eShard

Side-Channel attacks: Why performance matter?

COSADE 2022

Guillaume BETHOUART, Lionel RIVIERE *(presenter)*

[insert_whatever_here] **is secure!**

🤷‍♂️ it depends...

- The notion of **security** is relative
  - Context ⏱️💰👥🇪🇺🚨
- Security evaluation
  - Scheme
  - Interpretation
- The security analyst constraints
  - No time, not in the scope → can't guarantee the security
  - What can you do with more time?

The importance of performance

🏆 A security evaluation context

What the Joint Interpretation Library (JIL) says regarding the Common Criteria (CC) Methodology?

- **Interpretation**
- Based on smartcard evaluation experience and inputs from ISCI / JHAS
- **Guidance**
- CC does not distinguish between **identification** and **exploitation** phases, JIL does.
- Relevant factors for rating an attack:
  - Elapsed time
  - Expertise
  - Knowledge of the TOE
  - Access to the TOE
  - Equipment
  - Open samples availability.

https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3-1.pdf

The importance of performance

⏱️ Elapsed time

- Attack could be re-applied to other TOE

→ *What about elapsed time then?*

- Exploitation

→ *Uses script or set of instruction defined during the identification phase*

From weeks → hours?

🥷 Expertise

- Ability to implement attacks, develop setups and procedures

→ HW manipulation, SW attacks, cryptography, fault injection, side channel, reverse

- Capability to operate necessary tools and equipment
- Redesigning or adapting existing complex attack techniques

From Experts → Proficient?

🔬 Equipment

- Specialized

"hundred of PCs linked across the Internet"
"extensive attack scripts or programs"

- Bespoke

"very sophisticated software"
"complex and dedicated software"
"not available for purchase"

- Rated extra for identification

"an evaluator has to adapt his dedicated analysis software, alignment tools/scripts."

From Bespoke / Specialized → Standard?

	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical (see below)	*	*

Table 1: Rating for Elapsed Time

	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6

Table 3: Rating for Expertise

	Identification	Exploitation
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8

Table 7: Rating for Equipment

The importance of performance

🛠️ Tools

The range of equipment at the disposal of a potential attacker is constantly improving:

- Computation power increases
- Cost of tools decreases
- Availability of tools can increase
- New tools can appear, due to new technology or due to new forms of attacks

The importance of performance

🎯 Attack potential

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
> four months[4]	6	10
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*
Access to TOE (1)		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized (2)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples/Samples with known secrets		
Public	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

The importance of performance

🎯 Attack potential rating

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month		
> one month		
> four months[4]		
Not practical		
Expertise		
Layman		
Proficient		
Expert		
Multiple Expert		
Knowledge of the TOE		
Public		
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*

Access to TOE [1]		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
		*
		0
		2
		4
		6
		8
		NA
		NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

Range of values*	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

Table 13: Rating of vulnerabilites and TOE resistance

The importance of performance

Acquisition and attack

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week		4
< one month		6
> one month	5	8
> four months[4]	6	10
Not practical	*	*
Expertise		
Layman		0
Proficient		2
Expert		4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical	9	*
Not practical	*	*

Decreased duration

Reduced complexity

Access to TOE [1]		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard		2
Specialized		4
Bespoke		6
Multiple Bespoke	7	8
Open samples/Samples with known secrets		
Public	0	NA
Restricted	2	NA
Sensitive	5	NA
Critical	9	NA
Not practical (Samples with known secrets only)	*	NA

Optimized computation resources exploitation

The importance of performance

Same target different means

Imagine two security labs:

- The first one uses a cutting-edge tool. The expert can acquire, align and attack **50 million traces**, which represent 1TB of data, within **two weeks**. The analysis covers tens of intermediate data, with various leakage models and covers first and second order attacks.
- The second, within these **two weeks**, can collect and analyse only **2 million traces**. The analyses cover only the first order Hamming weight leakages.

→ **Is it fair to say that these two evaluations provide the same security assurance level?**

The importance of performance

Same outcome different effort

Imagine again... two security labs:

- The first one spent 3 experts, 3 weeks and concluded that the product is vulnerable.
- The second lab spent 1 expert, 3 days and came up with the same conclusion.

→ **Tools (and expert) performances directly impact the attack potential rating.**

SCA Acquisition

From the physical signal to the dataset

- Why does it takes time?
  - DUT / setup prep
  - DUT speed (especially communication)
  - Finding the right signal to acquire (triggering/filtering/processing on scope)
  - Acquiring (sequential loops)
  - Handling samples formats and associated metadata
  - Data transfers

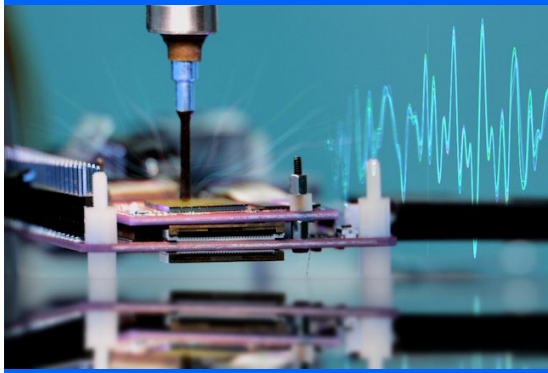
SCA Attacks

From the raw dataset to key extraction

- Why does it take time?
  - Big datasets: amount of traces, amount of samples per trace
  - Signal processing and resynchronization → highly dependent on the analyst skills
  - Multiple
    - information to recover (bit, byte, word, ...)
    - targets: selection functions
    - leakage models: hamming weight, hamming distance, monobit, value, ...
    - leakage detection techniques: TVLA, t-test, potential need for additional acquisition
    - attack techniques: Non-profiled, profiled (templates), deep learning, ...
    - distinguishers: CPA, DPA, MIA, LRA, ANOVA, NICV, SNR, ...
  - First order attack on large dataset and attack frames
  - Second order attack computational complexity
  - Maximize attack path coverage

Each step is potentially time consuming and **must** be optimized

SCA Framework & benchmark



SCARED

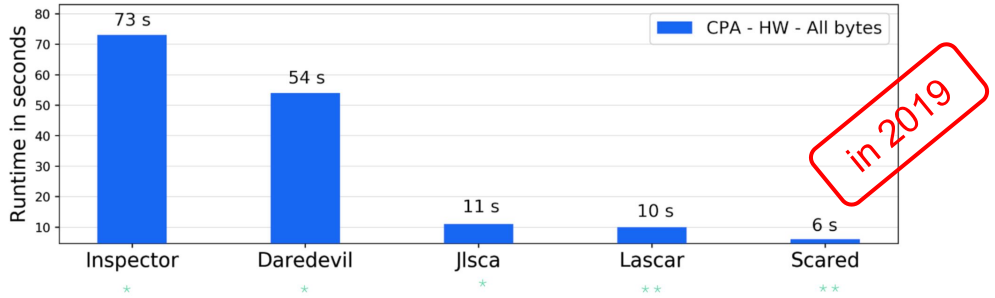
Side channel analysis framework

- Cost : 0 / Availability: open source / Optimized computation
- Features
  - Trace handling with `estraces`
    - binary, TRS, sqlite, ETS, RAM *+ write your own reader*
  - Signal processing for resynchronization purposes and preprocessing traces before analysis
    - pad, filter, fft, moving operators, pattern detection, peak detection
    - Center, serialize, standardize *+ write your own preprocess*
  - Container abstraction defined by
    - Your trace, an analysis frame and a list of preprocesses
  - Intermediate values tools and leakage models
    - Ready-to-use selection functions for DES, AES *+ write your own selection function*
    - Hamming weight, monobit, direct value
  - Analysis
    - Reverse (with the knowledge of the key)
    - Attack analysis
    - Distinguishers: CPA, DPA, ANOVA, NICV, SNR, MIA + Template attacks

Benchmarking

Comparing apples to apples?

- We benchmarked Scared to see where it stands in terms of performance → eshard.com/posts/scared
- We wanted to extend this benchmark but
  - Very few references can be found on the performance of side channel tools
  - Based our benchmark on the main available open source work → github.com/ikizhvatov/dpa-tools-benchmarking
- That was the result in 2019:
  - CPA on 100.000 traces of 512 float32 samples. AES 128 attacked with the Hamming Weight model



→ Time has gone by... there is still no means to compare.

A common ground

- Impossible to compare side-channel tools as most of them are closed
  - Commercial products
  - Internal tools of security labs

- Difficult to provide `scared` performance benchmarks on “reference” side-channel analysis that convinces everybody
  - The notion of “reference” analysis is relative to each analyst
  - Nobody has the same hardware

Solution: Benchmark `scared` on **your hardware** with **your dataset**

Your dataset, your hardware... do it yourself!

Releasing scared benchmark script

- Each lab has its reference dataset
- Each lab has its reference attack

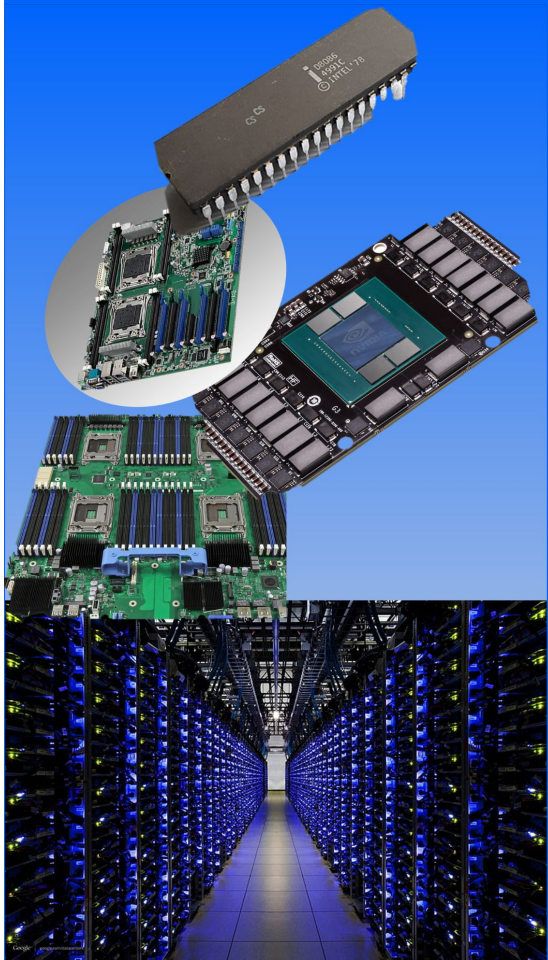
- The trace management library estraces has a new random_reader

- Install scared and estraces with just: `pip install scared estraces`
- Define a random dataset that fits your need
- Define your reference attack with scared

- **Launch it on your machine**

How does it compare with your own tool?!

Our approach



Performances in the industry

~~Plus~~ ~~max~~ ~~ultra~~ ~~extreme~~ → Professional

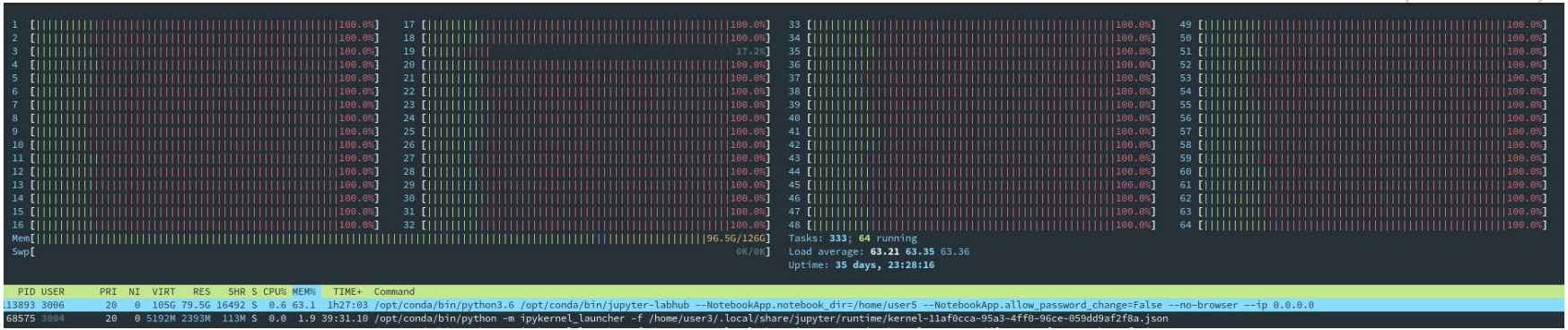
- Corporations and large companies have access to
  - Professional grade CPU
  - Professional grade GPU
  - Datacenters
  - GPU farms

How to get the best from your hardware?

The basics

- Your algorithm must be multithreaded to exploit many cores
- ⚠️ Take care of the memory → 💸
- Use an efficient data format

- Optimize your code, favor efficient operations



How to go further?

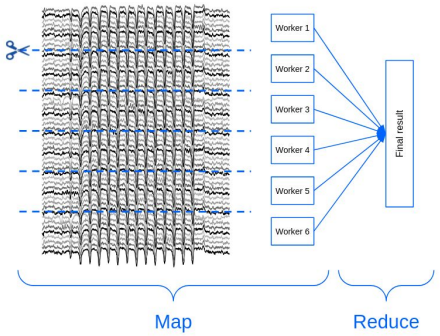
Distributed Computing

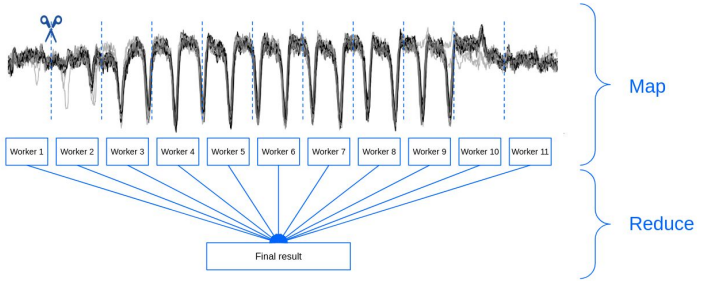
Divide and conquer

- Map / reduce algorithm easy to apply on side-channel analyses
- Also suitable for second-order analyses

- The distribution overhead is negligible for large attacks

Suitable to leverage a computing farm or a supercomputer with many nodes



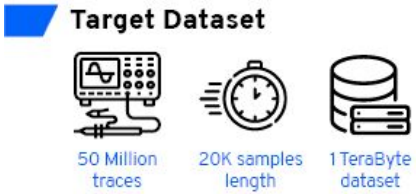


42 nodes ⇒ x42 speedup

GPU Computing

Speed up for first order attack

- 1TB dataset
- CPA on an AES targeting the Hamming weight after the SubBytes operation.
- On a server, with 2x CPU E5-2650 v4 @ 2.40GHz, this attack takes at least 8 hours and 45 minutes.
- For a known key characterization, i.e. without key guesses, the analysis requires at least an hour and a half.



GPU Computing

Speed up for second order attack

- The main bottleneck for GPU computing is the quantity of memory.
- A second order attack on 1400 samples leads to 16.1GB results (with a float32 precision)

→ Which is already too big for most of the consumer GPUs.

- With multiple GPUs in the same machine or within a computing farm, attacks can be performed in parallel.

→ Things that seem unrealistic become achievable: 50M traces, 1500 samples, centered product second order technique required about 100 days of CPU processing.

Fast Computing eXtension

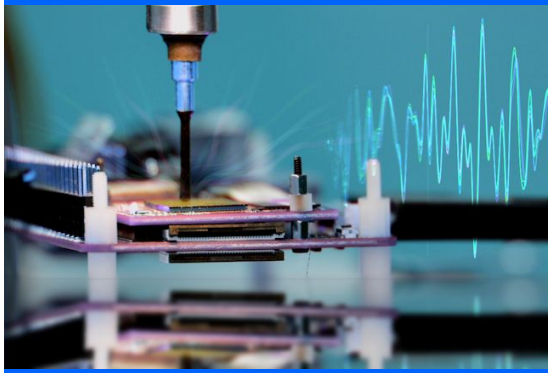
New module for equipped professionals

SCA Fast Computing eXtension module (SCA-FCx) extends the computing capabilities of esDynamic.

- Faster side-channel analyses help strengthening security level assessment
- Increase attack paths coverage in the same time frame
- Leverage both GPU and distributed computing, and even more by combining them

Coming soon...

Conclusion



Performance matters!

- Security level linked/related to a context
  - Your assets, the considered threats, the attack means
- We can always increase the means...

- Check our blog posts
  - https://eshard.com/posts/why-performance-matters
  - https://eshard.com/posts/benchmarking-side-channel-solutions-why-how
- Get `scared`...
- ... benchmark yourself!

ANY QUESTIONS?

Get in touch:

contact@eshard.com

www.eshard.com

/company/eshard

@eshard

eShard

France HQ

Bâtiment GIENAH
11 avenue de Canteranne
33600 Pessac, France

France R&D

7 rue Gaston de Flotte
13012 Marseille, France

Singapore

#04-01 Paya Lebar Quarter
1 Paya Lebar Link
Singapore, 408533

Germany

eShard GmbH,
Beethovenallee 21,
53173 Bonn