

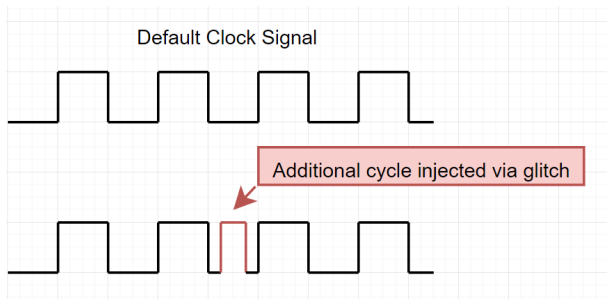
Voltage fault injection

23.3.2026.

Fault injection

External stimulus that causes undefined behaviour

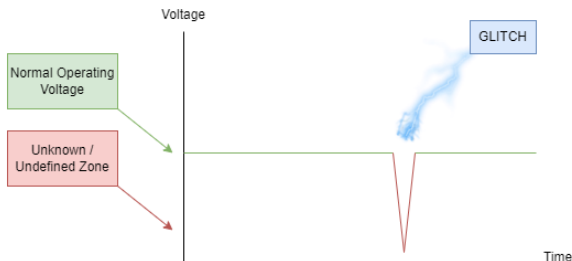
1. Clock glitching



Fault injection

External stimulus that causes undefined behaviour

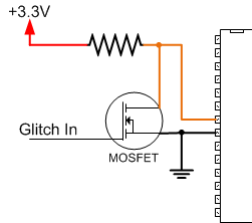
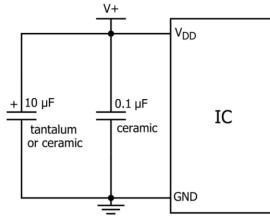
1. Clock glitching
2. Voltage glitching



Fault injection

External stimulus that causes undefined behaviour

1. Clock glitching
2. Voltage glitching



Fault injection

External stimulus that causes undefined behaviour

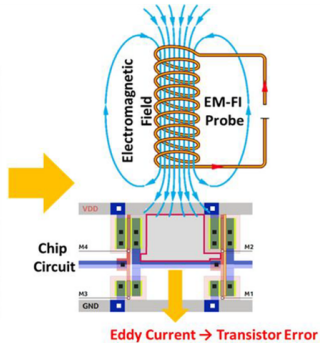
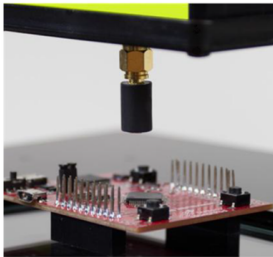
1. Clock glitching
2. Voltage glitching



Fault injection

External stimulus that causes undefined behaviour

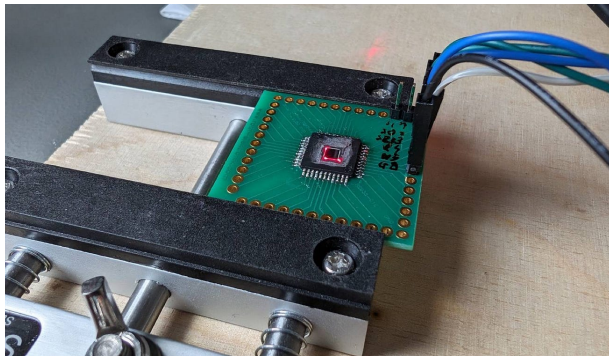
1. Clock glitching
2. Voltage glitching
3. EMI/RF glitching



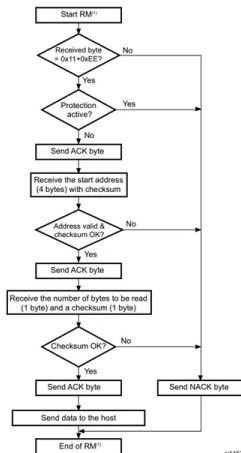
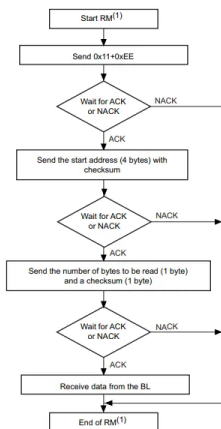
Fault injection

External stimulus that causes undefined behaviour

1. Clock glitching
2. Voltage glitching
3. EMI/RF glitching
4. Laser glitching



Stm32 UART bootloader



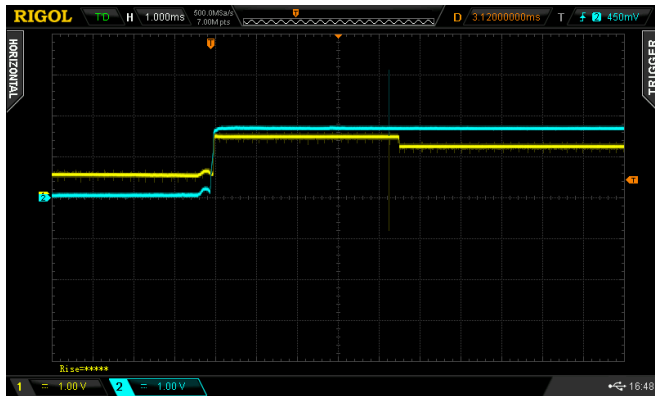
ai14638c

Stm32 UART bootloader

```
4 uint32_t check_RDP_and_get_addr(void)
5
6 {
7     byte bVar1;
8     byte bVar2;
9     byte bVar3;
10    byte bVar4;
11    byte bVar5;
12    int is_rdp_enabled;
13
14    is_rdp_enabled = is_RDP_enabled();
15    if (is_rdp_enabled == 0) {
16        usart_write_byte(0x79);
17        bVar1 = uart_get_char();
18        bVar2 = uart_get_char();
19        bVar3 = uart_get_char();
20        bVar4 = uart_get_char();
21        bVar5 = uart_get_char();
22        if (bVar5 == (byte)(bVar3 ^ bVar1 ^ bVar2 ^ bVar4)) {
23            usart_write_byte(0x79);
24            return (uint)bVar2 << 0x10 | (uint)bVar1 << 0x18 | (uint)CONCAT11(bVar3,bVar4);
25        }
26    }
27    return 0x55555555;
28 }
```

NRF52 APPROTECT bypass

Internal 1.1V voltage regulator

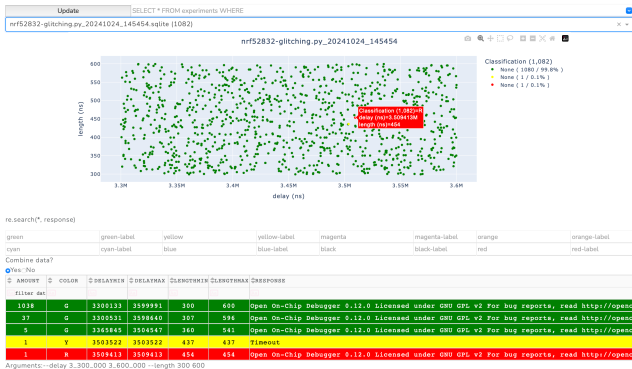


NRF52 APPROTECT bypass



NRF52 APPROTECT bypass

FAULT INJECTION ANALYSIS



Target

NRF52840 SuperMini dev board

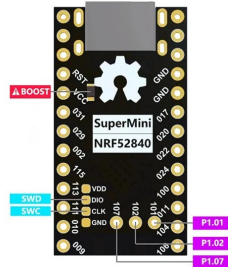
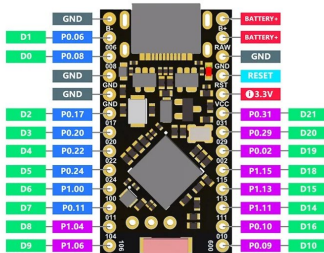
- High Frequency
- Low Frequency
- Power Pins
- Arduino Labels
- MCU Control

Charge current selection jumper:

Connect this jumper "BOOST", the charging current increases from 100ma to 300ma. Only do this if your battery is larger than 500mAh to avoid explosion.

External VCC cutoff control:

When P0.13 is set low, the power supply to the 3.3V ~VCC pin will be turned off. This is useful for components that use less power when idle, such as RGB LEDs.

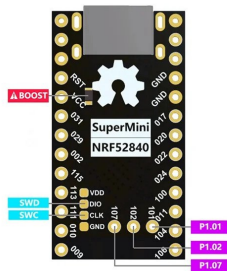
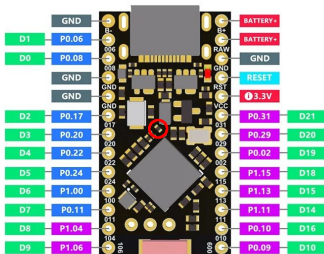


Target

NRF52840 SuperMini dev board

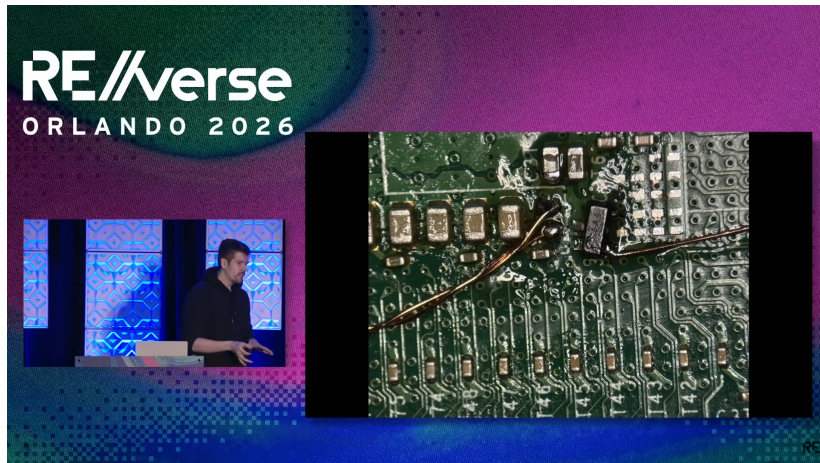


External VCC cutoff control:



Hardware

Direct MOSFET connection



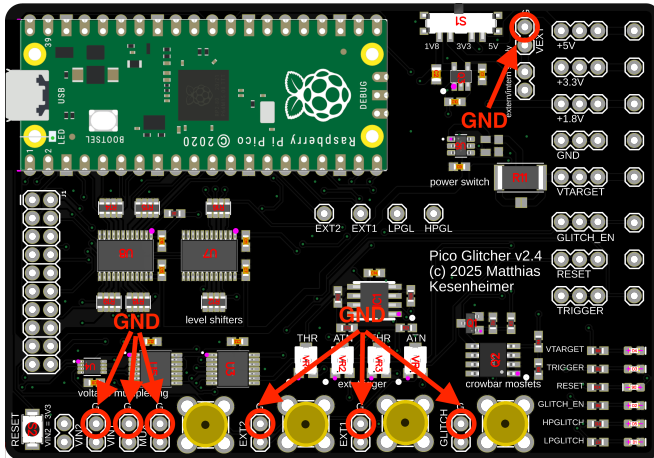
Hardware

ChipWhisperer

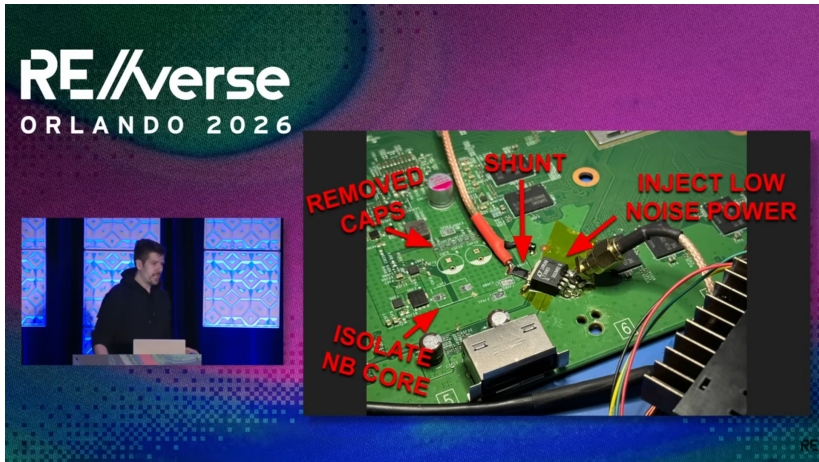


Hardware

Picoglitcher



Xbox One north bridge glitch



References

1. <https://voidstarsec.com/blog/replicant-part-1>
2. Microcontroller Exploits by Travis Goodspeed
3. The Hardware Hacking Handbook by Jasper van Woudenberg and Colin O'Flynn
4. <https://sec-consult.com/blog/detail/secglitcher-part-1-reproducible-voltage-glitching-on-s>

Q&A

Thank you for your attention.
Let's get glitching!