SoC, why should we care about Fault Injection Attacks ?

Guillaume BOUFFARD (guillaume.bouffard@ssi.gouv.fr) David EL-BAZE (david.elbaze@ssi.gouv.fr)

with the help of Thomas TROUCHKINE

Agence nationale de la sécurité des systèmes d'information

Journée JAIF – PARIS – 29 Mai 2018

ANSSI? Késako?

ANSSI (French Network and Information Security Agency) has InfoSec (and no Intelligence) missions:

- detect and early react to cyber attacks,
- prevent threats by supporting the development of trusted products and services,
- provide reliable advice and support and
- communicate on information security threats and the related means of protection.

These missions concern:

- governmental entities,
- companies and
- the general public.

From the SE to the SoC

- Sensitive assets are in and computed on the Secure Element (SE).
- Secure Element are designed to be tamper-resistant against physical and software attacks.
- System on Chips (SoC) are everywhere:
  - Automotive
  - Smartphone
  - IoT
- Secure Element are limited resources devices.
- For sensitive operations where more resources are required, SoCs are used.

From the SE to the SoC

- Sensitive assets are in and computed on the Secure Element (SE).
- Secure Element are designed to be tamper-resistant against physical and software attacks.
- System on Chips (SoC) are everywhere:
  - Automotive
  - Smartphone
  - IoT
- Secure Element are limited resources devices.
- For sensitive operations where more resources are required, SoCs are used.

What about security of the SoC?

What's a System On Chip (SoC) ?

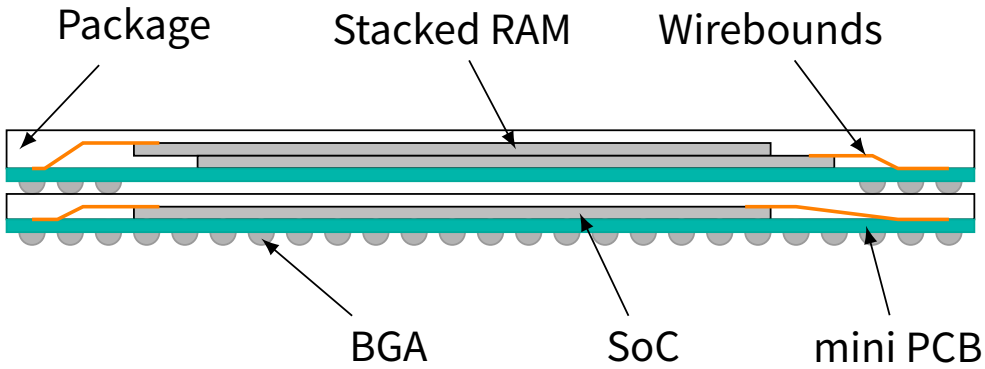
SoC

- μControllers
- μProcessors
- DSPs
- Memories
- Timing sources
- Timers
- I/O
- ADCs/DACs
- Voltage regulators/PMICs
- Communication BUS
- FPGA

Why ?

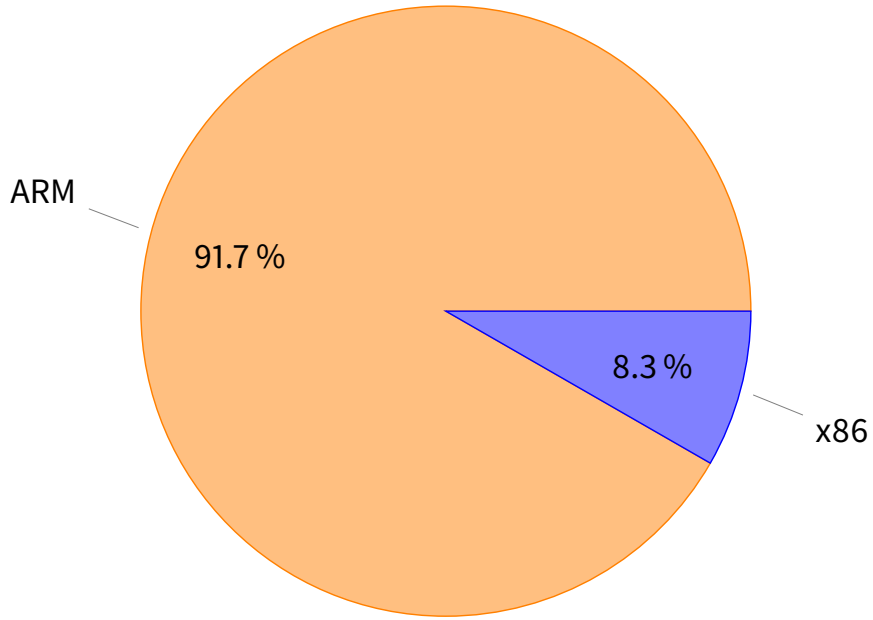
- Less space needed
- Low power consumption

No data storage $\rightarrow$ Package On Package



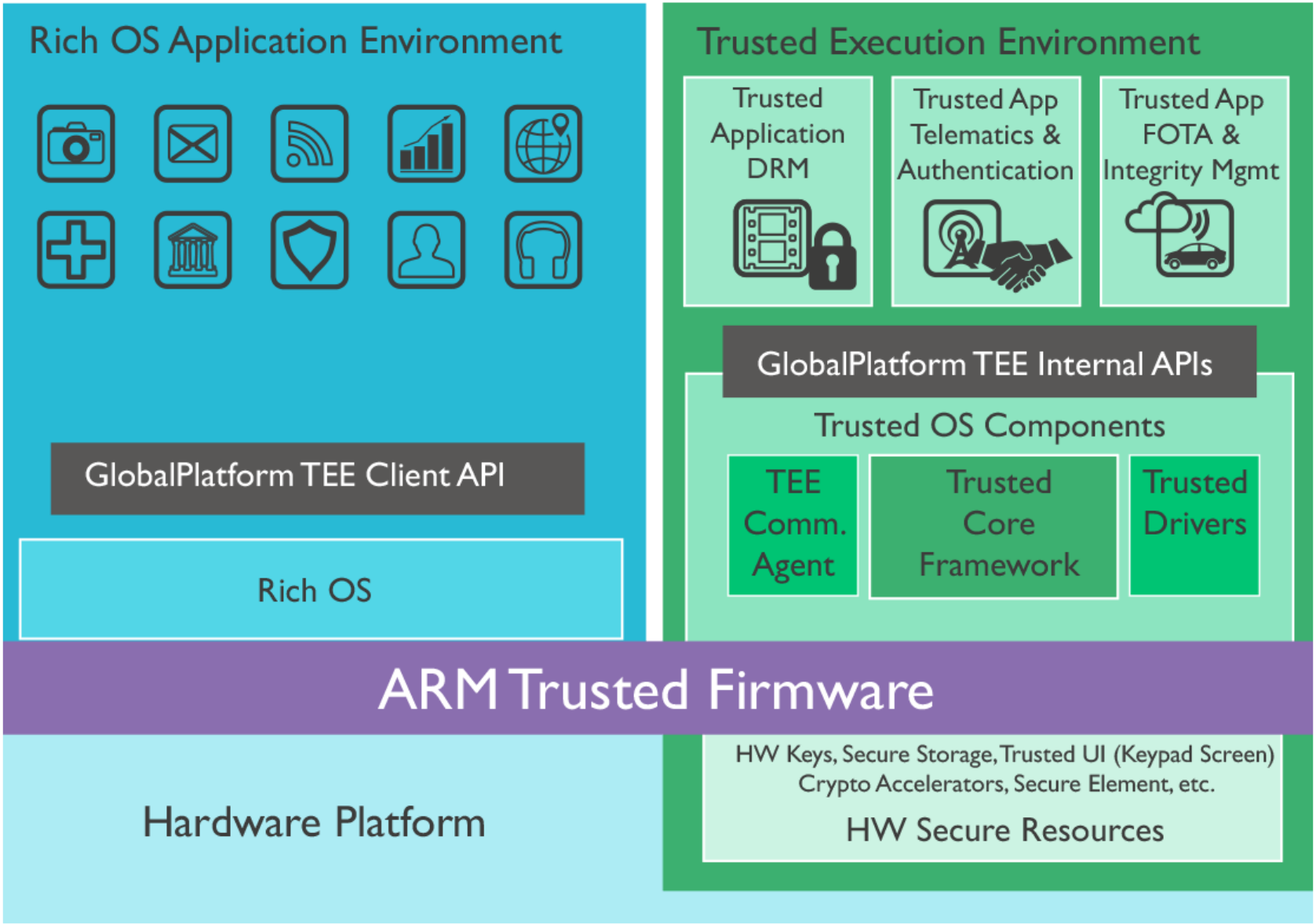
SoC Manufacturers

- **MSM** & **APQ** (Snapdragon) by Qualcomm
- **Exynos** by Samsung
- **MT & Helio** by MediaTek
- **Apple A** by Apple
- **Tegra** by Nvidia
- **Atom** by Intel (x86)
- **RK** by Fuzhou RockChip
- **Kirin** by Hisilicon
- **OMAP** by Texas Instrument
- **AML** by Amlogic
- **G-series** by AMD
- **Allwinner A** by Allwinner



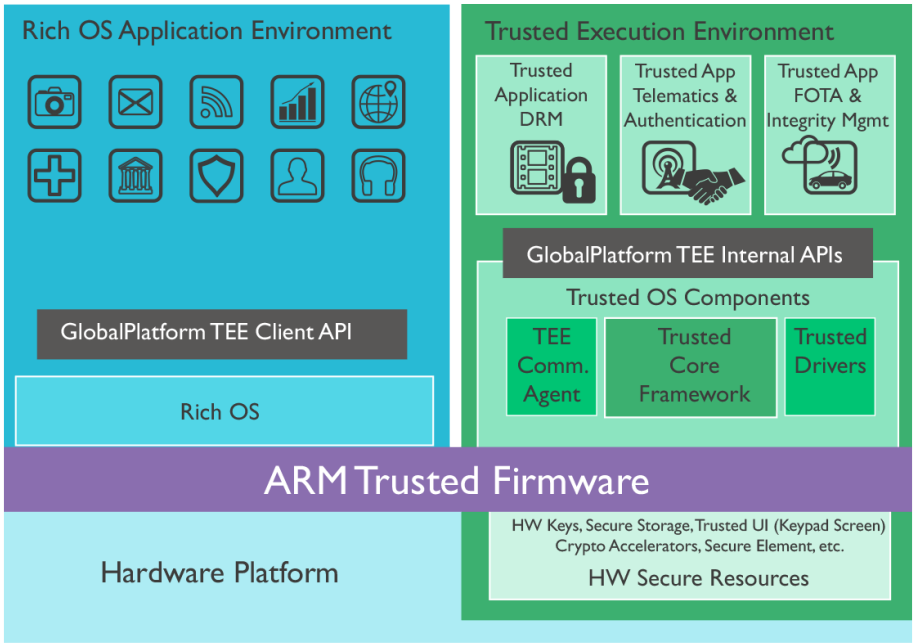
SoC architectures distribution

Software-security oriented component



(Source: `https://developer.arm.com/technologies/trustzone`)

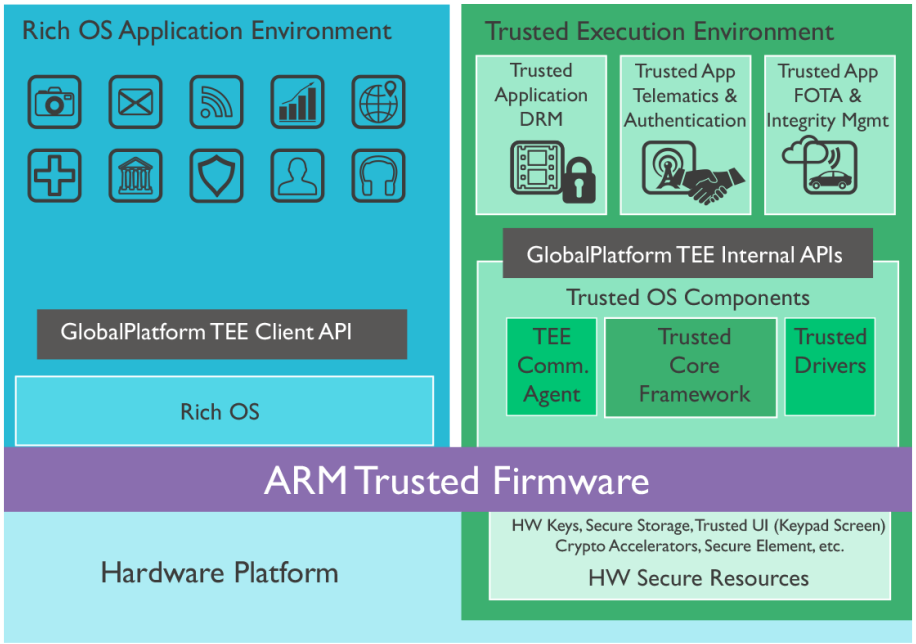
Software Impacts



(Source: `https://developer.arm.com/technologies/trustzone`)

- The secure enclave runs trusted apps

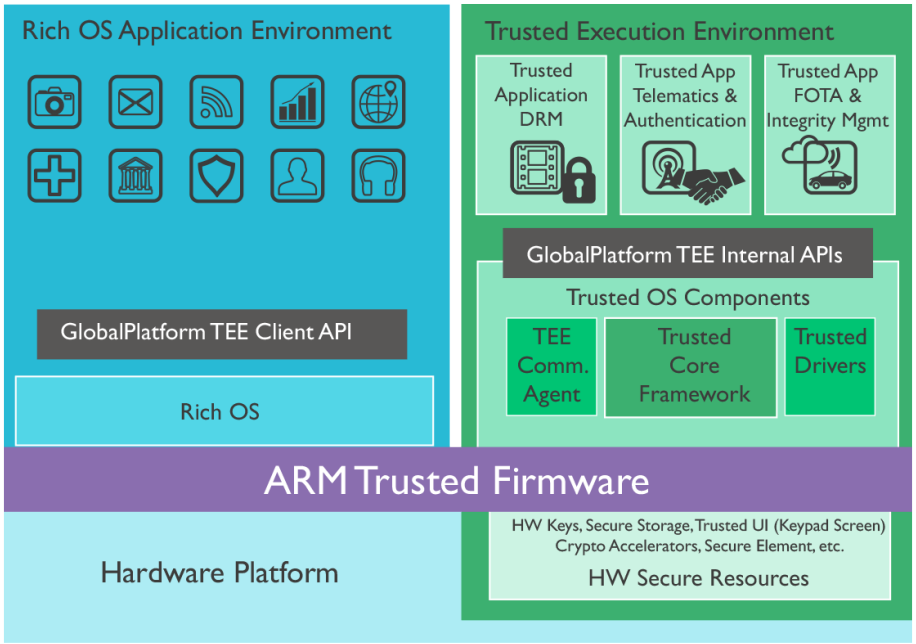
Software Impacts



(Source: `https://developer.arm.com/technologies/trustzone`)

- The secure enclave runs trusted apps
- Rich OS is complex and might have vulnerabilities

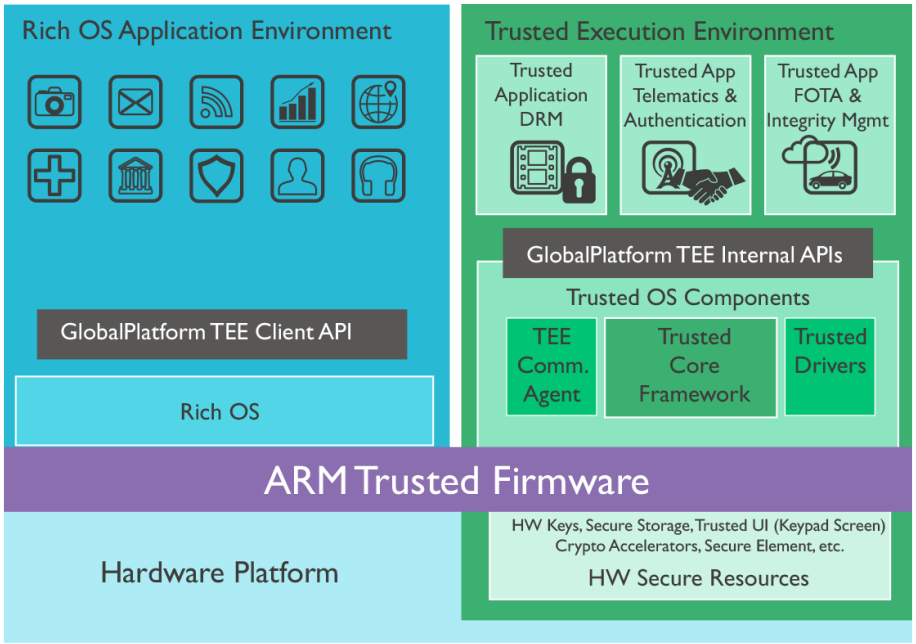
Software Impacts



(Source: `https://developer.arm.com/technologies/trustzone`)

- The secure enclave runs trusted apps
- Rich OS is complex and might have vulnerabilities
  - Rich OS integrity is ensured by the secure boot step.

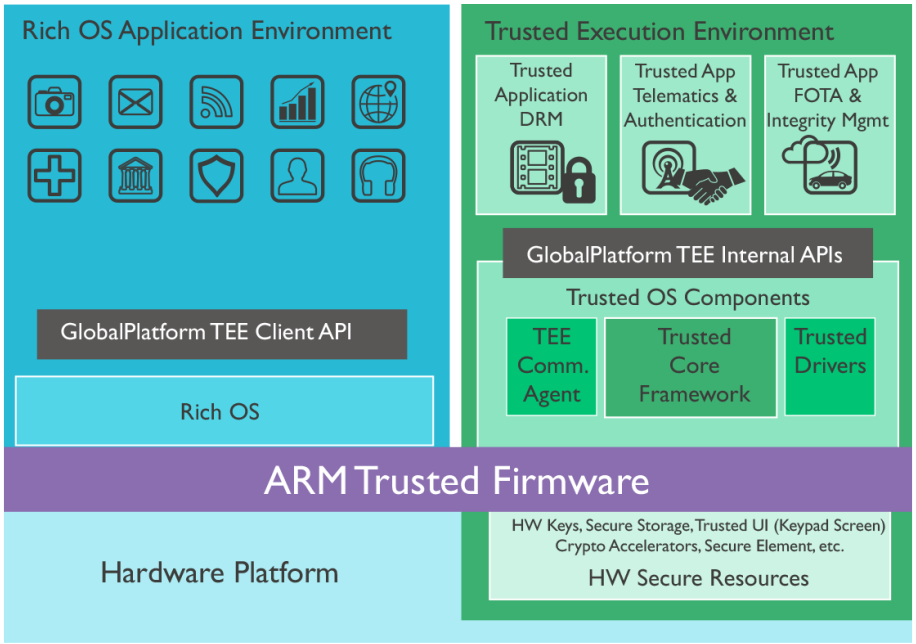
Software Impacts



(Source: `https://developer.arm.com/technologies/trustzone`)

- The secure enclave runs trusted apps
- Rich OS is complex and might have vulnerabilities
  - Rich OS integrity is ensured by the secure boot step.
  - Rich OS might be jailbreaked (like iOS and Android).

Software Impacts



(Source: `https://developer.arm.com/technologies/trustzone`)

- The secure enclave runs trusted apps
- Rich OS is complex and might have vulnerabilities
  - Rich OS integrity is ensured by the secure boot step.
  - Rich OS might be jailbreaked (like iOS and Android).
- Rich OS might break the security of secure enclave area.

State-of-the-art physical attacks

Injection medium	Physical target	Software target	Software security
Software	RAM	Virtual to physical translation table	Memory partitioning
Glitch voltage	Clock	Key	Cryptography
Laser	Register	Instruction	Secure boot
EM	Bus	Return value	Execution flow integry
BBI	Cache	Program counter	
UV	MMU	User rights	
	Pipeline		

State-of-the-art physical attacks

Injection medium	Physical target	Software target	Software security
Software	RAM	Virtual to physical translation table	Memory partitioning
Glitch voltage	Clock	Key	Cryptography
Laser	Register	Instruction	Secure boot
EM	Bus	Return value	Execution flow integry
BBI	Cache	Program counter	
UV	MMU	User rights	
	Pipeline		

Project Zero attack/Drammer (2015 - 2016) [Vee+16]

State-of-the-art physical attacks

Injection medium	Physical target	Software target	Software security
Software	RAM	Virtual to physical translation table	Memory partitioning
Glitch voltage	Clock	Key	Cryptography
Laser	Register	Instruction	Secure boot
EM	Bus	Return value	Execution flow integry
BBI	Cache	Program counter	
UV	MMU	User rights	
	Pipeline		

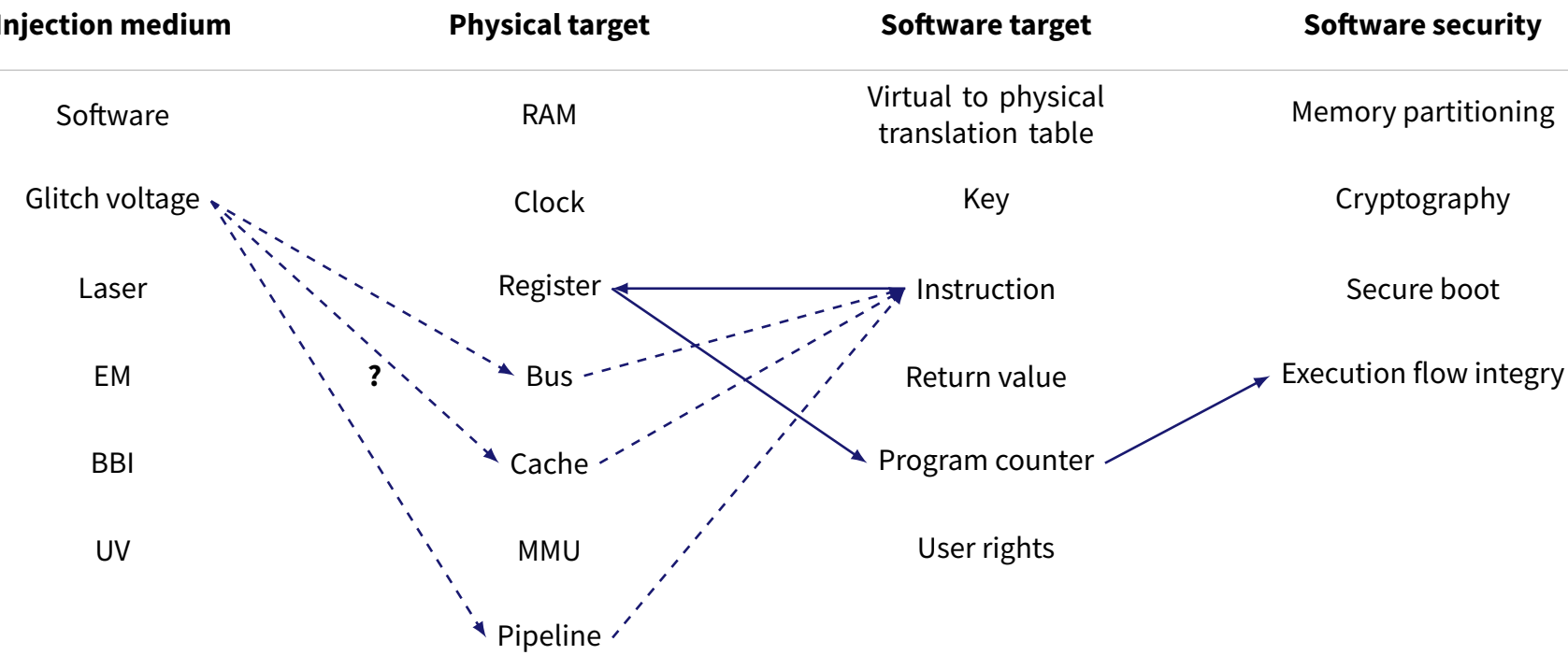
Project Zero NaCl/Rowhammer on TrustZone (2015) [Car17]

State-of-the-art physical attacks

Injection medium	Physical target	Software target	Software security
Software	RAM	Virtual to physical translation table	Memory partitioning
Glitch voltage	Clock	Key	Cryptography
Laser	Register	Instruction	Secure boot
EM	Bus	Return value	Execution flow integry
BBI	Cache	Program counter	
UV	MMU	User rights	
	Pipeline		

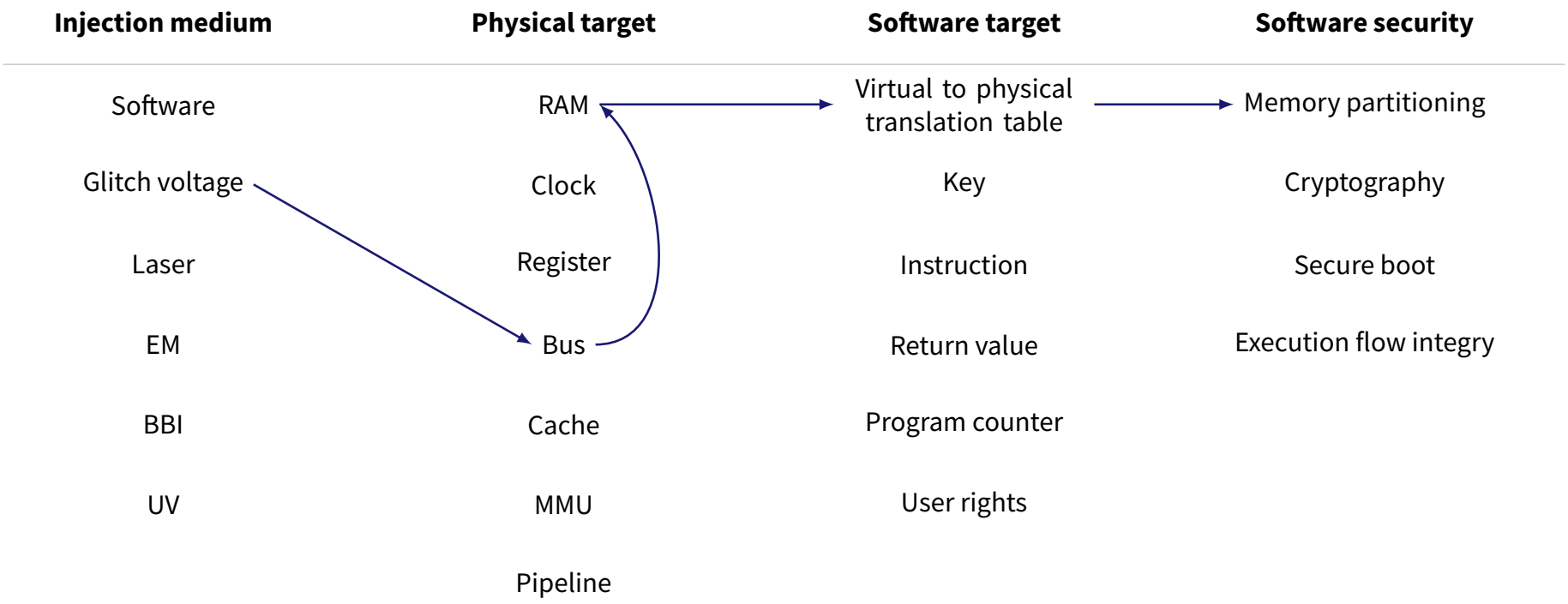
ClkScrew (2017) [TSS17]

State-of-the-art physical attacks



Controlling PC on ARM (2016) [TSW16]

State-of-the-art physical attacks



Attack on PS3

State-of-the-art physical attacks

Injection medium	Physical target	Software target	Software security
Software	RAM	Virtual to physical translation table	Memory partitioning
Glitch voltage	Clock	Key	Cryptography
Laser	Register	Instruction	Secure boot
EM	Bus	Return value	Execution flow integry
BBI	Cache	Program counter	
UV	MMU	User rights	
	Pipeline		

Attack on Xbox 360 (2015) [Bla15]

State-of-the-art physical attacks

Injection medium	Physical target	Software target	Software security
Software	RAM	Virtual to physical translation table	Memory partitioning
Glitch voltage	Clock	Key	Cryptography
Laser	Register	Instruction	Secure boot
EM	Bus	Return value	Execution flow integry
BBI	Cache	Program counter	
UV	MMU	User rights	
	Pipeline		

Laser induced fault on smartphone (2017) [Vas+17]

Hardware Impacts

Cons points for security :

- Many new components inside the SoC can be targeted :
  - Crypto accelerators,
  - TRNG,
  - Memories,
  - Schedulers,
  - Timers,
  - USB controllers,
  - Radio controllers...
- Substrate thickness

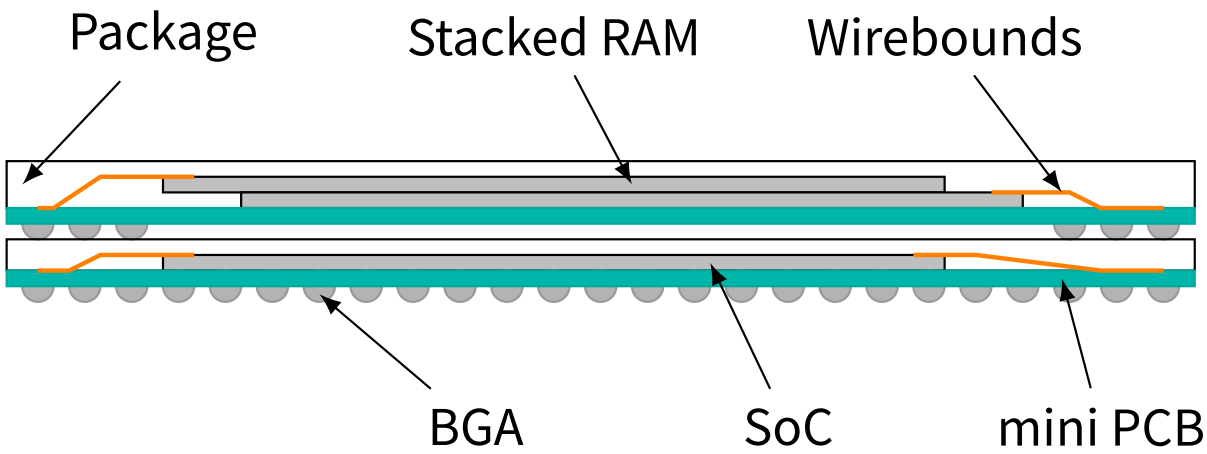
Crypto accelerators may be protected against FI, but what about the rest ?

Security still have to be a global thing !

Hardware Impacts

Pro points for security :

- **big chips** with lot of embedded components $\rightarrow$ not easy to scan (and to find PoI) with classic EM, Laser or BBI attacks,
- **stacked chips** $\rightarrow$ complicates the use of conventional ways of injecting faults (Laser two-photons technology ?),
- **High operating frequency** $\rightarrow$ not easy to sync an attack.



Mixed Attacks

Side Channel

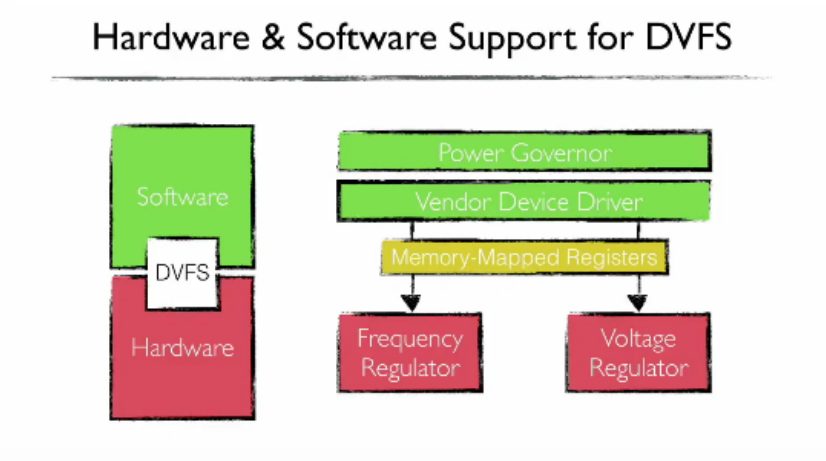
- Cache Attacks,
- Spectre 1 & 2,
- Spectre 3 (Meltdown),
- Spectre 4 (Speculative Store Bypass).

Fault Injection

- Clkscrew
- Rowhammer, Nethammer
- ...

ClkScrew

Clkscrew



- DVFS means Dynamic Voltage and Frequency Scaling.
- It allows a software to change power and frequency parameters.
- With a corrupted software, you can put the chip into operating borders.

To Conclude

- SoCs are widely deployed.
- SoCs are more and more used to compute sensitive operations.
- SoCs are complex devices with a large attack area.
- Can the SoC security level be proved?
- Thomas Trouchkine's PhD thesis on SoC security against physical attacks in progress.

Questions?

Guillaume Bouffard
<guillaume.bouffard@ssi.gouv.fr>

David El Baze
<david.elbaze@ssi.gouv.fr>

References

[Bla15] BlackHat. “XBOX 360 Glitching on fault attack”. Nov. 2015.

[Car17] Pierre Carru. “Attack TrustZone with Rowhammer”. In: *GreHack* (2017).

[TSS17] Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo. *CLKSCREW: Exposing the perils of security-oblivious energy management*. Tech. rep. Columbia University, 2017.

[TSW16] Niek Timmers, Albert Spruyt, and Marc Witteman. “Controlling PC on ARM Using Fault Injection”. In: *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016*. IEEE Computer Society, 2016, pp. 25–35. DOI: 10.1109/FDTC.2016.18.

[Vas+17] Aurélien Vasselle et al. “Laser-induced fault injection on smartphone bypassing the secure boot”. In: (Sept. 2017).

References (cont.)

[Vee+16] Victor van der Veen et al. “Drammer: Deterministic Rowhammer Attacks on Mobile Platforms”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. Ed. by Edgar R. Weippl et al. ACM, 2016, pp. 1675–1689. DOI: 10.1145/2976749.2978406.