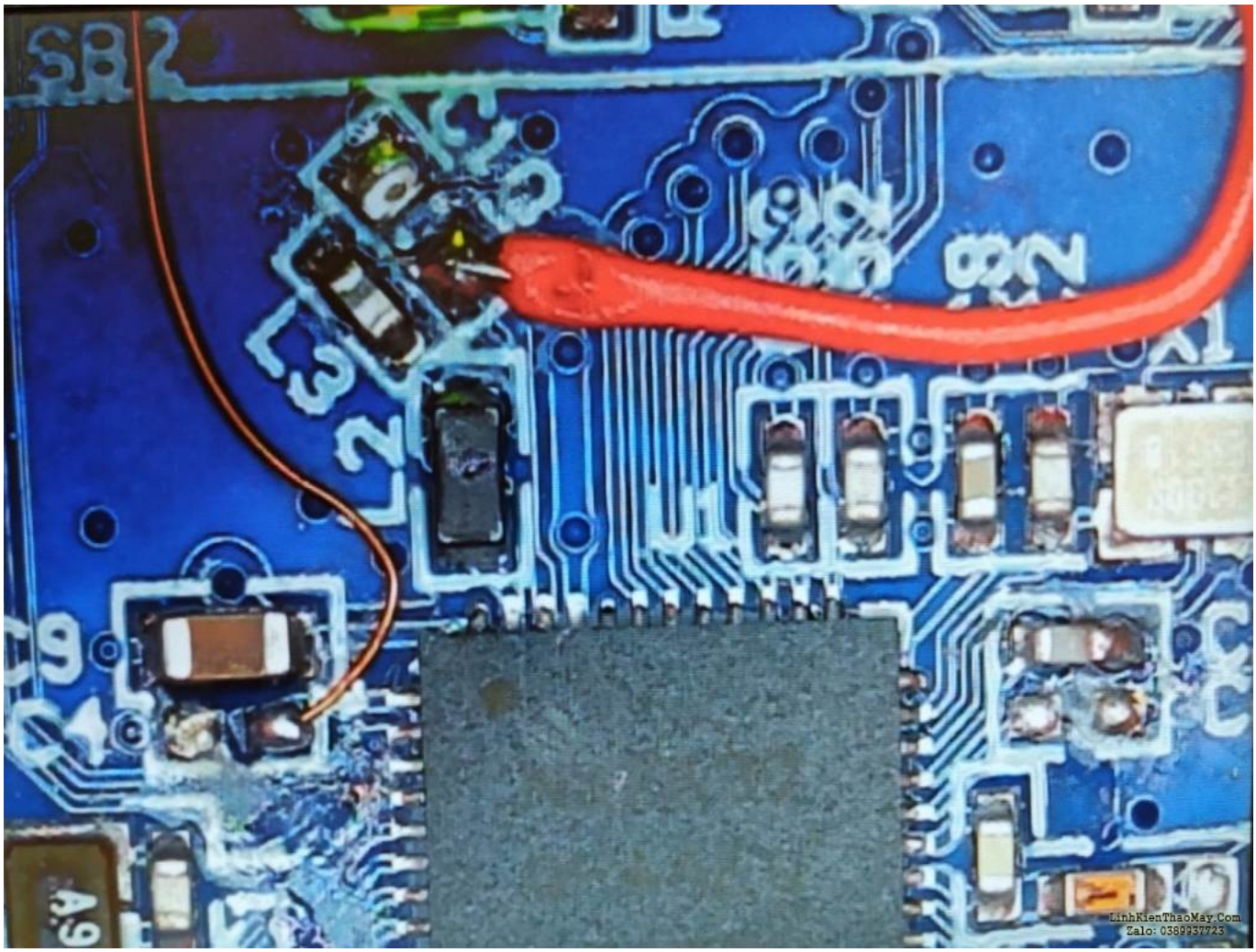
Hai bộ công cụ phát triển đã được đặt hàng. Chi phí = 150$.

Kết quả trên nRF58232

Các thử đã đạt được trên **nRF52-DK** , dựa trên **nRF52832** . Bo mạch phát triển được sửa đổi bằng cách loại bỏ tụ điện và dây hàn:



sơ đồ tham chiếu nRF52832



dây mỏng nRF52832 hàn vào DEC1, dây màu đỏ vào DEC4.

Lưu ý: chỉ có dây mỏng kết nối với DEC1 là đủ để thực hiện cuộc tấn công.

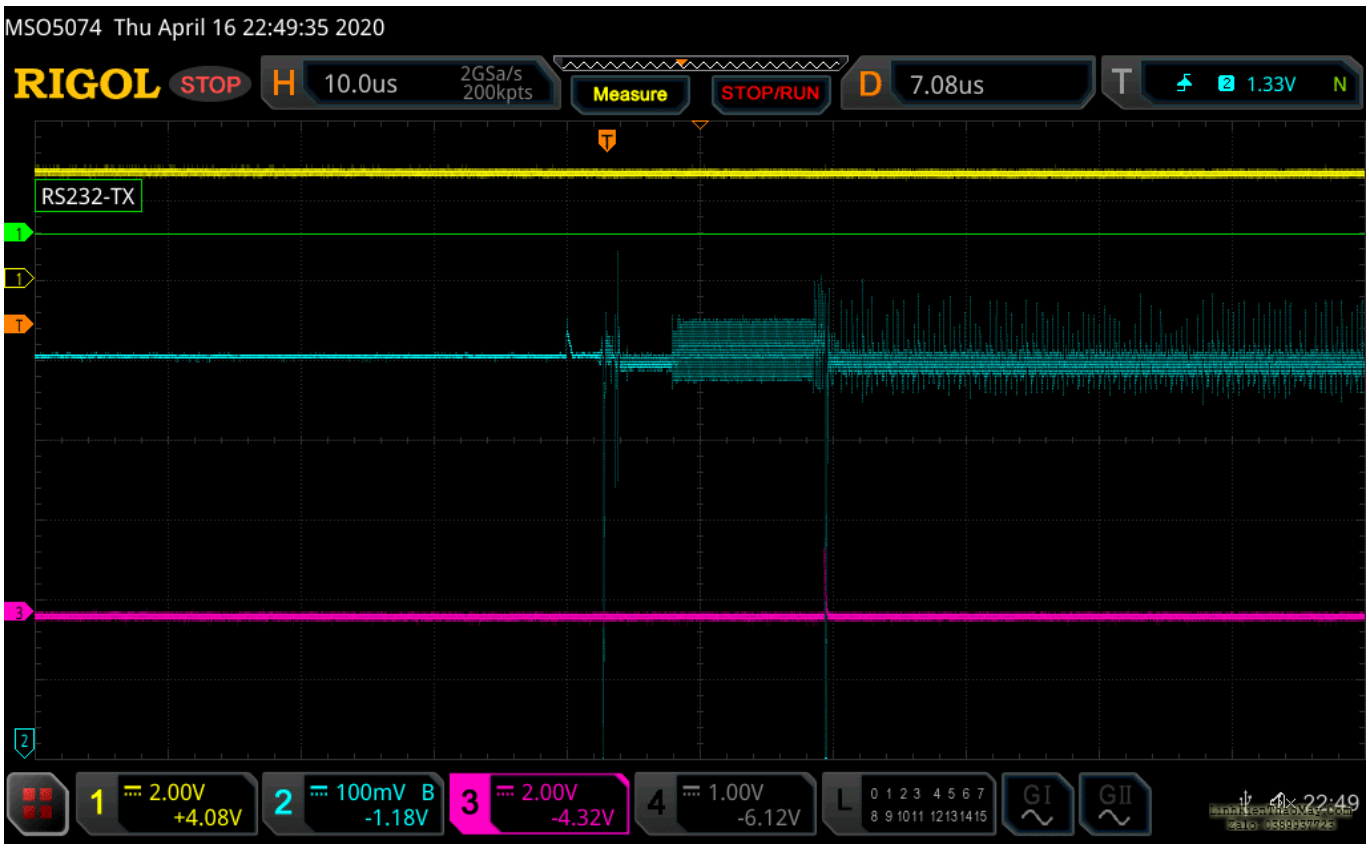
Máy hiện sóng được sử dụng để xác định mô hình thú vị.

mình đã cải thiện một chút cách theo dõi mức tiêu thụ điện năng trên dòng DEC1. Tỷ lệ nhiễu tín hiệu cao hơn.

Theo mức tiêu thụ điện năng được hiển thị bên dưới, hoạt động trong quá trình khởi chạy Bộ điều khiển Flash là như nhau:

Phân tích mức tiêu thụ điện năng của CPU trong quá trình khởi động. CH1= UART TX, CH2 = mức tiêu thụ điện năng DEC1, CH3 = lệnh debug.

Đây là một ví dụ về một debug thành công:



debug thành công. CH1= UART TX, CH2 = mức tiêu thụ điện năng DEC1, CH3 = lệnh debug.

Gỡ lỗi SWD được kích hoạt lại:

```
(gdb) target remote :3333
Remote debugging using :3333
0x000060ac in ?? ()
(gdb) info mem
Using memory regions provided by the target.
Num Enb Low Addr   High Addr  Attrs
0   y   0x00000000 0x00080000 flash blocksize 0x1000 nocache
1   y   0x00080000 0x10001000 rw nocache
2   y   0x10001000 0x10001100 flash blocksize 0x100 nocache
3   y   0x10001100 0x100000000 rw nocache
(gdb) x/1x 10001208
0x989b38:       0x00000000
(gdb) x/1x 0x10001208
0x10001208:     0xffffff00
(gdb) x/10x 0x0
0x0:    0x20010000      0x000002b5      0x000002dd      0x000002df
0x10:   0x000002e1      0x000002e3      0x000002e5      0x00000000
0x20:   0x00000000      0x00000000
```

```
xPack OpenOCD, 64-bit Open On-Chip Debugger 0.10.0+dev (2019-07-17-11:25)
Licensed under GNU GPL v2
For bug reports, read
        http://openocd.org/doc/doxygen/bugs.html
0
Info : J-Link OB-SAM3U128-V2-NordicSemi compiled Jan 21 2020 17:30:48
Info : Hardware version: 1.00
Info : VTarget = 3.300 V
Info : clock speed 1000 kHz
Info : SWD DPIDR 0x2ba01477
Info : nrf52.cpu: hardware has 6 breakpoints, 4 watchpoints
Info : Listening on port 3333 for gdb connections
Info : Listening on port 6666 for tcl connections
Info : Listening on port 4444 for telnet connections
Info : accepting 'gdb' connection on tcp/3333
target halted due to debug-request, current mode: Thread
xPSR: 0x61000000 pc: 0x000060ac msp: 0x2000fff8
Info : nRF52832-QFAA(build code: E0) 512kB Flash
```

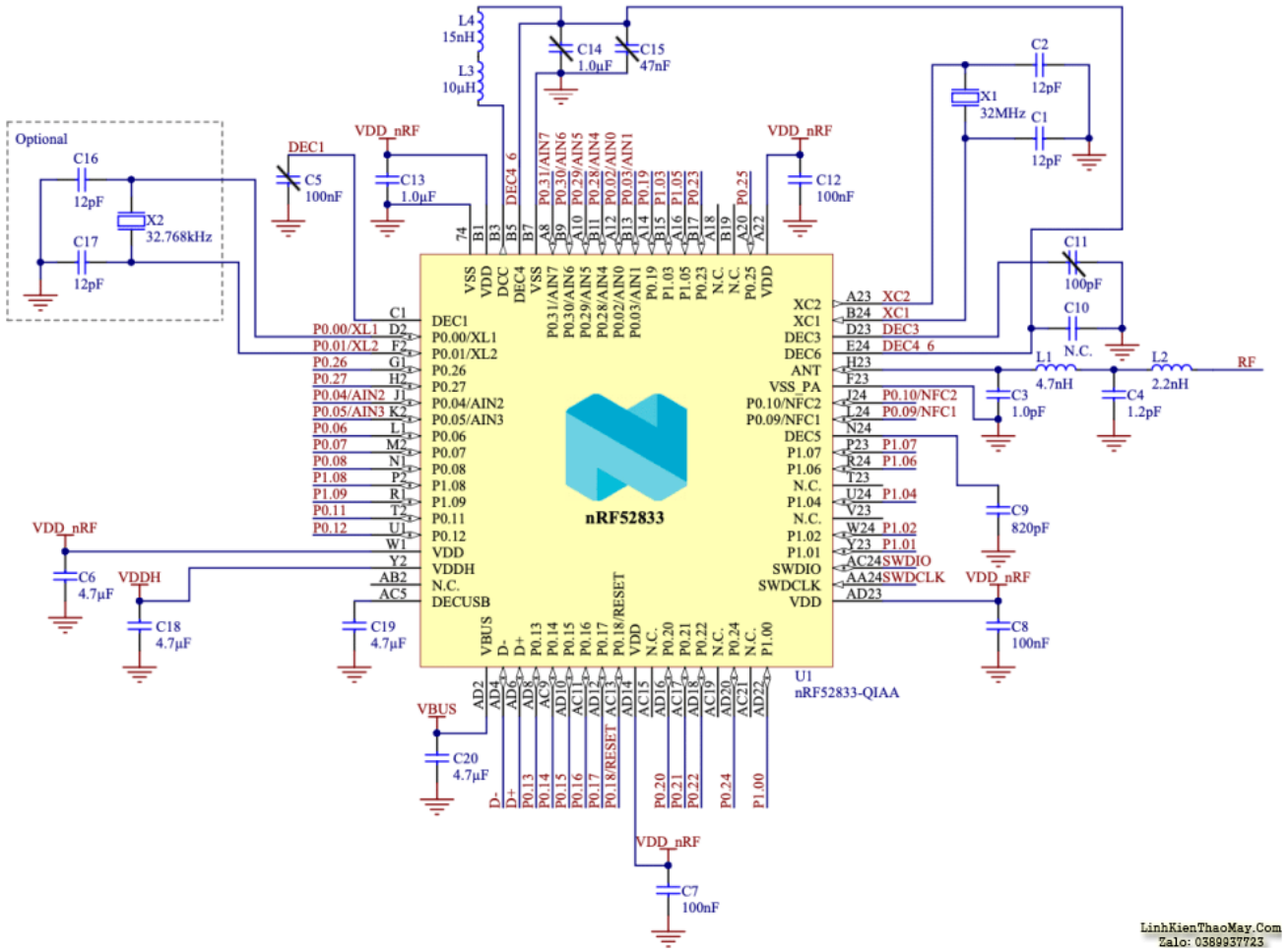
Trình gỡ lỗi được gắn vào mục tiêu nRF52832.

Những kết quả này chứng minh rằng nRF52832 dễ bị khai thác APPROTECT.

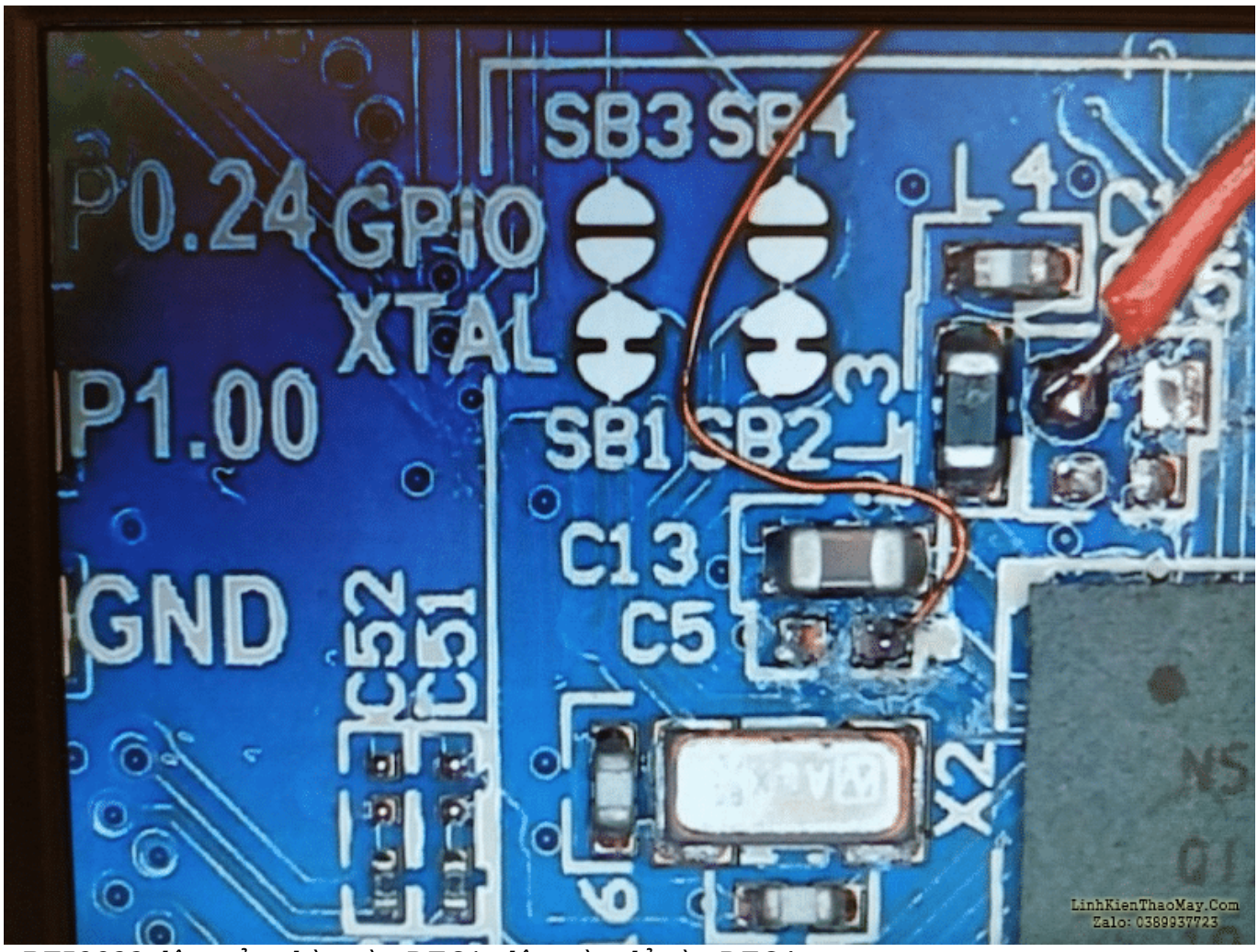
Kết quả trên nRF58233

Một lần nữa, các thử tương tự cũng đạt được trên **nRF52833-DK** , dựa trên **nRF52833** .

Sơ đồ và chế độ xem PCB để tham khảo:

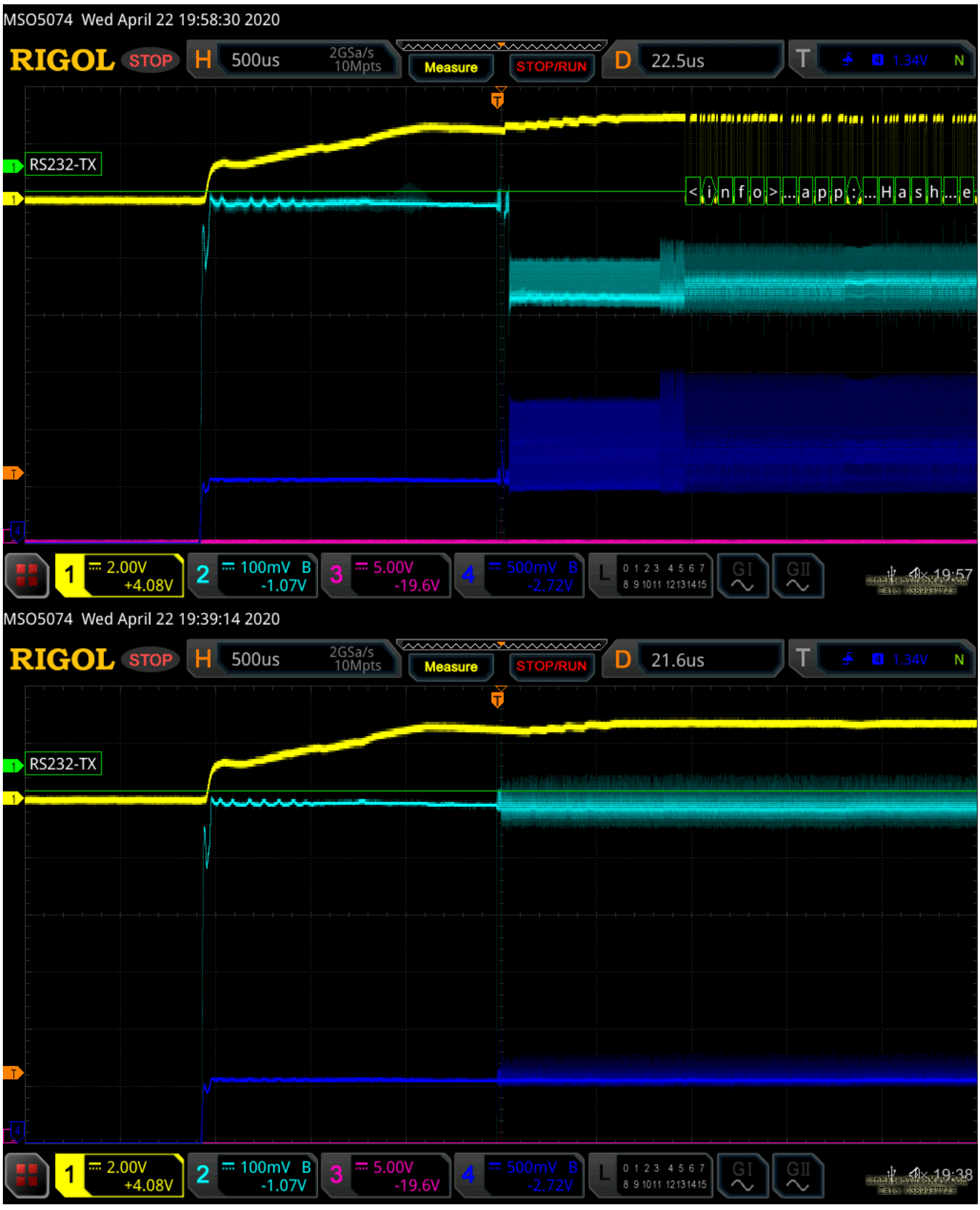


sơ đồ nRF52833

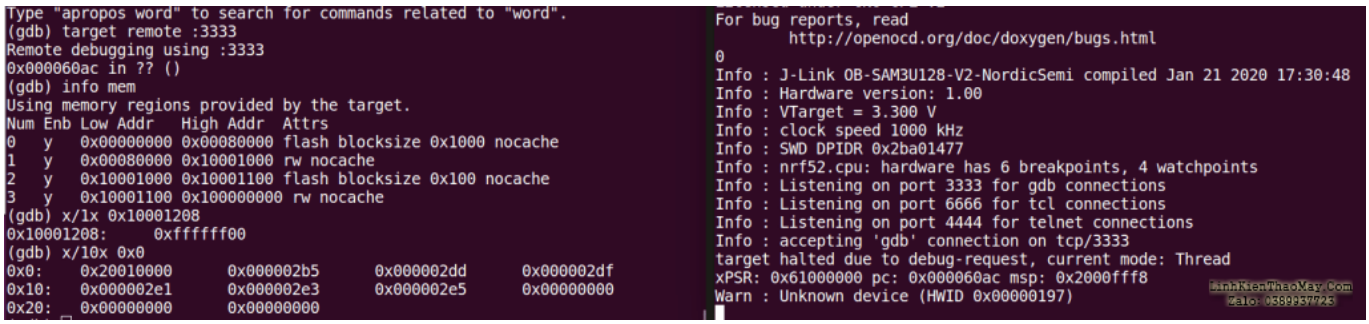


nRF52833 dây mỏng hàn vào DEC1, dây màu đỏ vào DEC4.

Trên nRF52833, việc khởi tạo Bộ điều khiển Flash tương đương với các nRF52 được phân tích trước đó. Việc chèn lỗi được thực hiện trên CPU Power Line DEC1:



Tương tự ở đây, SWD được kích hoạt lại:



Trình gỡ lỗi được gắn vào mục tiêu nRF52833.

NRF52833 dễ bị khai thác APPROTECT.

Sau những thử này, chắc chắn tất cả các phiên bản nRF52 đều dễ bị tấn công.

Sự va chạm

Nordic đã xác nhận các vấn đề bảo mật trong **thông báo** gửi cho tất cả khách của họ vào ngày 12 tháng 6 năm 2020.

Theo mình, tính năng APPROTECT của nRF52 có thể bị đánh bại trong một khoảng thời gian ngắn và với ngân sách rất hạn chế.

Điểm CVSS là 7,6 (Mức độ nghiêm trọng = Cao) CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H .

Các phiên bản nRF52 Bắc Âu sau đây dễ bị tấn công :

- nRF52810
- nRF52811
- nRF52820
- nRF52832
- nRF52833
- nRF52840

và do đó, **các Mô-đun dựa trên nRF52 cũng dễ bị tấn công.**

Các mô-đun này có thể tận dụng tất cả các tính năng của kiến trúc Phần cứng và Phần mềm SoC của Nordic để tạo ra một 'sản phẩm mô-đun duy nhất' mà không cần thêm bộ vi điều khiển để chạy ứng dụng của bạn.

Nordic cung cấp tài liệu tham khảo về các mô-đun của bên thứ ba **tại đây** , chẳng hạn như:

- Tập đoàn Fantel
- lãnh chúa
- của mình
- Raytac
- Taio Yuden
- U-blox

- Điện tử Wurth
- Murata
- Dòng chảy
- Fujitsu
- .... và hơn thế nữa

Phần kết luận

APPROTECT **Bypass** đã được chứng minh trên một thiết bị thương mại, Chuột Logitech Pro G.

Các thử bổ sung đã đạt được trên nRF52832 và nRF52833. Kết quả cho thấy các nền tảng này cũng dễ bị tấn công. NordicSemiconductor xác nhận tất cả các phiên bản nRF52 của họ đều dễ bị tấn công.

Điều này hiện đang tác động đến một số lượng lớn thiết bị trên hiện trường, từ các sản phẩm dựa trên nRF52 đến Mô-đun của bên thứ ba (sử dụng nền tảng nRF52).

Lỗ hổng nằm ở Silicon. Không có cách nào để vá mà không sửa đổi CTNH.

Các bài viết tương tự:

1. 16994. Tivi LCD – TOSHIBA 47L5450
2. canon 2900 – hư ecu đèn nguồn nhấp nháy càn thay thế linh kiện ji nhỉ mấy anh
3. canon lbp 810 – nhấn núc in test tren may thi may chay hoài tói lúc gat reley nguon thi dung lai chu khong in
4. chào các thành viên mình mới làm thêm máy giặt tủ lạnh – mới nhận con máy giặt AW-E920Lv cọn chế độ giặt và cấp nước(ko vặt và xả)thì máy giặt xong tự tăt máy được,,còn nếu chọn giặt có văt có xả máy giặt xong các quá trình thì ko tự tăt được chỉ hiện về 0 phút nhưng ko tăt(tăt là tăt nguồn)
5. dell – thao den nguon ra kiem tra thick co tu kick 12v,khi gan den vao thi co tieng keu rit rit,nhung den ko len
6. Project trò chơi điện tử trên ESP32 xuất lên màn hình CRT
7. Giải nén file dune_service_XXXX.dsf của Dune
8. máy hàn que diện tử 2 pha – do khách cắm điện 1 pha nên em nó bốc khói
9. Nguyên lý làm việc của tụ điện
10. tcl ic tong av303 – co duong nam ngang khoảng 1 cm va nhao nháy phia tren man hinh
11. tim mua ic STU407D – Hoặc APM4052D hoặc APM4048D
12. Vượt APPROTECT trên nRF52 (Phần 1)