Free EMFA for all!

Alberto Battistello

Outline

- *Why, What, Where and How* Fault Attacks
- *Recent Low cost* attacks and tools
- A *0$* EMFA tool

Why, What, Where and How
Fault Attacks

SEC
PAT

About Me

- Battistello Alberto
- Ph.D @ UVSQ
- 10+ years experience in smartcard red team @IDEMIA
- Joined Security Pattern in 2020
- Provided Side channel and Fault attack courses at University of Bordeaux and Milan.
- Several publications and patents.
- @linkedin albertobattistello

Where Fault Attacks

- PIN Verification

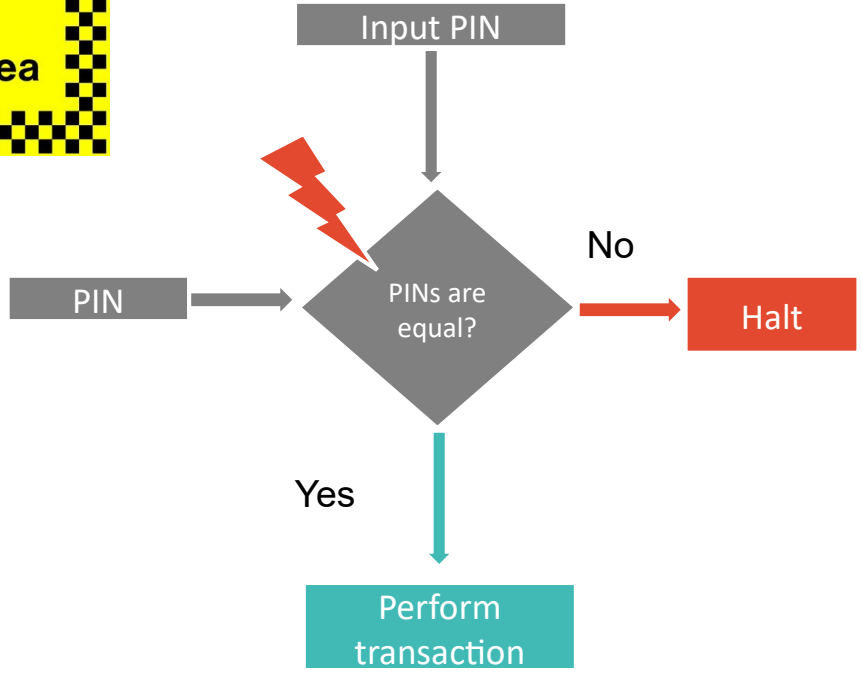
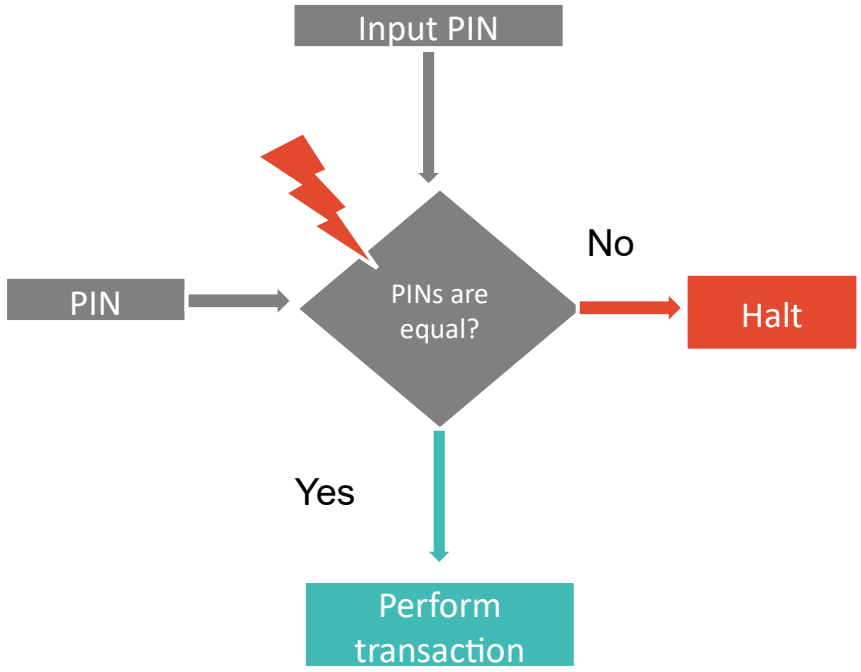


Image by www.zettle.com and https://www.archersafetysigns.co.uk/

How do Fault Attacks work

```
1. procedure VERIFY PIN(candidate PIN V )
2. status = COMPARISON(U,V)
3. if status = TRUE then
4.     Perform transaction
5. else
6.     Halt
7. end if
8. return
```



Le Bouder, Hélène, et al. "A template attack against VERIFY PIN algorithms." *SECRYPT 2016*.

How do Fault Attacks work

Fault attacks models:

- Corrupt instruction
- Corrupt value
- Skip instruction

```
1. procedure VERIFY PIN(candidate PIN V )
2. status = COMPARISON(U,V)
3. if status = TRUE then
4.     Perform transaction
5. else
6.     Halt
7. end if
8. return
```

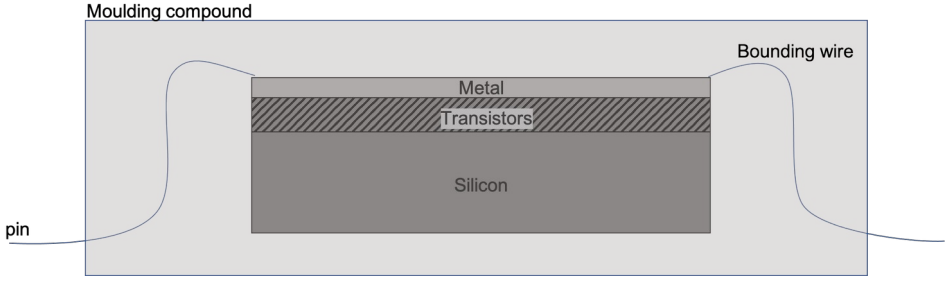
What to Fault

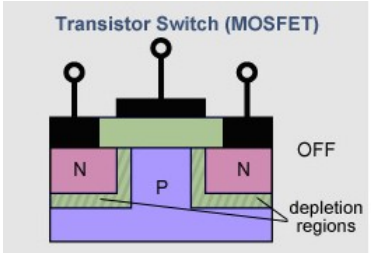
- Security Mechanisms
  - Access protected features/ Bypass limitations
    - Smartcard, automotive, IoT
    - activation codes, secure boot, sandboxes, privilege escalation
  - Disable protections/restrictions
    - Vendor’s limitations (eg. Drones No flight zones)
    - Bypass PayTV restrictions
  - Avoid security measures
    - Smartcard PIN counter decrement
- Crypto
  - Retrieve secret keys
    - DES, AES, RSA, ECC, Lightweight, Post-quantum, etc…

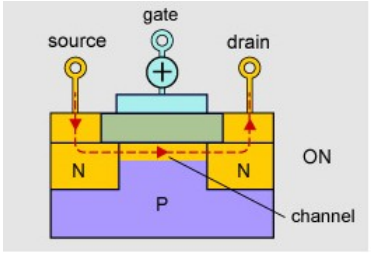
Timmers, Niek, and Cristofaro Mune. "Escalating privileges in linux using voltage fault injection." *FDTC* 2017.
Vasselle, Aurélien, et al. "Laser-induced fault injection on smartphone bypassing the secure boot." *FDTC* 2017.
O'Flynn, Colin. "BAM BAM!! On Reliability of EMFI for in-situ Automotive ECU Attacks.” *ePrint* 2020.

Why Fault attacks

- Electronic devices are made up of transistors (maaany).
  - Transistors acts like switches
  - They are activated by current/voltage







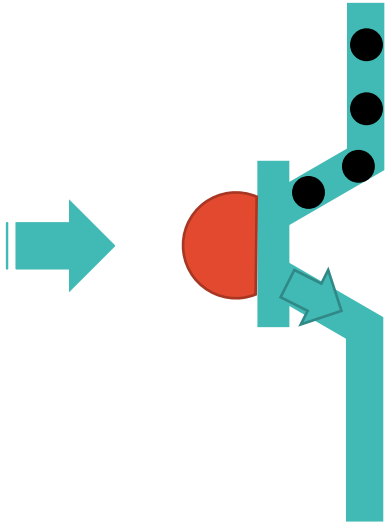


Image credit to www.abc.net.au/

Why Fault attacks

- Electronic devices are made up of transistors (maaany).
  - Transistors acts like switches
  - They are activated by current/voltage

Fault attack vectors

- Temperature
  - Apple Coldgate!
  - Preparation:
    - Nothing – to decapsulation
  - Countermeasures: Temp. sensor

- Clock glitches
  - Preparation:
    - Nothing
  - Countermeasures: Use internal clock

- Voltage glitches
  - Preparation:
    - Nothing -- to decupling capacitor removal
  - Countermeasures: Regulators are there for something!

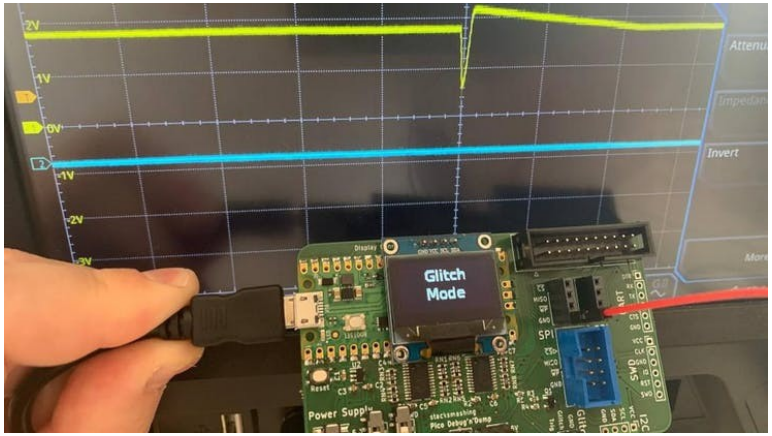
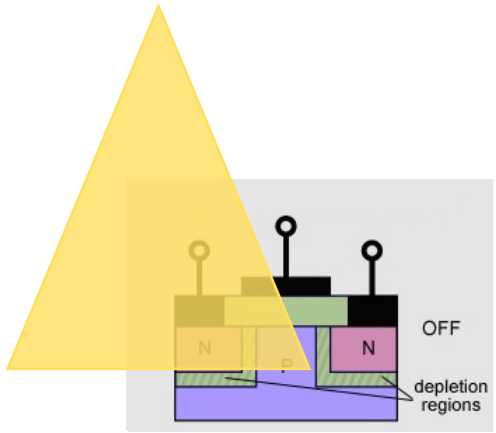


Image credit to laptoprepair101.com and Thomas Roth

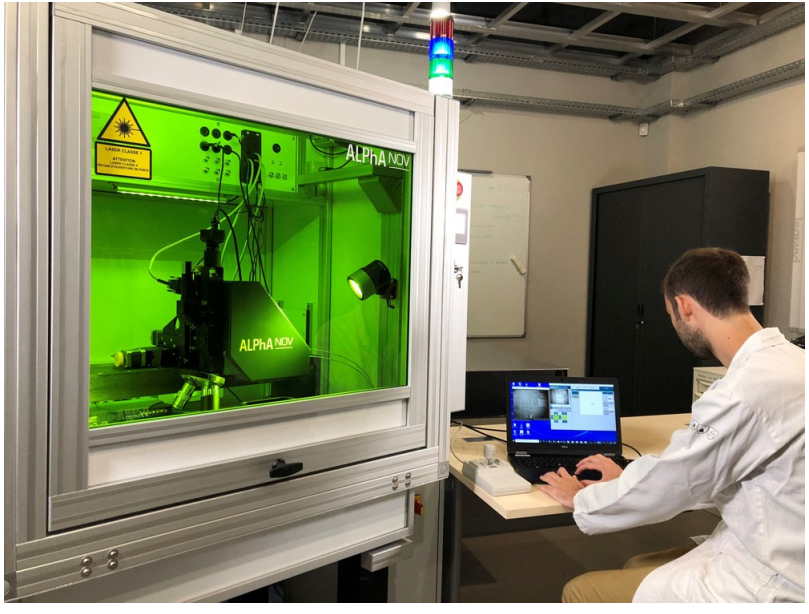
Fault attack vectors -- light

- Lasers/Light

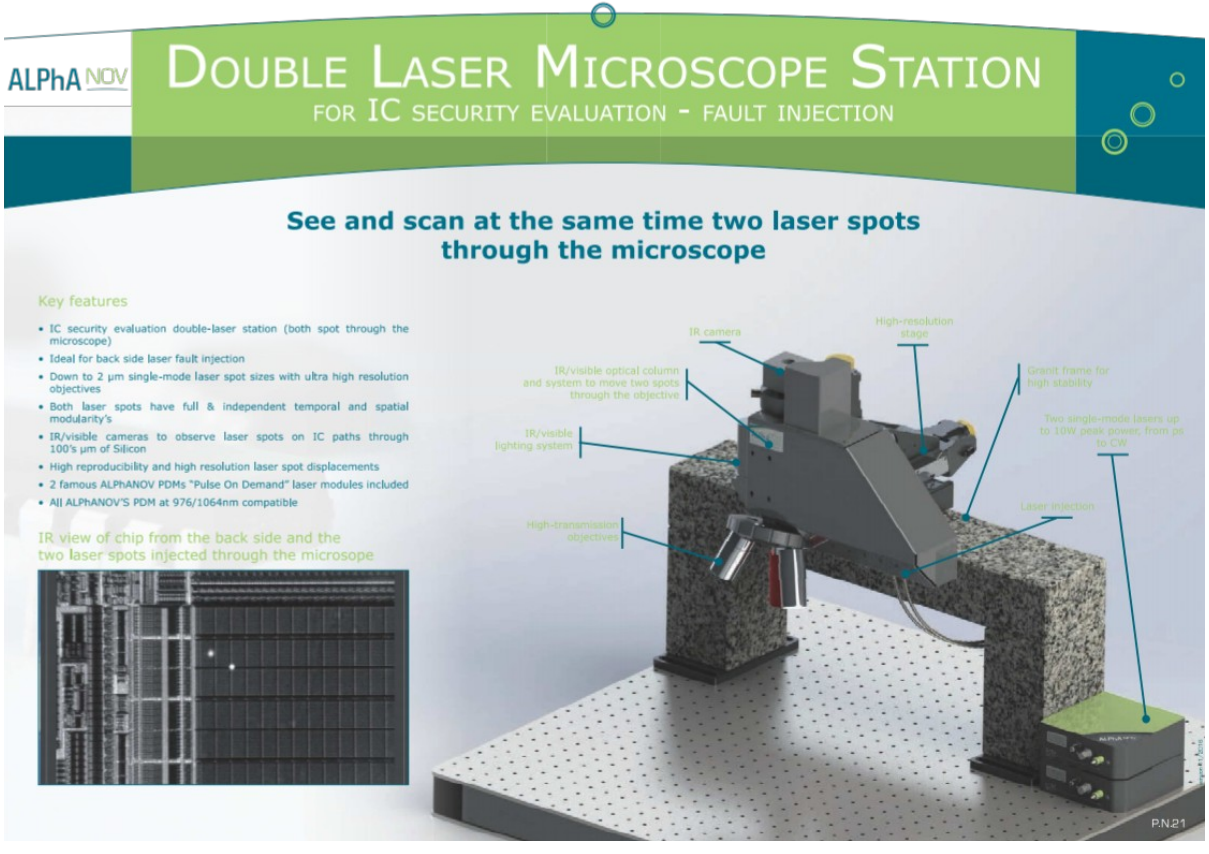


Fault attack vectors – light cont'd

- Lasers/Light



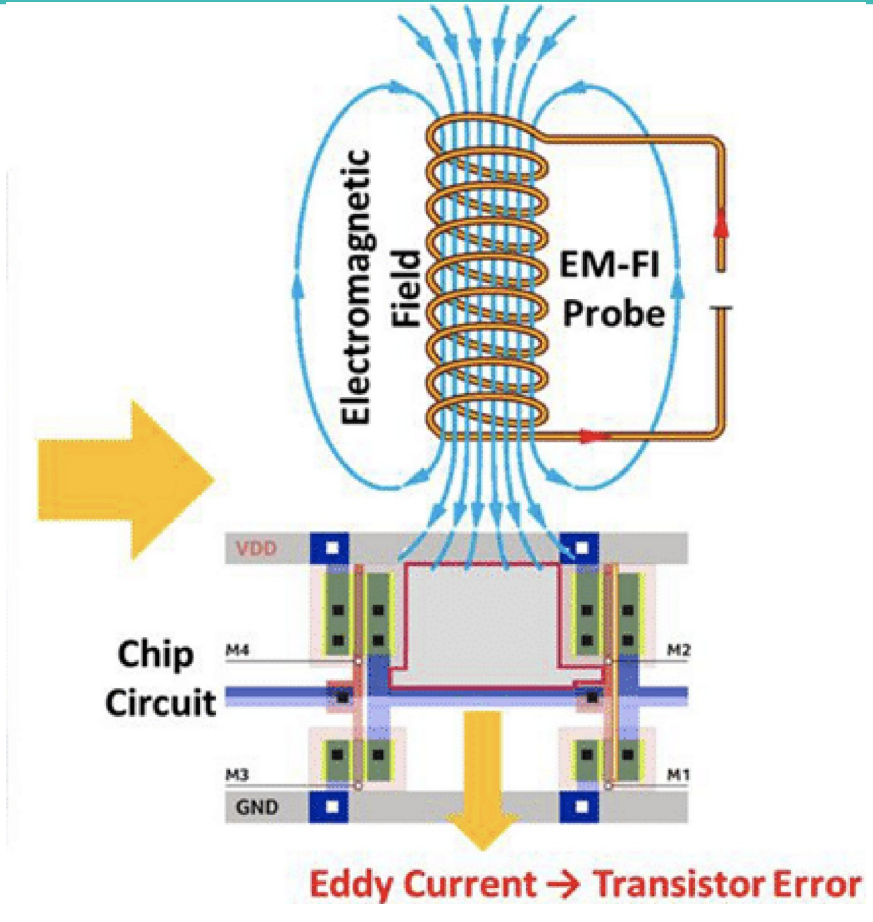
AlphaNov 2020



Images credit to www.alphanov.com

Fault attack vectors -- EMFA

- Electro Magnetic



Lim, H., Lee, J., & Han, D. G. Novel Fault Injection Attack without Artificial Trigger. *Applied Sciences*, 2020.

Fault attack vectors -- BBI

- Body Bias

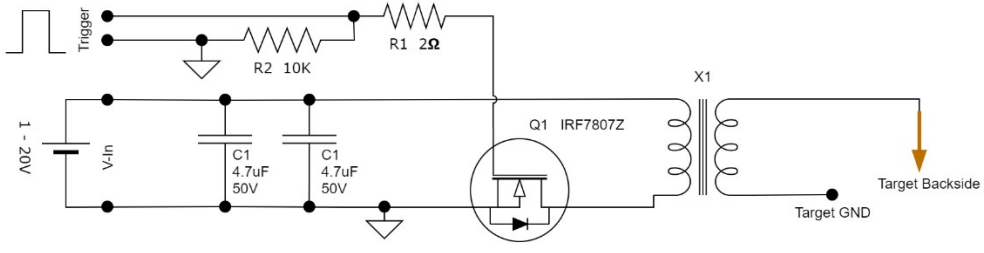
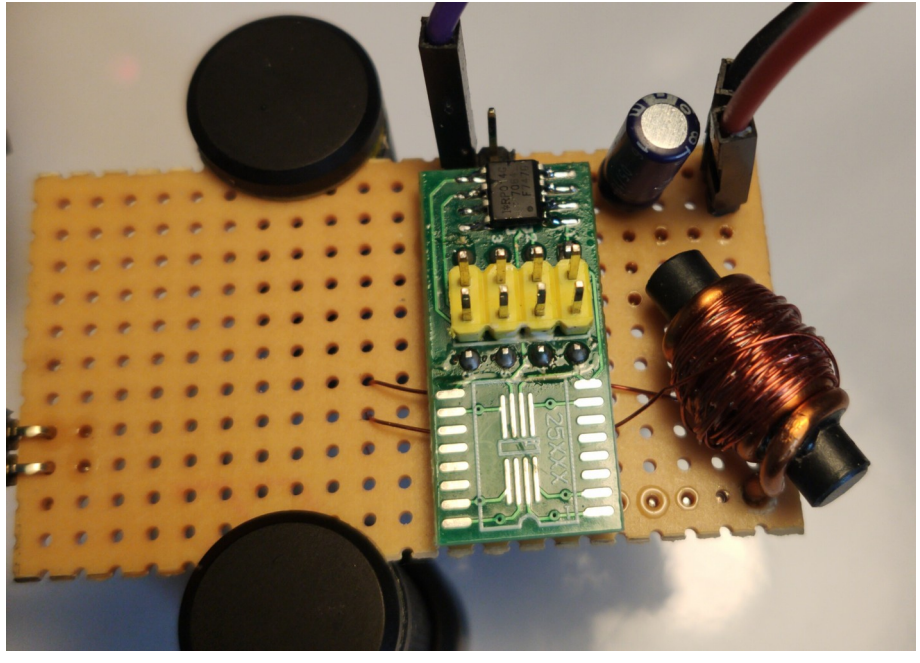


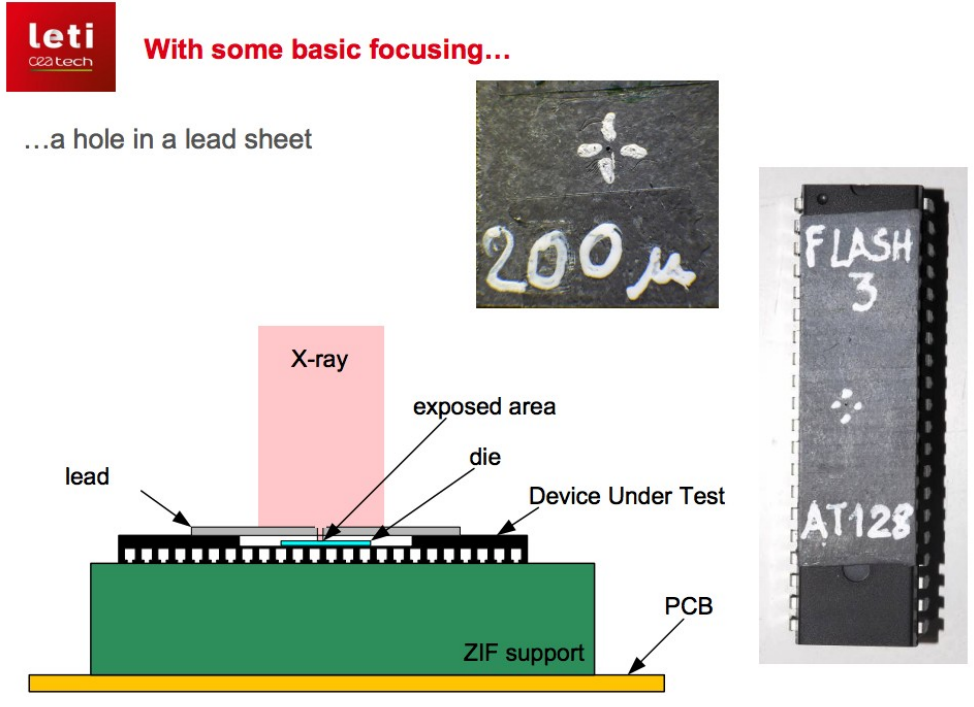
Fig. 2: The BBI injection device relies on transformer X1 to produce a higher voltage from a simple capacitor based circuit.



https://www.balda.ch/posts/2021/Oct/05/bbi-experiments/

Fault attack vectors

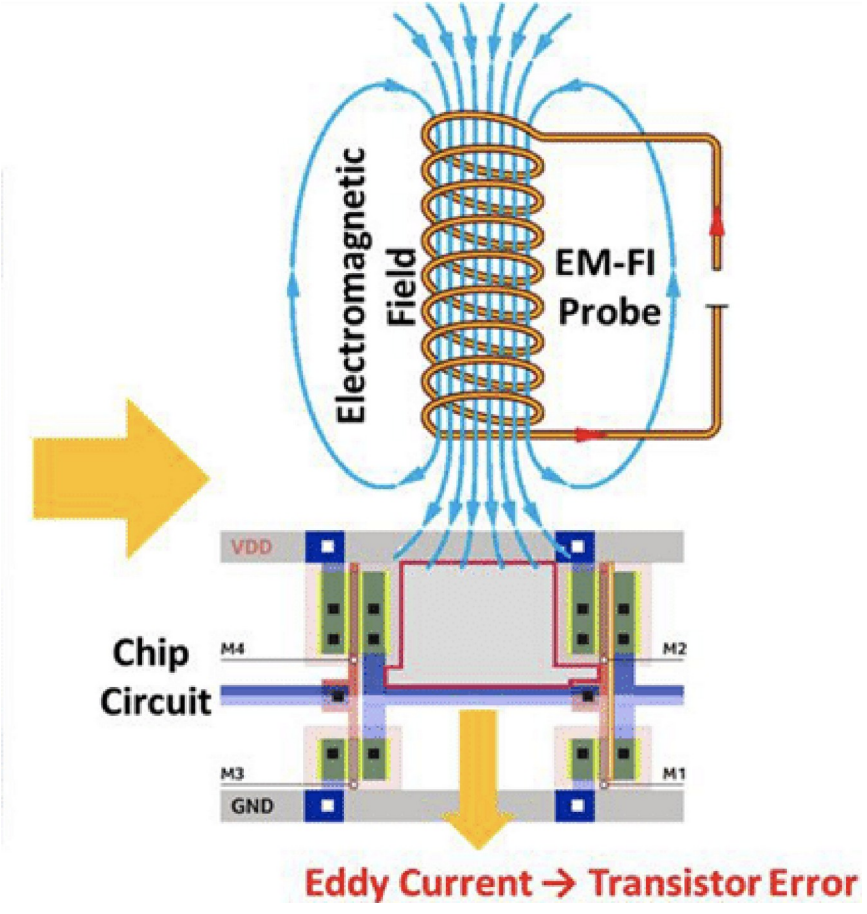
- X-rays



Anceau, S.et al. “Nanofocused X-ray beam to reprogram secure circuits”. CHES 2017.

Why EMFA?

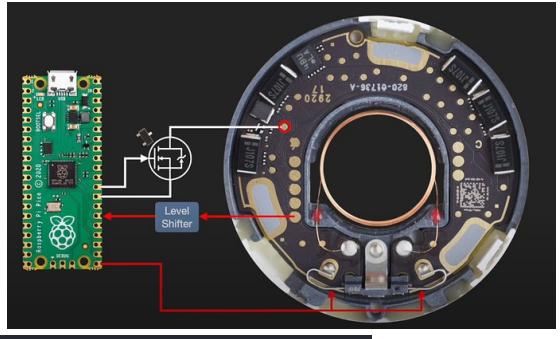
- No depackaging
- Relatively reduced risk
- Portable
- Very effective



Recent Low cost attacks and tools

Recent low-cost attacks in literature

- Chip.Fail
  - bring fault-injection attacks to the masses
  - Targets: STM32F2, ESP32, SAM L11 and D21 ,nRF52840
- Wallet.fail
  - Ledger Nano S
- Raelize
  - Fault attack on AUTOSAR
  - ESP32 Secure Boot bypass using iceGlitch
- LimitedResults
  - nrf debug resurrect/ EFM32 Gecko
- Kraken.com
  - Glitching Trezor's hardware wallets

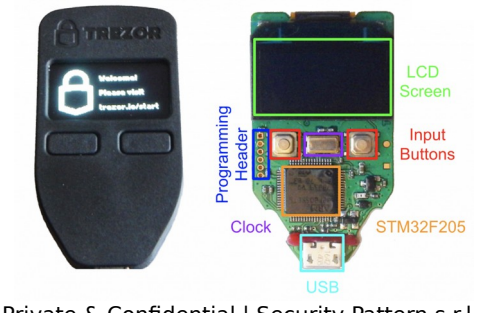


Espressif ESP32: Bypassing Secure Boot using EMFI

Friday, Jul 24, 2020

nRF52 Debug Resurrection (APPROTECT Bypass) Part 1

Posted on June 10, 2020 by LimitedResults



Enter the EFM32 Gecko

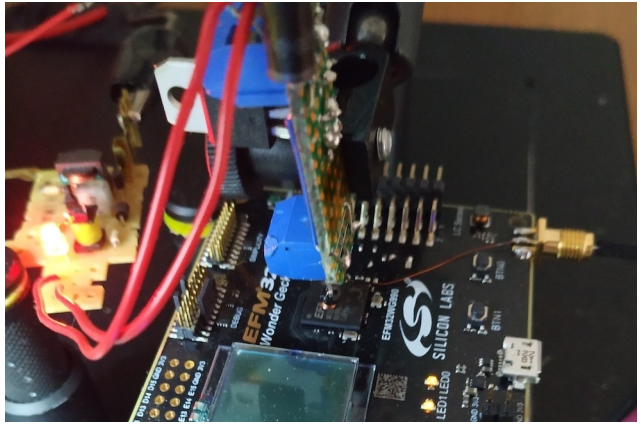
Posted on June 22, 2021 by LimitedResults

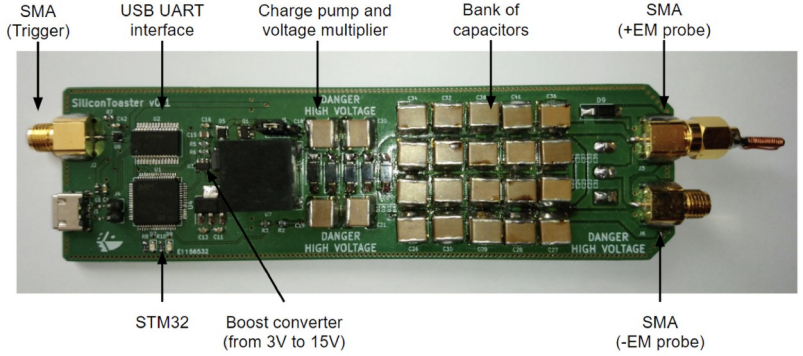
This new post presents a hardware exploit to unlock the debug port on the EFM32 Gecko MCUs Series 1 designed by Silicon Labs.

SEC PAT

EMFA tools

- ChipShouter -- NewAE
- SiliconToaster -- Ledger
- Der Injektor -- LimitedResults





https://www.newae.com/products/NAE-CW520
https://limitedresults.com/2021/06/enter-the-efm32-gecko/
Abdellatif, K. M. et al. "SiliconToaster: a cheap and programmable EM injector for extracting secrets." *FDTC* 2020.

ChipYeller?

- Uses a Capacitor
- Presented ~2 weeks ago

A 0$ EMFA tool

Dangerous experiment

Image credits to Wikipedia.com author: Sonarpulse

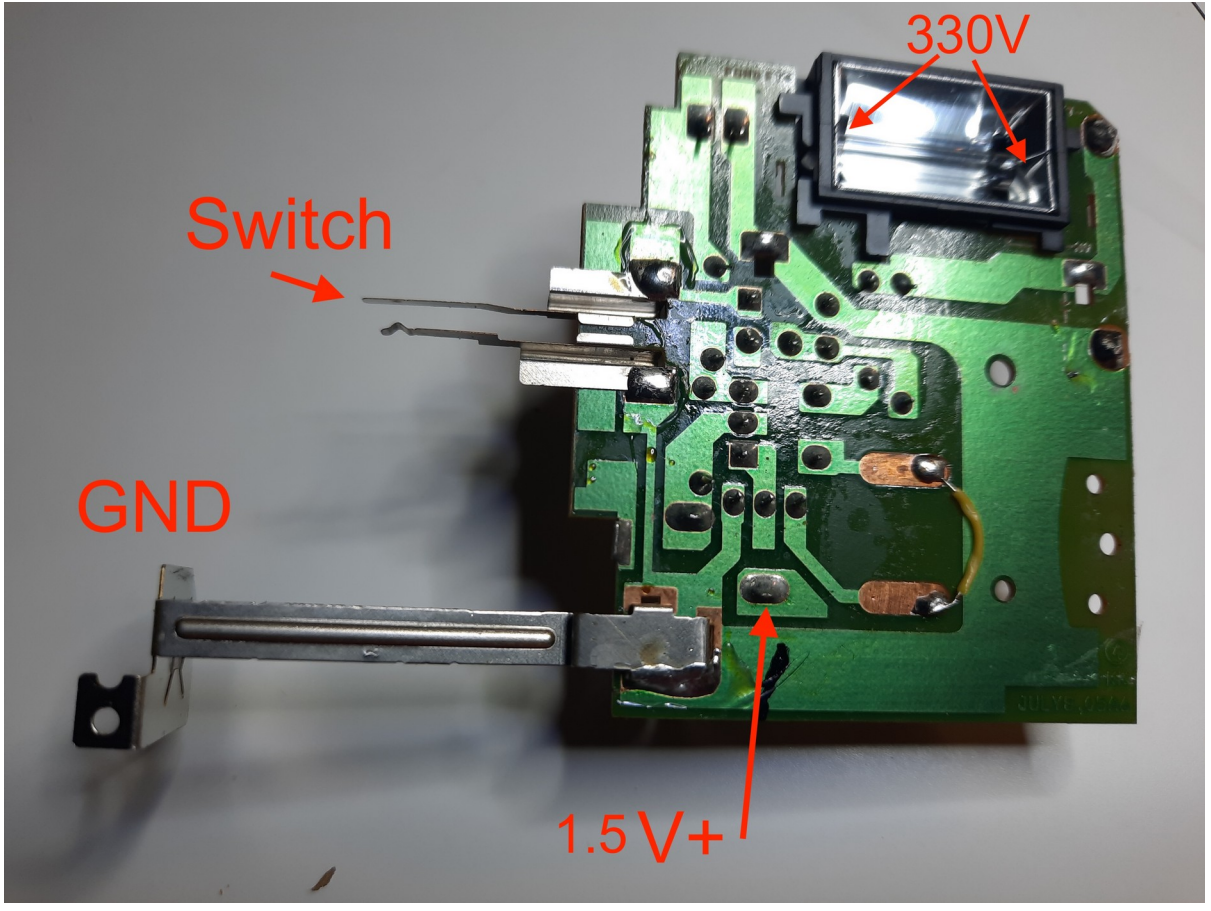
Overview

- Attacker
  - ILFORD HP5 plus 400 disposable camera

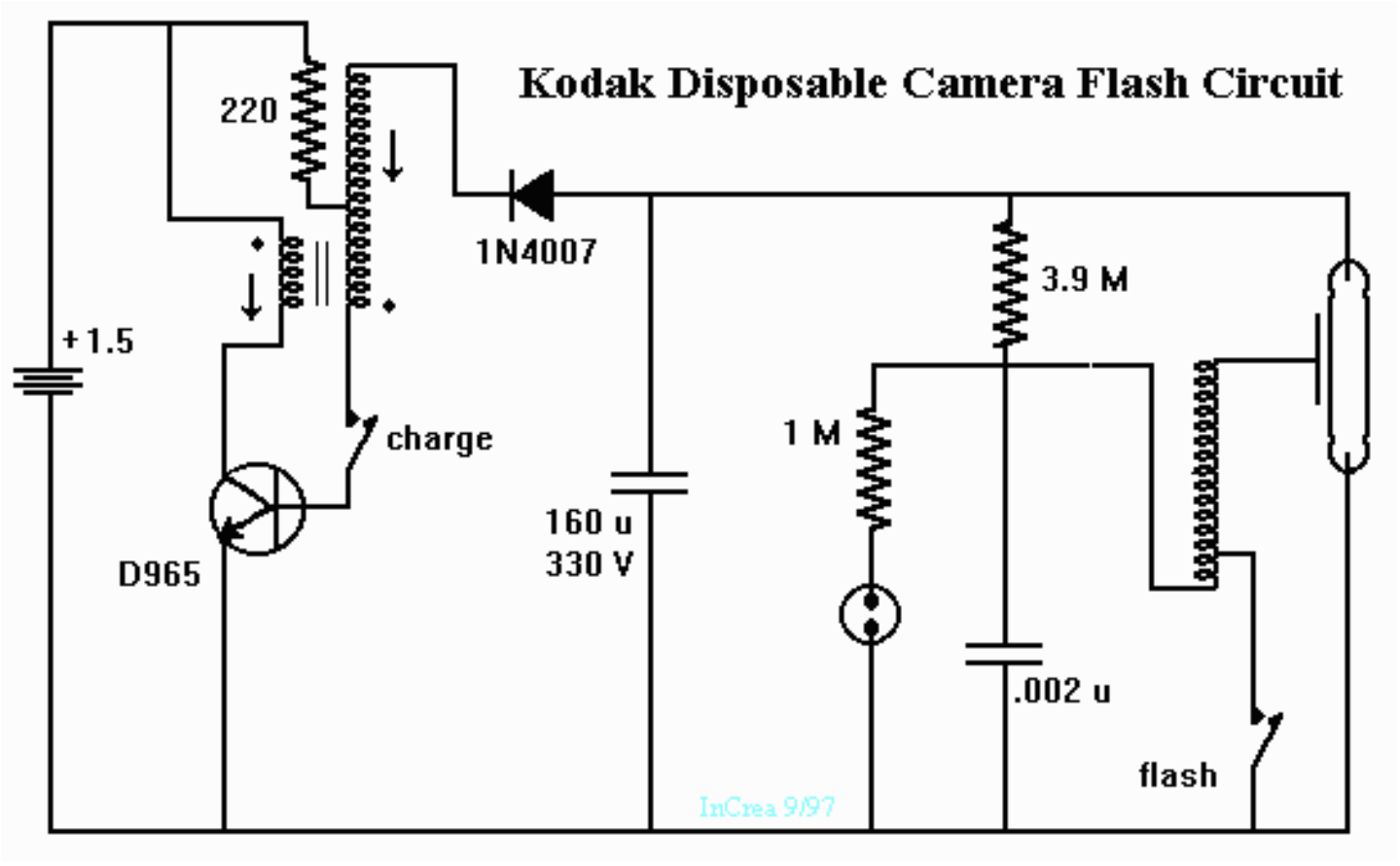
- Target
  - Arduino mini
  - ATMega328

Images credit to ILFORD and Arduino

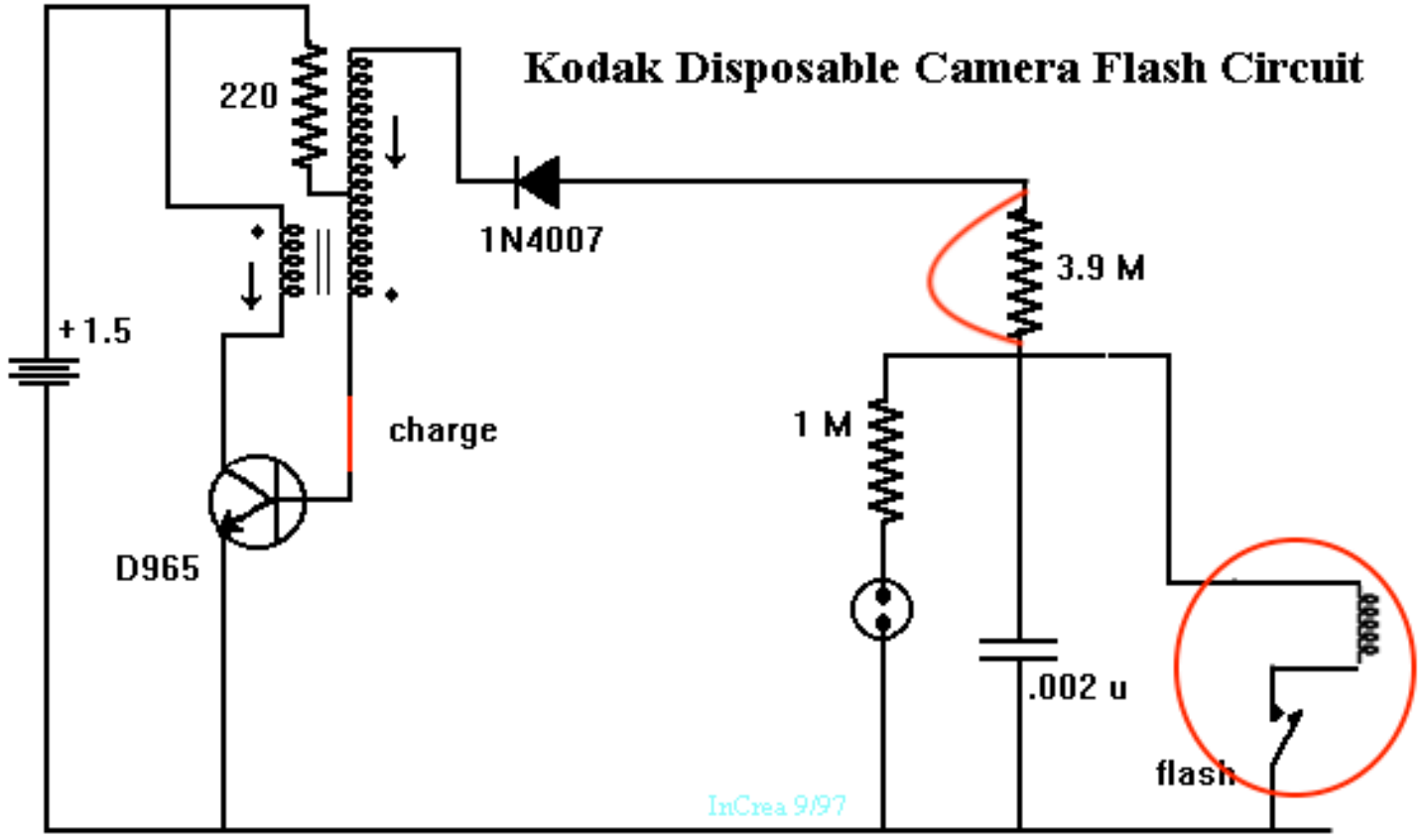
Camera opening



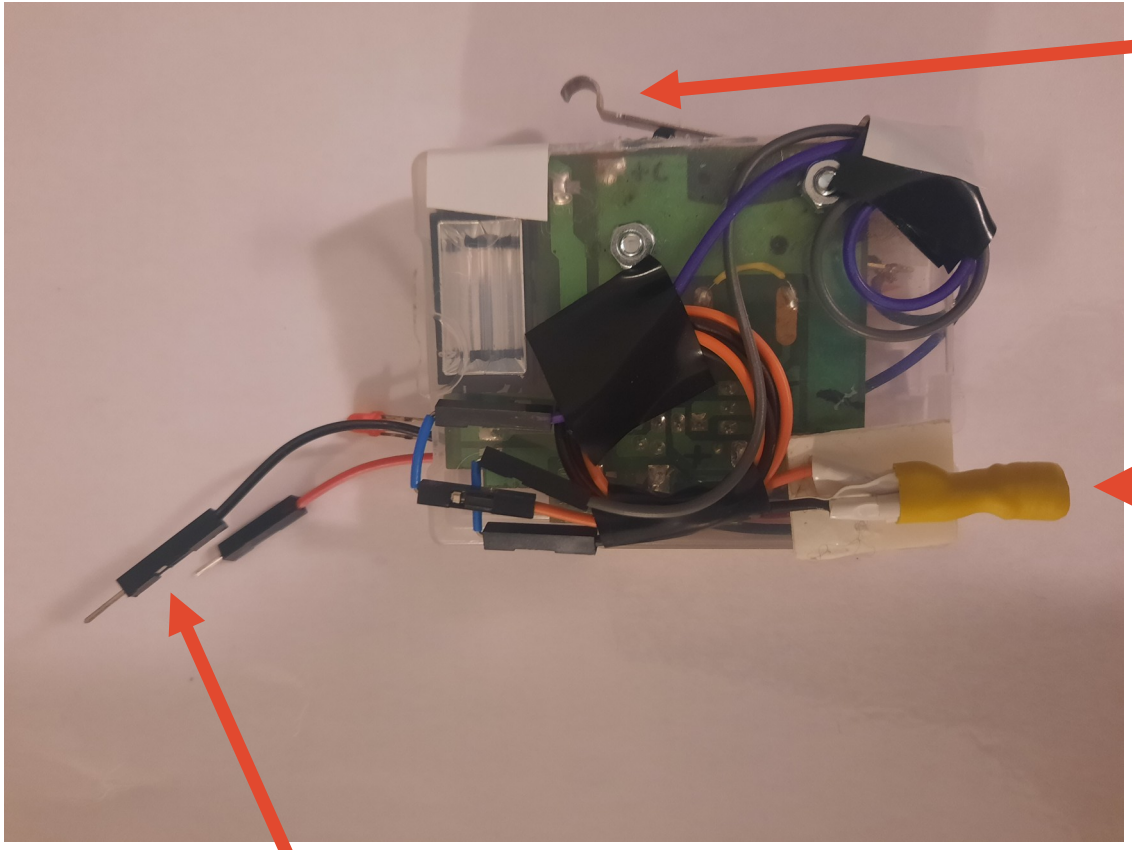
Camera circuit



Brian Mork @ http://www.increa.com/reverse/dc/


Kodak Disposable Camera Flash Circuit
220
1N4007
3.9 M
+1.5
charge
1 M
D965
.002 u
flash
InCrea 9/97

M0lesTA



Demo

- Attacker
  - ILFORD HP5 plus 400 disposable camera

- Target
  - Arduino mini
  - ATMega328

Conclusions

- Fault attacks are a real threat
  - Easily and commonly exploited in the wild
  - IoT usually not protected against
- You don’t need expensive tools to start hacking
  - Nor deep knowledge
- EMFA don’t need to decap target
  - Work from distance!
  - Very effective and used also against top security (passports/credit card)
- Not all fault attacks concern crypto
- Recycling is fun!