Relevance of post-silicon emulation for code validation

JAIF 2021

Lionel Rivière, Aurélien Vasselle, **Guillaume VINET**

eShard

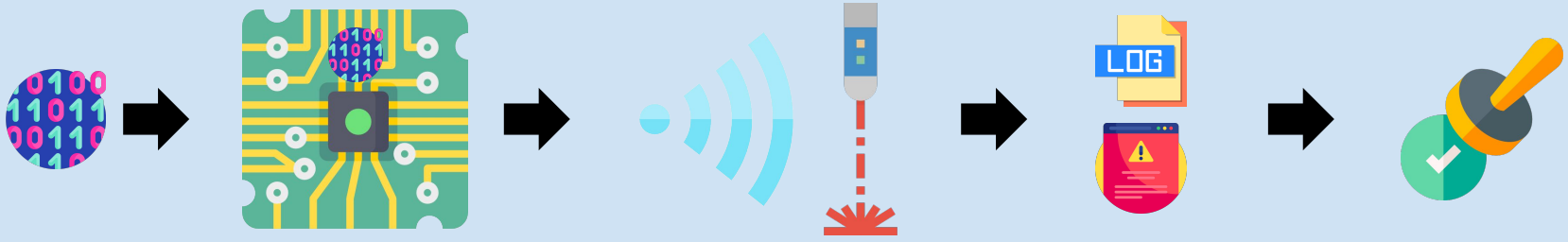
Agenda

Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Who am I?

- Senior security analyst in embedded devices security
- 15 years assessing the security of
  - smart cards (banking applications, electronic passports, Integrated Circuit),
  - point-of-sale (POS),
  - Mobile Application.
- Areas of expertise:
  - Reverse engineering of Android applications
  - Code emulation
  - White-Box Cryptography (WBC),
  - Perform security analysis/trainings.

How to validate your code?



Binary code

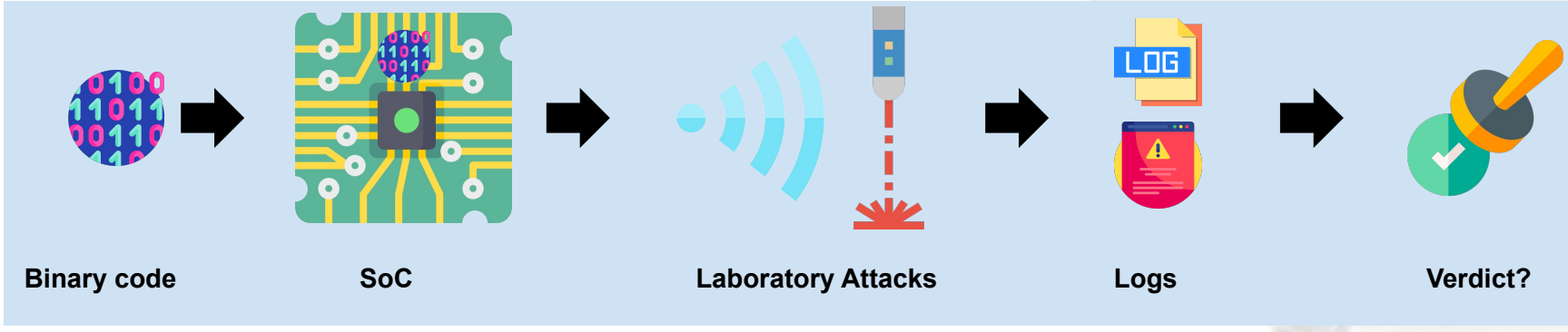
SoC

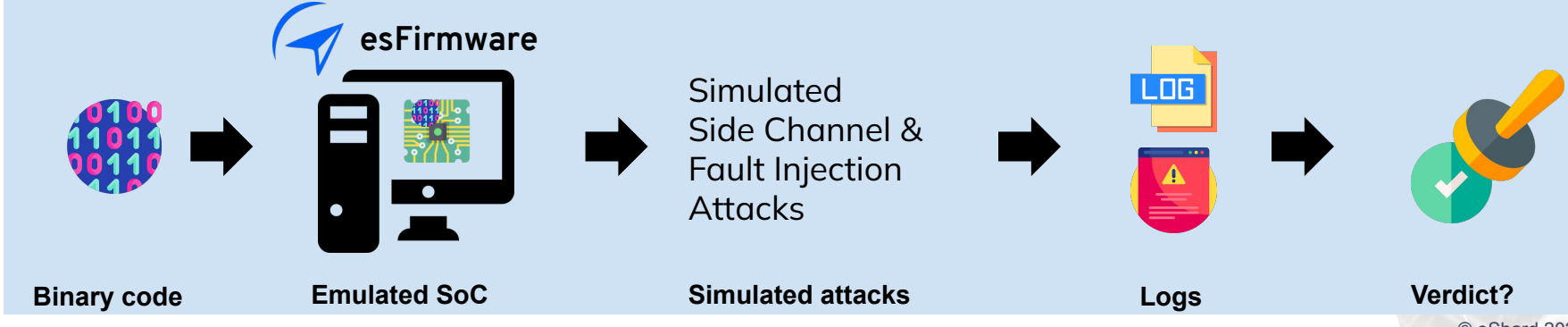
Laboratory Attacks

Logs

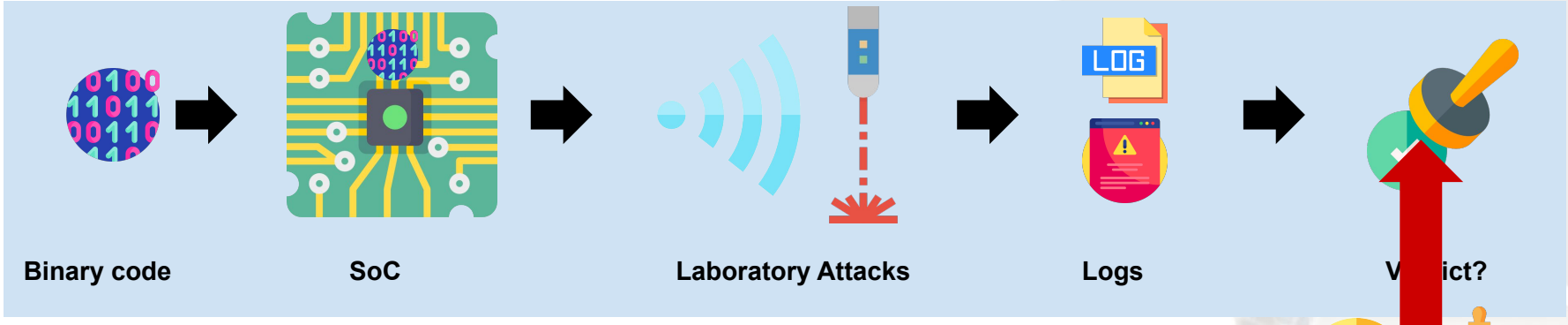
Verdict?

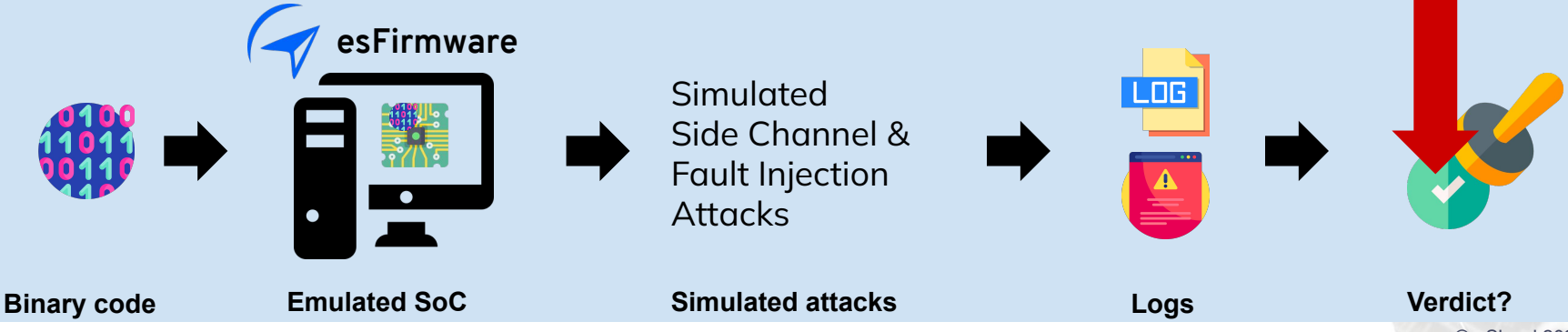
How to validate your code?





How to validate your code?

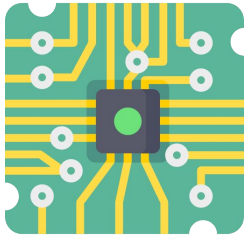




Agenda

Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Target



Hardware target

Software target

System on a Chip (SoC):
- 4 cores Cortex-A53 (up to 1.8GHz per core)
- 1x Cortex-M4 core up to 400MHz
- 1 GPU (2D/3D)
- Lithography: 14 nm

Usage:
- Automotive (Engine Control Unit),
- Smart Home (Set Top Boxes),
- Energy gateway

Bare-metal Operating System:
- Based on customized U-boot bootloader
- 1 core Cortex-A53
- UART shell with test commands
- Triggers with GPIO
- Naïve AES-128 algorithm

Agenda

Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Attack on the real target

1 **LASER Fault Injection**

With test code:
- ARM 64 registers x0 to x30 sensitivity area identified
- Bit flip fault model confirmed

670,740 faults (in ~ 3 days)
- 77.8% : no effect
- 17.57% : mutism
- 4.44% : faulty outputs

- 29,792 faulty outputs (14778 different)
- Key found!

Attack on the real target

1 LASER Fault Injection

With test code:
- ARM 64 registers x0 to x30 sensitivity area identified
- Bit flip fault model confirmed

670,740 faults (in ~ 3 days)
- 77.8% : no effect
- 17.57% : mutism
- 4.44% : faulty outputs

- 29,792 faulty outputs (14778 different)
- Key found!

2 Electro-Magnetic Fault Injection

With test code:
- No registers sensitivity area identified
- No fault model confirmed

406,824 faults (in ~ 1 day 18 hours)
- 95.13% : no effect
- 3.89% : mutism
- 0.18% : faulty outputs

- 722 faulty outputs (604 different)
- Key found!

Attacks on the real target

Freeze-and-wake-up fault model with Electro-Magnetic Attacks

1

Correct execution

```
0x2010    ...
0x2014    MOV     X3, 0xF5
0x2018    OR      X3, 0x100
0x201C    AND     X3, 0x0F
```

```
X3 = 0xA7
X3 = 0xF5
X3 = 0x1F5
X3 = 0x5
```

2

Freeze-and-wake-up model: bits values are unchanged during X instructions**:**

- **Mask**: which bits are frozen
- **Persistence of effect**, number of instructions

Target: X3
Mask: 0xF0F
Persistence of effect: 4 instructions

```
0x2010    ...
0x2014    MOV     X3, 0xF5
0x2018    OR      X3, 0x100
0x201C    AND     X3, 0x0F
```

```
X3 = 0xA7
X3 = 0xF7
X3 = 0x0F7
X3 = 0x007
```

Agenda

Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Target emulation

esFirmware: overview

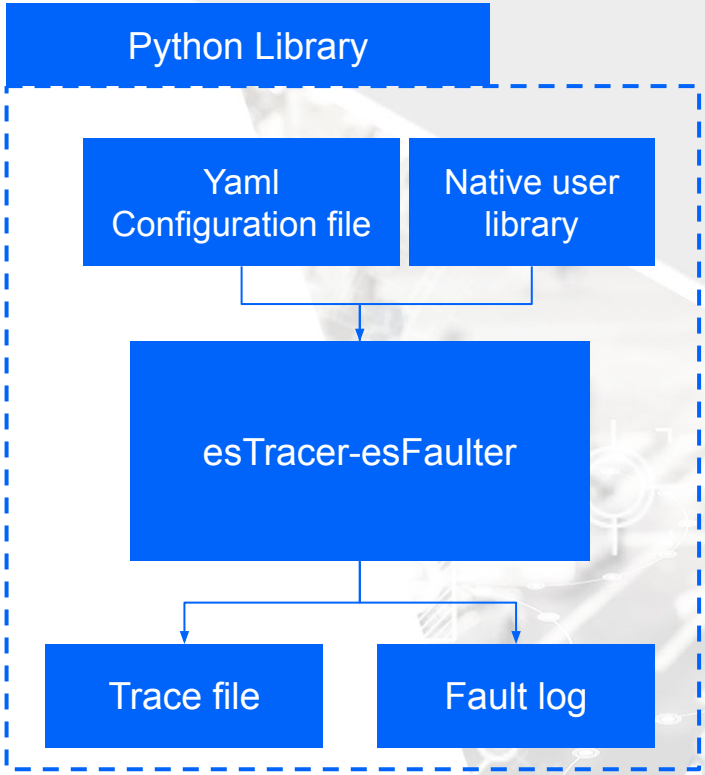
Supported architecture:
- i386, x86-64,
- ARM 32 & 64 bits (ARMv7, ARMv8)

What to attack?
- registers

How to attack?
- Fault model: Bit flip, set/reset …

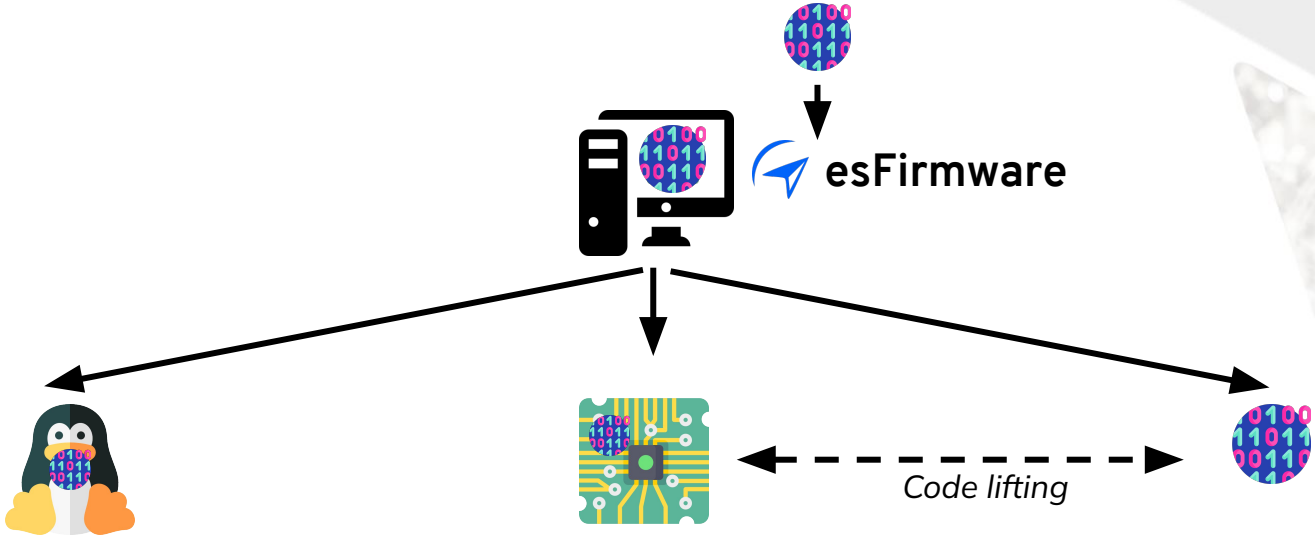
When to attack?
- Instruction number
- Pattern detector

Where to attack?
- PC registers
- Instruction type



Target emulation

esFirmware: emulation mode



Linux ELF Application

GDB
The GNU Project Debugger

SoC Firmware

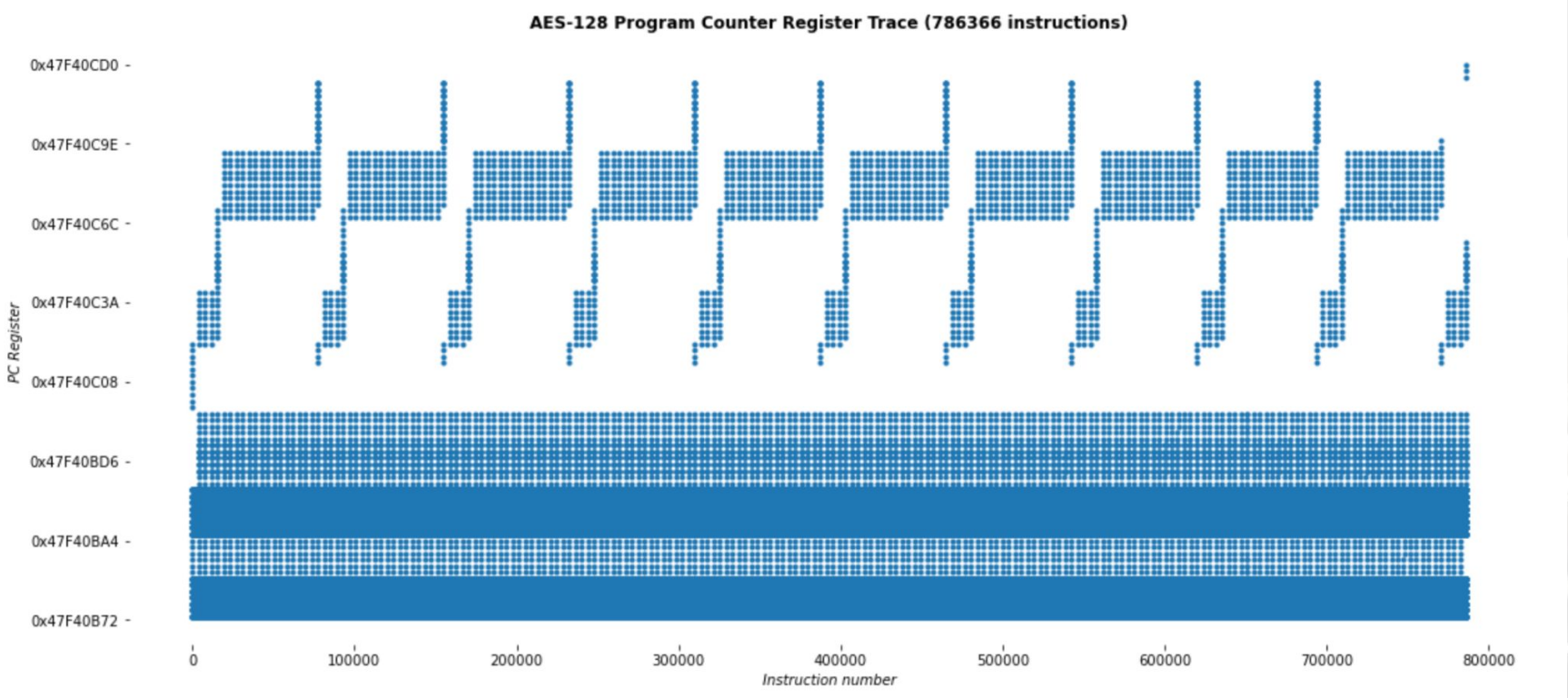
GDB
The GNU Project Debugger

Piece of binary

GDB
The GNU Project Debugger

Target emulation

AES-128 Tracing



Agenda

Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Attacks on the emulated target

Avoiding ineffective faults

Example with X3 register alteration

1 **Fault injection inducing duplicated results**

Instruction 1	MOV	X21, X4
Instruction 2	CMP	X3, #4

2 **Fault injection ignored**

Instruction 3	MOV	X3, #4

registers	distribution
x5	2
x6	2
x4	22
x1	132
x0	206
x11	684
x13	855
x2	968
x3	52983
x7	52987
x12	103622
x15	103733
x8	155435
x10	209888
x14	261867

Attacks on the emulated target

Results

1 LASER Fault Simulation

Targets:
- 15 registers targeted

Bit flip fault model:
- from bit 0 to 31

28,225,017 faults:
- 512 runs in ~17h with 32 cores*

Results:
- 27.2% : no effect
- 0.2% : mutism
- 72.6% : faulty outputs

- 20,501,100 faulty outputs (58,939 different)
- Key found!

** Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz (28 physical cores - 56 logical cores)*

Attacks on the emulated target

Results

1 LASER Fault Simulation

Targets:
- 15 registers targeted

Bit flip fault model:
- from bit 0 to 31

28,225,017 faults:
- 512 runs in ~17h with 32 cores*

Results:
- 27.2% : no effect
- 0.2% : mutism
- 72.6% : faulty outputs

- 20,501,100 faulty outputs (58,939 different)
- Key found!

2 Electro-Magnetic Fault Simulation

Targets:
- 15 registers targeted

Freeze-and-wake-up fault model:
- Freeze mask: 0xFF, 0xFFFF, 0xFFFFFF, 0xFFFFFFFF
- Persistence of effect: 1 to 9 instructions

Focus on two last rounds

10,034,476 faults:
- 540 runs in ~4h with 32 cores*

Results:
- 67.35% : no effect
- 0.08% : mutism
- 32.57% : faulty outputs

- 3,268,395 faulty outputs (16,357 different)
- Key found!

** Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz (28 physical cores - 56 logical cores)*

Agenda

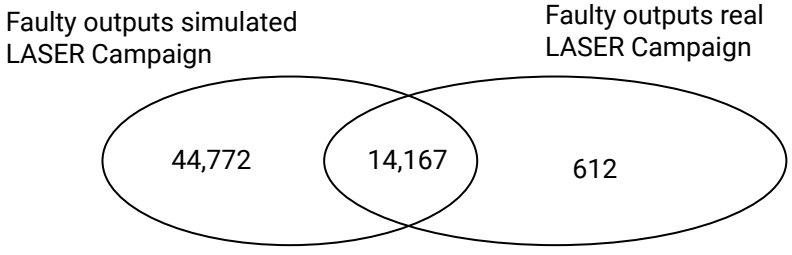
Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Real Life & Emulation result comparison

Results

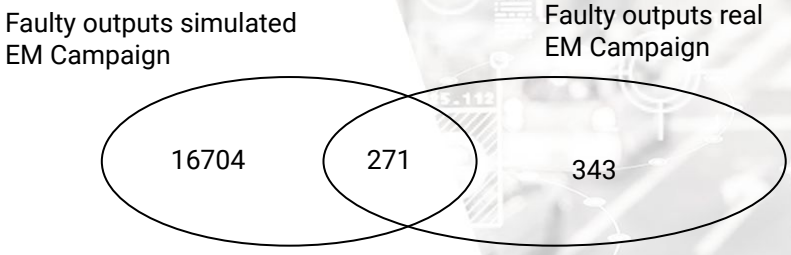
1 **Simulated LASER Fault Injection**

- 95.8% outputs found (14,167)
- 4.14% outputs not found (612)



2 **Simulated Electro-Magnetic Fault Injection**

- 44.1% outputs found (271)
- 55.9% outputs not found (343)

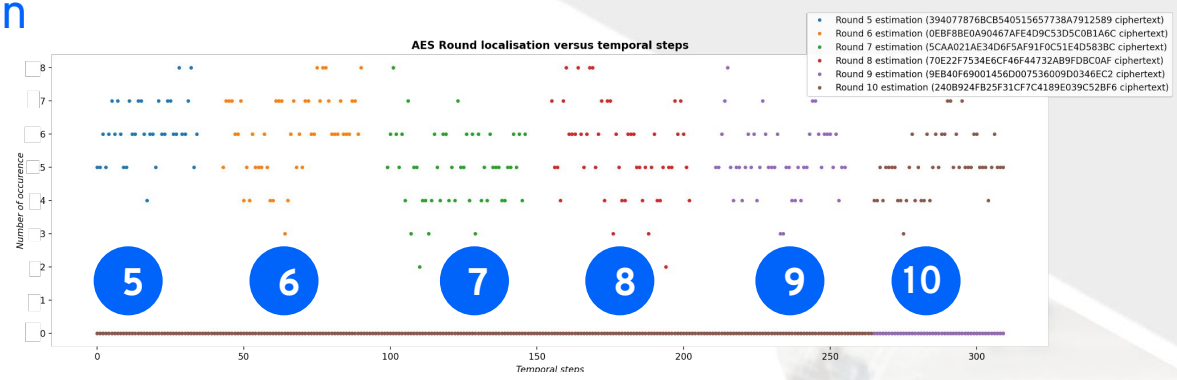


Successful fault model validation with test code is a significant asset

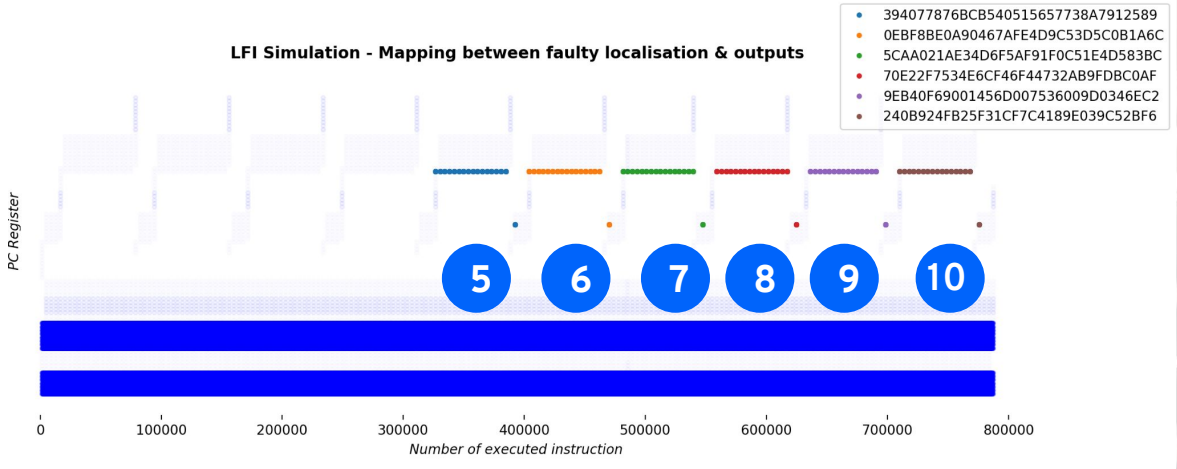
Real Life & Emulation result comparison

Results - Fault localization

LASER Real attack



LASER Simulation



Agenda

Introduction
Target
Attacks on the real target
Target emulation
Attacks on the emulated target
Real Life & Emulation results comparison
Conclusion

Conclusion

Disturbance of a naïve AES-128 on a SoC with fault injection:

- LASER: success
- Electro-magnetic: success

Simulation of this code with esFirmware:

- Validation platform: ELF/SoC/Piece of binary
- Simulated attacks:
  - LASER: success with 95.8% faulty output recovered
  - EM: less successful with 44.1 %
- Fault model validation is a key point

ANY QUESTION ?