Trusted Analysis Platform

Laurent Sauvage, Télécom Paris

February 2022

Equipment and Software

SCA boards

- NewAE ChipWhisperer
  - Nano: Cortex-M0 32-bit
  - Level 1 Kit: XMEGA 8-bit, STM32F3 32-bit
- SASEBO
  - R: ASIC, Xilinx Virtex-II Pro XC2VP30
  - B: Altera Stratix II EP2S15 and EP2S30
  - G: Xilinx Virtex-II Pro XC5VP7 and XC2VP30
  - GII: Xilinx Virtex-5 XC5VLX30/LX50 and Spartan-3A XC3S400A
  - W: Xilinx Spartan-6 XC6SLX150 and Atmel ATMega-163 IC card

Other FPGA victim boards

- M2S090TS-EVAL-KIT SmartFusion2 Security Evaluation Kit: Microsemi M2S090TS
- M2S150-AV-DEV-KIT SmartFusion2 Advanced Development Kit: Microsemi M2S150TS
- Digi-Key SmartFusion 2 Maker Board: Microsemi M2S010
- Avnet ZedBoard: Xilinx Zynq-7000 SoC
- iCEstick Evaluation Kit: Lattice iCE40HX-1k
- Arrow MAX1000: Intel MAX10 10M08SAU169C8G
- FF324 Proto Board: Xilinx Virtex-5 LX

Other CPU victim boards

- LAUNCHXL2-RM57L Hercules RM57Lx LaunchPad Development Kit: Texas Instruments RM57L843 32-bit
- ATSAM4C-EK SAM4C32 Evaluation Kit: Atmel SAM4C16C 32-bit
- STM32F4DISCOVERY: STMicroelectronics STM32F407 32-bit
- Kanda STK300 AVR Starter Kit: Atmel ATmega128 8-bit

Virtual victims (traces generated by simulation)

- any FPGA
- STM32F103RB, STM32F107VC, STM32F405RG, STM32F407VG, STM32F407ZG, STM32F429ZI, STM32L152RE
- RISC-V ISA

Digital storage oscilloscope (DSO) & digitizer (DC)

Provider	Model	Max Bandwith	Max Sampling Rate	Resolution	Memory Depth
Keysight	DSO90404A	4 GHz	20 GSa/s	8 bits	**512 Mpts**
Agilent	DSO9254A	2.5 GHz	20 GSa/s	8 bits	51 Mpts
Agilent	DSO54855A	**6 GHz**	**40 GSa/s**	8 bits	1 Mpts
Acqiris	DC252	3 GHz	8 GSa/s	**10 bits**	512 kpts
Acqiris	DC440	100 MHz	420 MSa/s	**12 bits**	64 kpts

Signal analyzer (for e.g., TEMPEST)

- Agilent Technologies PXA N9030A, 3 Hz – 8.4 GHz, **250 MHz analysis bandwith**

Electromagnetic probes

- Langer RF1 set
  - RF-K 7-4, H-Field Probe 30 MHz up to 1 GHz
  - RF-U 2.5-2, H-Field Probe 30 MHz up to 3 GHz
  - RF-R 3-2, H-Field Probe 30 MHz up to 3 GHz
  - RF-E 10, E-Field Probe 30 MHz up to 3 GHz
- Langer RF2 set
  - RF-R 400-1, H-Field Probe 30 MHz up to 3 GHz
  - RF-R 50-1, H-Field Probe 30 MHz up to 3 GHz
  - RF-U 5-2, H-Field Probe 30 MHz up to 3 GHz
  - RF-B 3-2, H-Field Probe 30 MHz up to 3 GHz
- Langer RF3 mini set
  - RF-B 0.3-3, H-Field Probe mini 30 MHz up to 3 GHz
  - RF-R 0.3-3, H-Field Probe mini 30 MHz up to 3 GHz
- Langer ICR HH100-6 set, **100 µm**, 2.5 MHz – 6 GHz, horizontal field
- Langer ICR HV100-6 set, **100 µm**, 2.5 MHz – 6 GHz, vertical field

Langer IC scanner

- FLS 102
- ICS 105 **4-Axis** Positioning System

Digital signal processing

- Filtering (LP, HP, BP)
- Denoising
- Realignment (cross correlation, SAD, elastic, etc.)
- FFT, STFT, wavelet

Fault injection attack

- Clock glitch: Tektronix DTG5078, **1 ps resolution**
- EM glitch: AVTECH AVL-5-B-TR, **400 V**, 2.5 ns (tr)
- EM glitch: Agilent MXG Analog Signal Generator N5181A, **1 ns (tr)**
- Laser glitch: ALPhANOV Laser station, **double source**
- Bitstream fault injection attack (BiFI)

Supported Leakage Assessment Methods

- NICV, TVLA (t-test, χ^2-test), DL-LA using Jean Zay supercomputer (28 petaflops per second, 2696 GPU-based accelerators)
- Acquisition campaign up to 1,000,000 traces or more
- Typical DUT clock: 10 MHz (IoT) to 1 GHz (smartphone)

All of State-of-the-Art Attacks Supported

- SPA, DPA, CPA, MIA, TA, LRA, etc.
- Idem using EM (SEMA, DEMA, CEMA, etc.)
- SFA, DFA, FSA, DFIA, FBA
- Same graphical representations as in DPA Contest:
  - minimum traces to disclosure (MTD)
  - global success rate (GSR)
  - partial success rate (PSR)
  - partial guessing entropy (PGE)

Sharing of Measurements

- FTP server
- SQL server

Feedback Meetings by Visioconference

Personnel

- Prof. Laurent Sauvage, head of Trusted Analysis Platform
- Arnaud Varillon, PhD student

- Ibrahim Maassarani, PhD student
- Alexandre Sanson, undergraduate student

Lab Operation From March 15 to June 30

Contact: laurent.sauvage@telecom-paris.fr