SECURE-IC
THE SECURITY SCIENCE COMPANY

Accurate fault detection & classification based on embedded machine learning algorithms

Smart Monitor

Sylvain Guilley, CTO
Tuesday May 29, 2018.

Presentation Outline

General introduction on trends in embedded systems security

Innovative product 1: Digital sensor v2

Innovative product 2: Smart monitor

Conclusions

Presentation Outline

General introduction on trends in embedded systems security

Innovative product 1: Digital sensor v2

Innovative product 2: Smart monitor

Conclusions

It is *machine* against *machine*

Attackers get smart:

- **Automatic** generation of specialized fault attacks
- **Machine learning** assisted pattern recognition in traces
- **Deep learning** in side-channel analysis

In response, protections must be smart

- Rich information . . . . **big data**
- Clever analysis . . . . **artificial intelligence**

Similar situation in IT security

ARTIFICIAL INTELLIGENCE FOR CYBER-SECURITY

INTRODUCTION

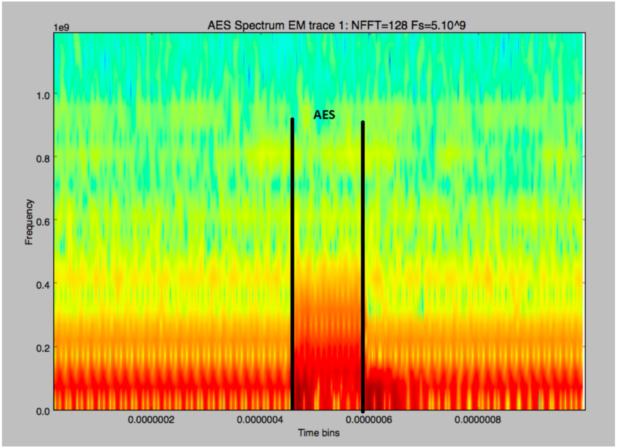
- Cyberspace: Are humans thrown on scrapheap?

DARPA's Cyber Grand Challenge: World's first automated network defence tournament

Source: http://archive.darpa.mil/cybergrandchallenge/.

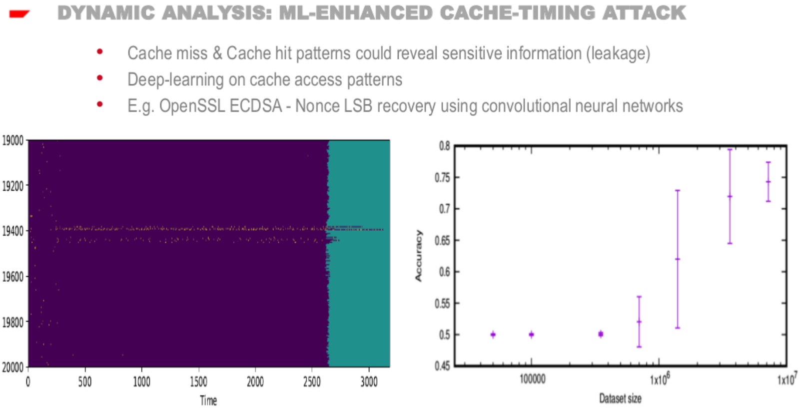
Noisy EM analysis

Side-channel analysis and machine learning: A practical perspective (IJCNN 2017 [PHJ+17])



Microarchitectural Analysis

Cachyzr (tool in CTZ)



DYNAMIC ANALYSIS: ML-ENHANCED CACHE-TIMING ATTACK

- Cache miss & Cache hit patterns could reveal sensitive information (leakage)
- Deep-learning on cache access patterns
- E.g. OpenSSL ECDSA - Nonce LSB recovery using convolutional neural networks

How we handle smart attacks?

Security by design

- Formal models of protection rationale
- Validation by VTZ tool (Virtualyzr [DGN+17]), throughout the design flow
- Evaluation in rich platform

Machine learning (ML)

- Sensors fusion
- Embedded ML
- Nice byproduct: allows to tolerate noise, e.g., technology dispersion

Presentation Outline

General introduction on trends in embedded systems security

Innovative product 1: Digital sensor v2

Innovative product 2: Smart monitor

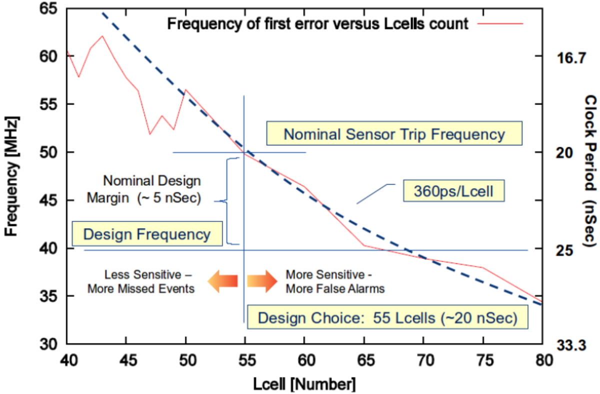
Conclusions

Digital sensor V2 [GP17]

New features:

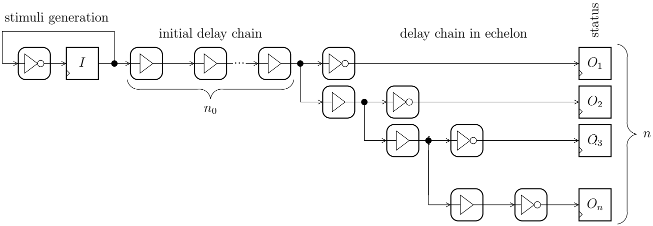
- Centered status: can see as well speed decrease as speed increase
- More fine: delta temperature/bit, etc.
- History (internal oscilloscope)
- Spatial efficiency (= smart monitor)

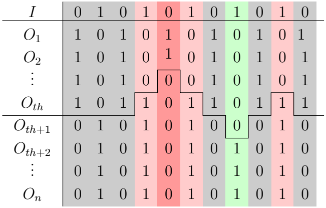
New feature: finer resolution (illustration)



Objective: by proper selection of buffers, make the slope more steep.

New features: history (illustration)





I	0	1	0	1	0	1	0	1	0	1	0
O_1	1	0	1	0	1	0	1	0	1	0	1
O_2	1	0	1	0	1	0	1	0	1	0	1
⋮	1	0	1	0	0	0	1	0	1	0	1
O_{th}	1	0	1	1	0	1	1	0	1	1	1
O_{th+1}	0	1	0	1	0	1	0	0	0	1	0
O_{th+2}	0	1	0	1	0	1	0	1	0	1	0
⋮	0	1	0	1	0	1	0	1	0	1	0
O_n	0	1	0	1	0	1	0	1	0	1	0

A unique signature:
Fig. 14, page 189, of [SBGD11]

The Digital Sensor V2: new usages

- As always: **fully digital**, i.e., using precharacterized standard cells from the PDK
  - Can replace analog sensors (see below)
  - Less costly than analog sensors for small technological nodes (7 nm, 5 nm, etc.)

- **One *single* instance** is sufficient for:
  - low clock frequency: have n_0 set to a large value
  - high clock frequency: have n_0 set to 0
  - low / high temperature: increase n / decrease n_0 (*see slide 19*)
  - better voltage (higher than nominal): increase n beyond 32 bits (*see slide 20*)
- ***Multiple* instances** are needed for local attacks, such as:
  - EM pulse injection attack
  - laser injection attack
  - Number and location of sensors: spread by supply net of P/G network, close to sensitive registers

Experimental results

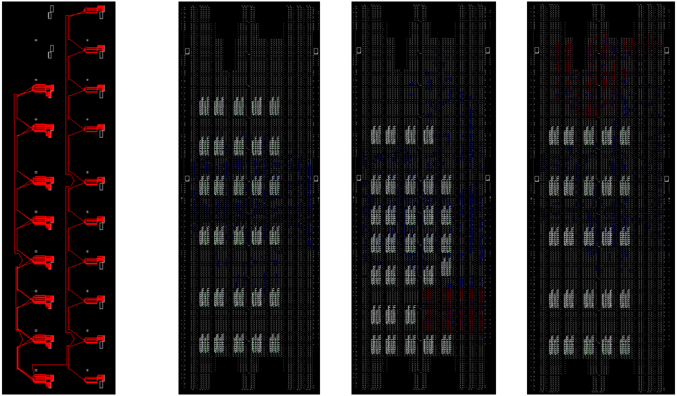
Dimensioning on SAKURA G, SPARTAN 6 FPGA:

- FIFO depth: **40**
- Status: **16** to **32** — chain length: n_0=**70** + **16-32**
- Number of instances: ≈ **50**
- Sensitivity (see next slides):
  - **0.04 bit/°C**
  - **0.18 bit/mV**
- Without and with crypto running in parallel (AES core)

Big data: **64000** bits ready to be analyzed at each clock cycle.

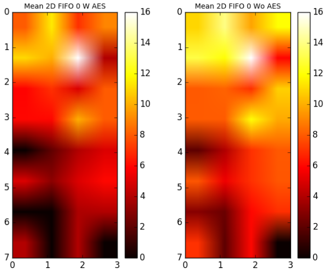
Layouts

Various experimental setups

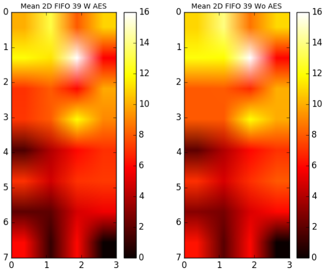


1 60 64 50

Natural variability



Time sample #0

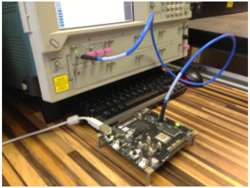


Time sample #39

- In a threshold-based approach, the threshold is not easy to set
- Depends on the location, depends on the internal activity

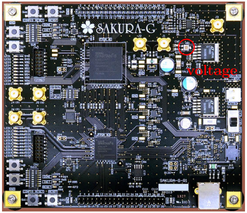
Characterization & attack means (LBZ)

Clock



Temperature

Power



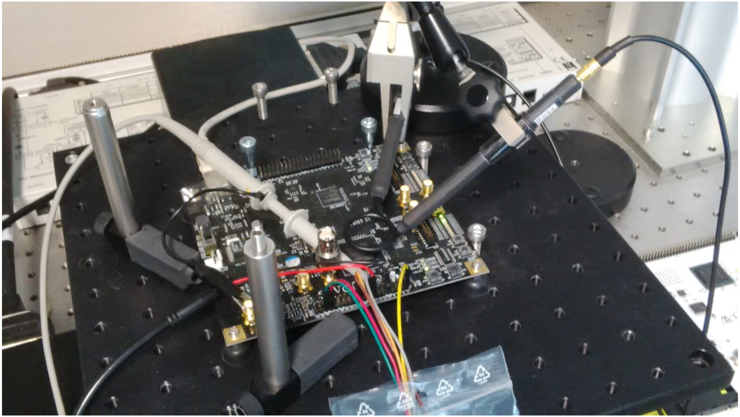
EM field

Experiments at Rennes SSF

Security Science Factory

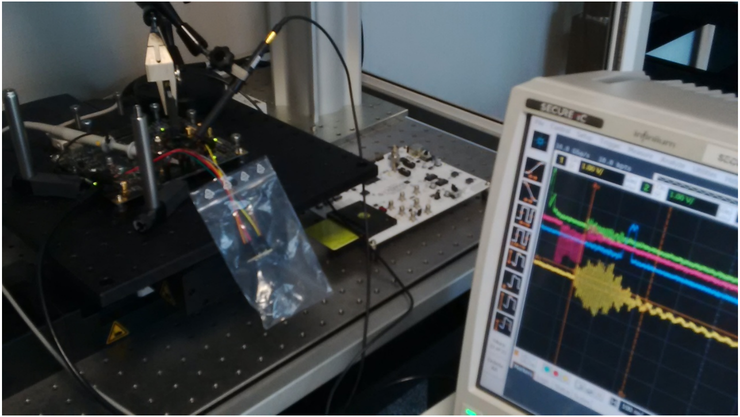
Experiments at Rennes SSF

Security Science Factory



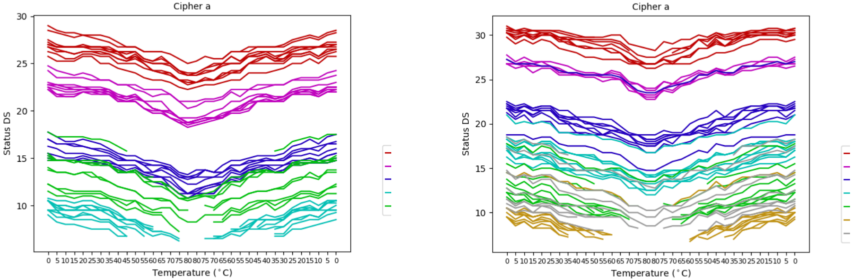
Experiments at Rennes SSF

Security Science Factory



Variability is by techno dispersion, not P&R

Automatic routing | Manual routing

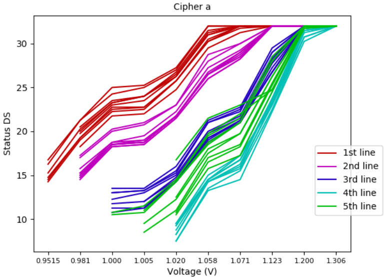


Characterization: **0.04 bit/°C**

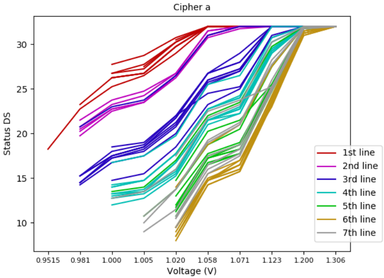
- Saturation at ≤ 32 can be leveraged by increasing n
- Saturation at ≥ 0 can be leveraged by decreasing n_0

Variability is by techno dispersion, not P&R

Automatic routing



Manual routing



Characterization: **0.18 bit/mV**

- Saturation at ≤ 32 can be leveraged by increasing n

Innovative product 1: Digital sensor v2

Summary

Security feature innovation ("*big data*" allowing "*analytics*"):

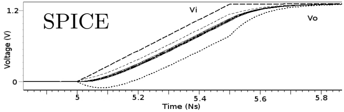
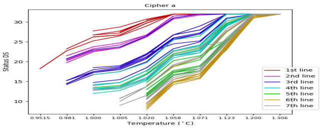
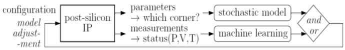
- Captures complete waveforms
- Monitors when conditions get worse but also when they unexpectedly get more favorable
- Increased environmental condition sampling resolution

Demonstration / proof of maturity:

- Show-case of an FPGA board with a matrix of DS V2
- Illustration of sensitivity even to internal activity change
- Illustration of sensitivity when external conditions change

Robust design-for-security and -for-yield approach

DfS and DfY for the DS V2

1. Mathematics stochastic model	$$T = n \times C(P,V,T) \times T_0$$ $$C(P,V,T) = \alpha P + \beta V + \gamma T$$
2. Simulation parameters characterization	
3. Emulation parameters validation	
4. Post-silicon release *in situ* configuration	

Presentation Outline

General introduction on trends in embedded systems security

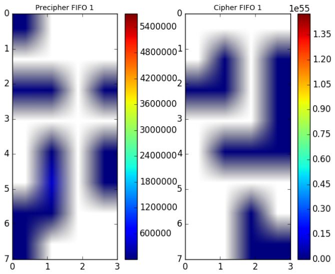
Innovative product 1: Digital sensor v2

Innovative product 2: Smart monitor

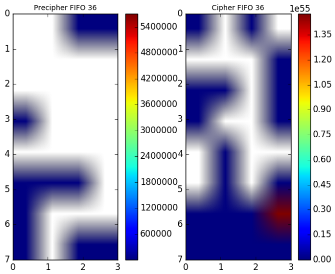
Conclusions

Distinguishing internal activity, with T-Test [Wel47]

Time sample #1

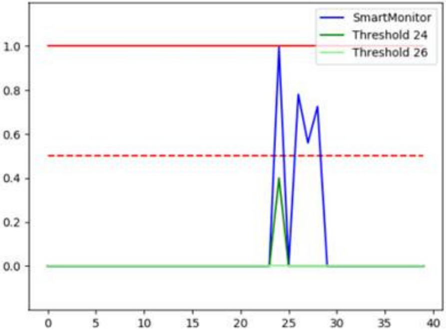


Time sample #36 (EM inj)



- Normalized difference between *with* and *without* EM injection
- Those figures require *multiple* measures to be computed

Distinguishing internal activity, with ML [Vap98]

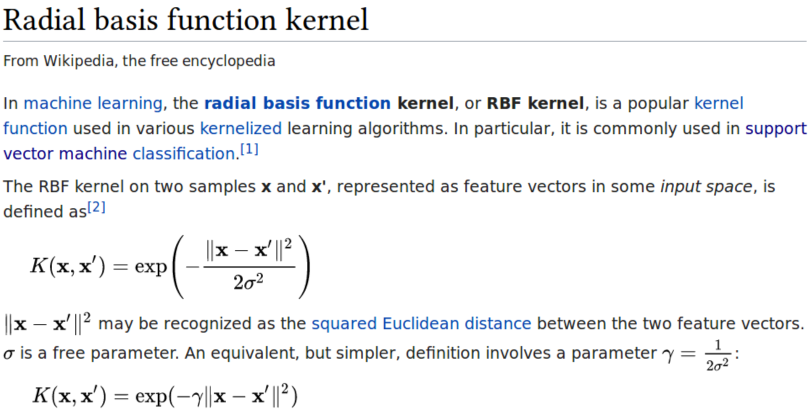


Description of the results

- 100% (±1) detection by Smart-Monitor
- 40% (±1) detection by one DS V2
- Others are completely blind

- **Blue:** 32 DS V2, using 3 samples, instantaneous reaction, and accurate damping
- **Green:** threshold at each DS V2, equal to: normalized mean(with EM) - mean(w/o EM).

Radial Basis Function (RBF) kernel



Radial basis function kernel

From Wikipedia, the free encyclopedia

In machine learning, the **radial basis function kernel**, or **RBF kernel**, is a popular kernel function used in various kernelized learning algorithms. In particular, it is commonly used in support vector machine classification.[1]

The RBF kernel on two samples **x** and **x'**, represented as feature vectors in some *input space*, is defined as[2]

$$K(\mathbf{x},\mathbf{x'}) = \exp\left(-\frac{\|\mathbf{x}-\mathbf{x'}\|^2}{2\sigma^2}\right)$$

$\|\mathbf{x}-\mathbf{x'}\|^2$ may be recognized as the squared Euclidean distance between the two feature vectors. σ is a free parameter. An equivalent, but simpler, definition involves a parameter $\gamma = \frac{1}{2\sigma^2}$:

$$K(\mathbf{x},\mathbf{x'}) = \exp(-\gamma\|\mathbf{x}-\mathbf{x'}\|^2)$$

Our best fit is for $\gamma \approx \frac{1}{4}$.

Innovative product 2: Smart monitor

Summary

Security feature innovation:

- Can be fed by DS V2, but also other sensors, incl. CyberEU
- Robust benign / malicious observation classification

Demonstration / proof of maturity:

- Detection before the AES is faulted
- Model robustness w.r.t. device architecture

Presentation Outline

General introduction on trends in embedded systems security

Innovative product 1: Digital sensor v2

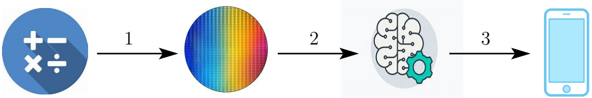
Innovative product 2: Smart monitor

Conclusions

Flow for Smart-Monitor management of chip fabrication uncertainties

Mathematics: for the modelization of delays
Simulation: for validation of the model
Emulation: for cross validation of simulations with real data
⟹ dimensioned architecture, RTL

Deployment



Netlist, GDSII
⟹ **Tapeout**
⟹ **Samples back**

Characterization of the engineering samples:
- nominal *vs* EM
- nominal *vs* underfeed, overclock, etc.

Off-chip learning phase:
⟹ support vectors (SVs) generated by SVM algorithm

Programmation of SVs in mass production:
⟹ countermeasure is armed

Bibliographical references I

[DGN+17] Jean-Luc Danger, Sylvain Guilley, Philippe Nguyen, Robert Nguyen, and Youssef Souissi.
Analyzing security breaches of countermeasures throughout the refinement process in hardware design flow.
In David Atienza and Giorgio Di Natale, editors, *Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017*, pages 1129–1134. IEEE, 2017.

[GP17] Sylvain Guilley and Thibault Porteboeuf.
Dispositif et procédé pour étalonner un capteur numérique, May 24 2017.
Patent EP2960665B1.

Bibliographical references II

[PHJ+17] Stjepan Picek, Annelie Heuser, Alan Jovic, Simone A. Ludwig, Sylvain Guilley, Domagoj Jakobovic, and Nele Mentens.
Side-channel analysis and machine learning: A practical perspective.
In *2017 International Joint Conference on Neural Networks, IJCNN 2017, Anchorage, AK, USA, May 14-19, 2017*, pages 4095–4102. IEEE, 2017.

[SBGD11] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger.
Security evaluation of application-specific integrated circuits and field programmable gate arrays against setup time violation attacks.
IET Information Security, 5(4):181–190, December 2011.
DOI: 10.1049/iet-ifs.2010.0238.

Bibliographical references III

[Vap98] Vladimir N. Vapnik.
Statistical Learning Theory.
Wiley-Interscience, September 1998.
ISBN: 978-0-471-03003-4.

[Wel47] B.L. Welch.
The Generalization of “Student’s” Problem when Several Different Population Variances are Involved.
Biometrika, 34(1/2):28, January 1947.