
# Fault attacks on System On Chip

**Thomas TROUCHKINE** Guillaume BOUFFARD Jessy CLÉDIÈRE

ANSSI - Hardware Security Labs

May 22, 2018

# Context

Smartcard

Mobile device

**Same services, different securities**

# Context

**Based on a Secure Element**

- Simple SoC
- Designed for security
- Evaluated

**Based on a Computer on Chip**

- Complex SoC
- Designed for performance
- Adding TEE[1] for software security

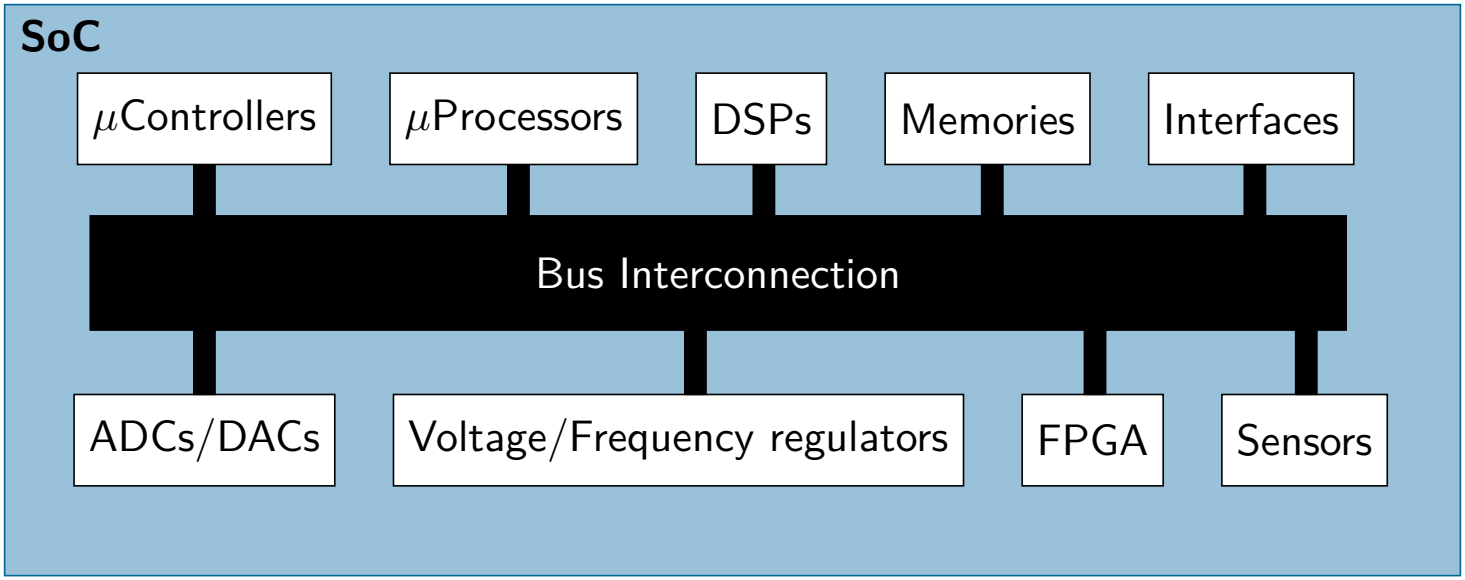
[1] **Trusted Environment Execution**

# Hardware attacks ?

Fault attacks

- Laser/EM injection
- Clock glitch
- Voltage glitch
- Rowhammer
- Heating
- Body biasing

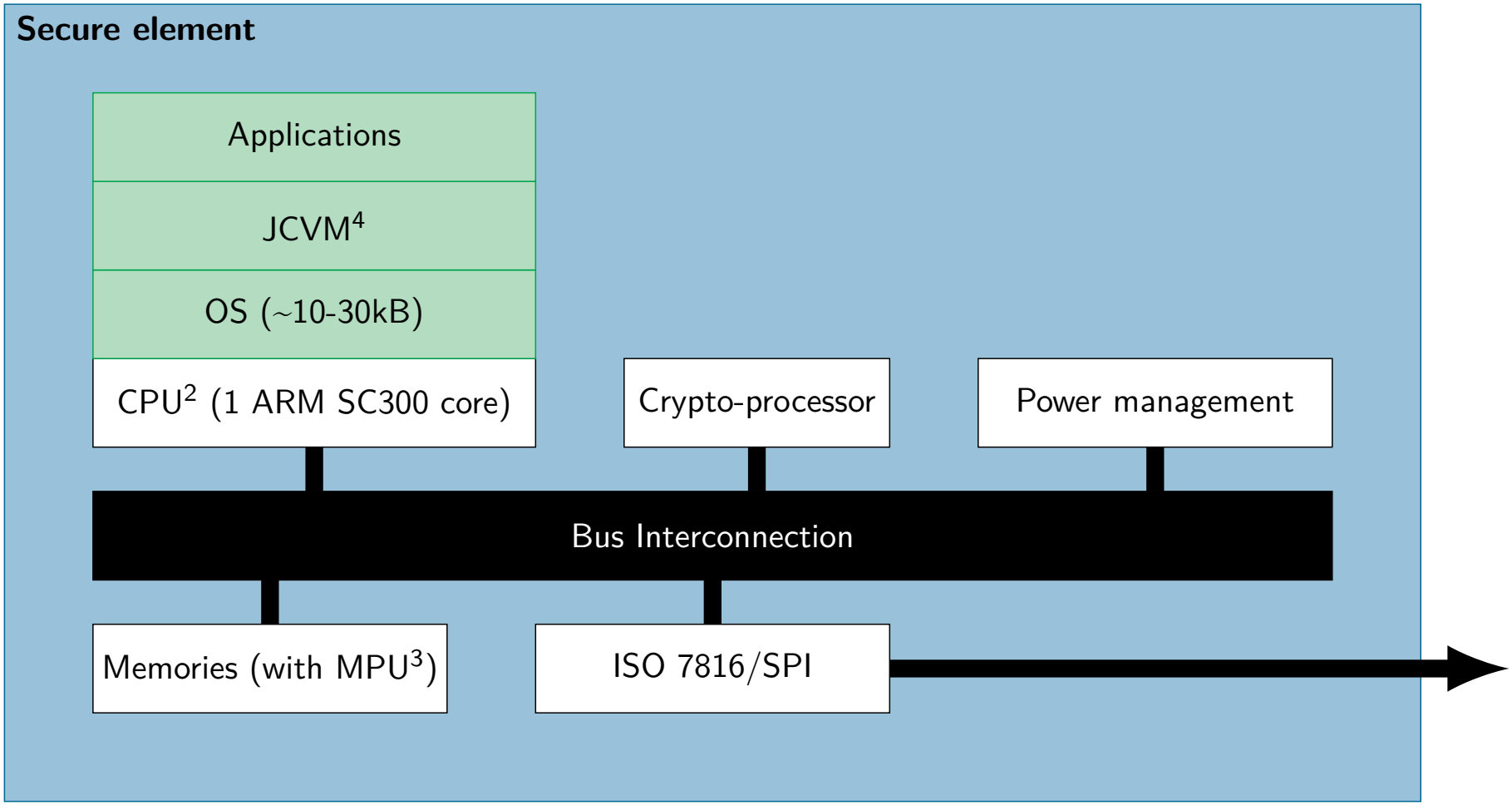
# What is a System on Chip ?





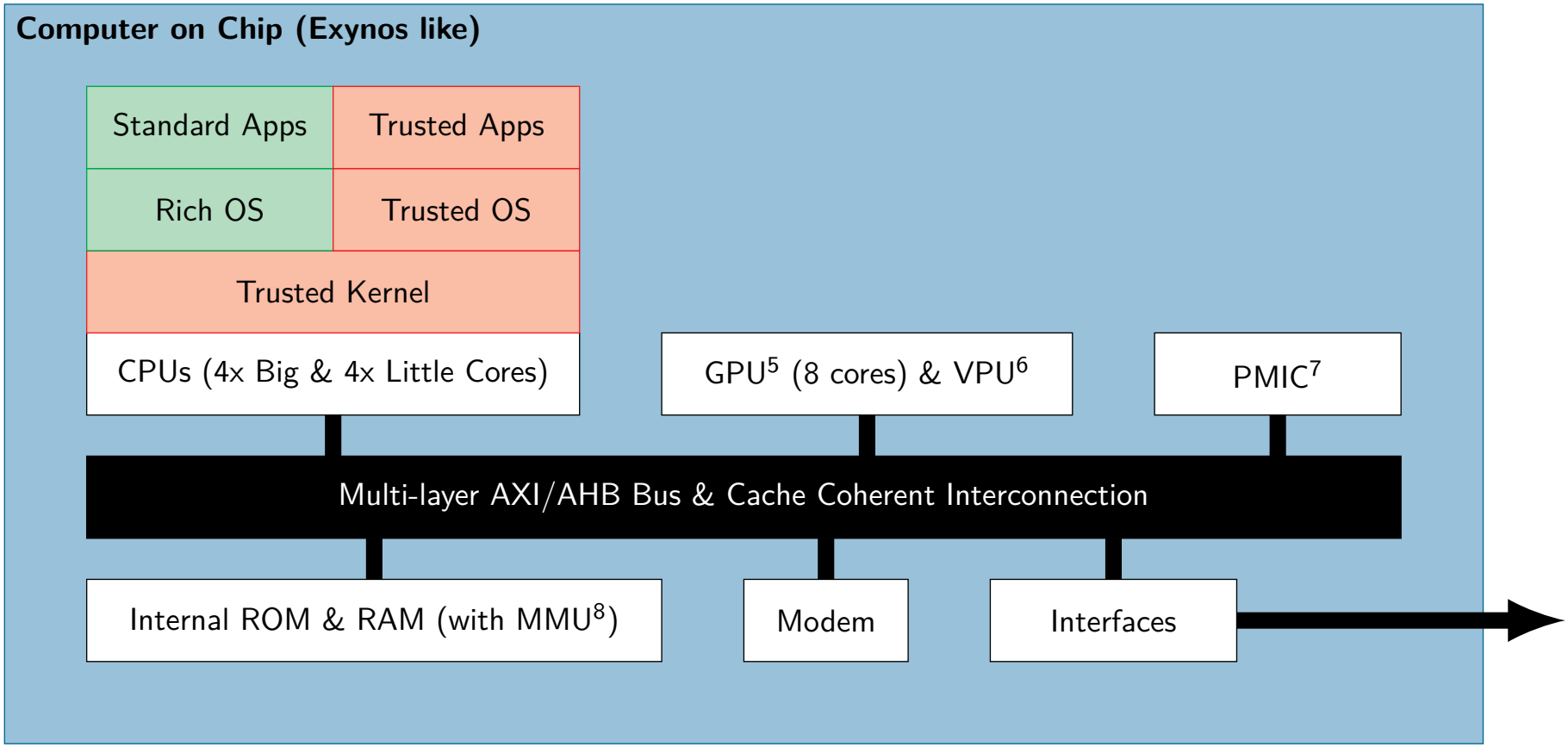
- Integrate all components on the same chips
- Reduce power consumption
- Reduce chip size

# What is a Secure Element ?



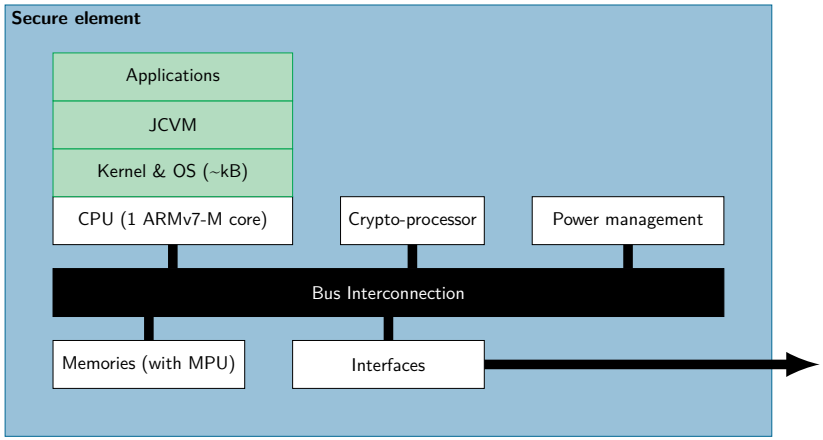

[2] **Central Processing Unit**
[3] **Memory Protection Unit**
[4] **Java Card Virtual Machine**

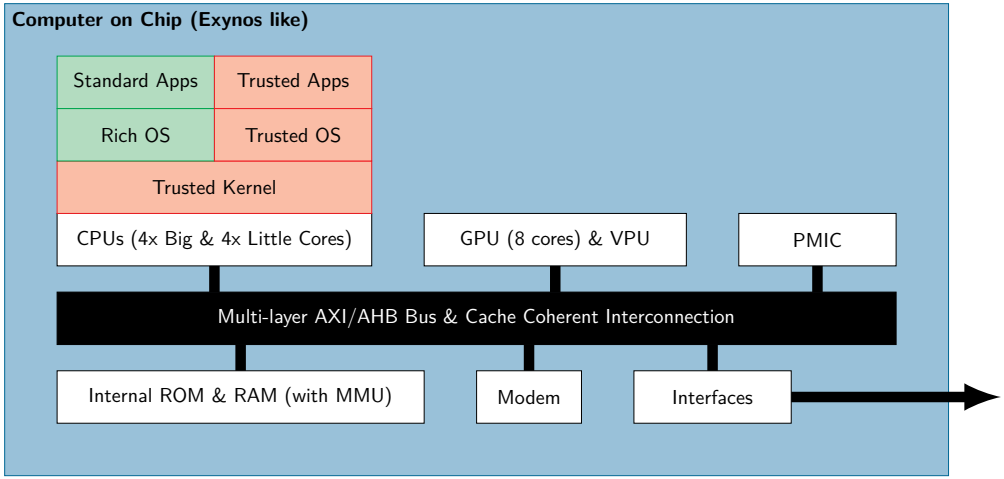
# What is a Computer on Chip ?




[5] **Graphical Processing Unit**
[6] **Video Processing Unit**
[7] **Power Management Integrated Circuit**
[8] **Memory Management Unit**

# Secure element vs Computer on Chip



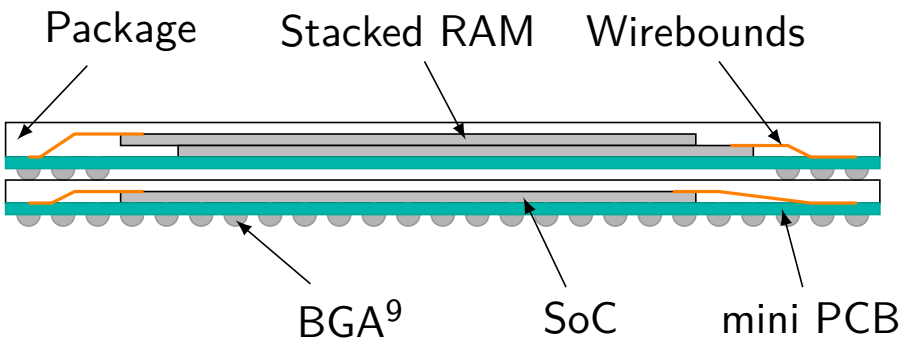




- Run at 4 to 60MHz
- Not multithreaded
- Fine engraving $>$ 40 nm
- Constant Voltage & Frequency
- Trusted hardware & Trusted apps only
- Hardware mitigations

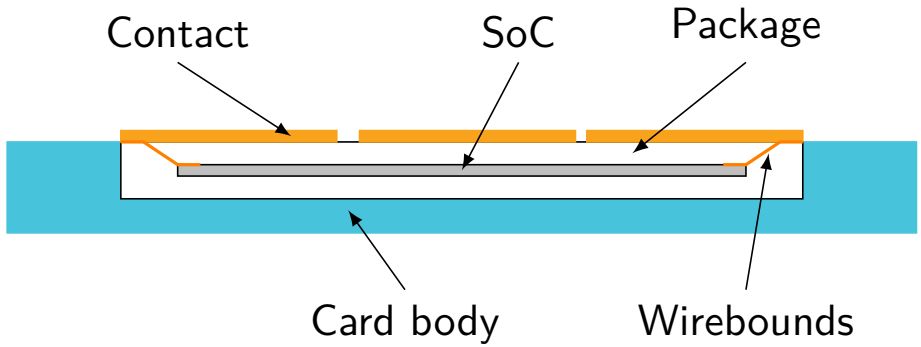
- Run at 300MHz to 3Ghz
- Multithreaded
- Fine engraving $<$ 20 nm
- Dynamic Voltage & Frequency management
- Trusted Environment Execution
- No hardware mitigations

# The packaging

## Computer on Chip package on package




## Secure element package




[9] **Ball Grid Array**

# Assets to protect

- Cryptographic secrets and operations
- Secure boot
- Memory partitioning
- Execution flow integrity
- Trusted part isolation

# Unknowns

- Repeatability ?
- Design impact ?
- Technology impact ?
- New attack paths ?

# Soooo let's start !

- Computer on Chip $\rightarrow$ software security only
- Hardware quite similar with Secure Elements
- Some attacks already exist:
  1. Evaluate their difficulty
  2. Push some uncompleted attacks
  3. Find new paths

# Known 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |

# Known 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |

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

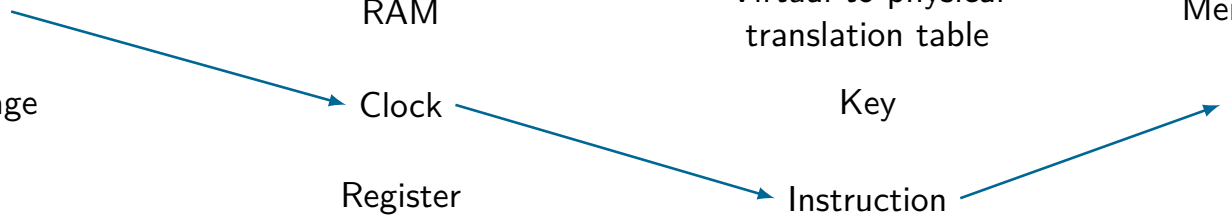
# Known attacks

| 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |

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

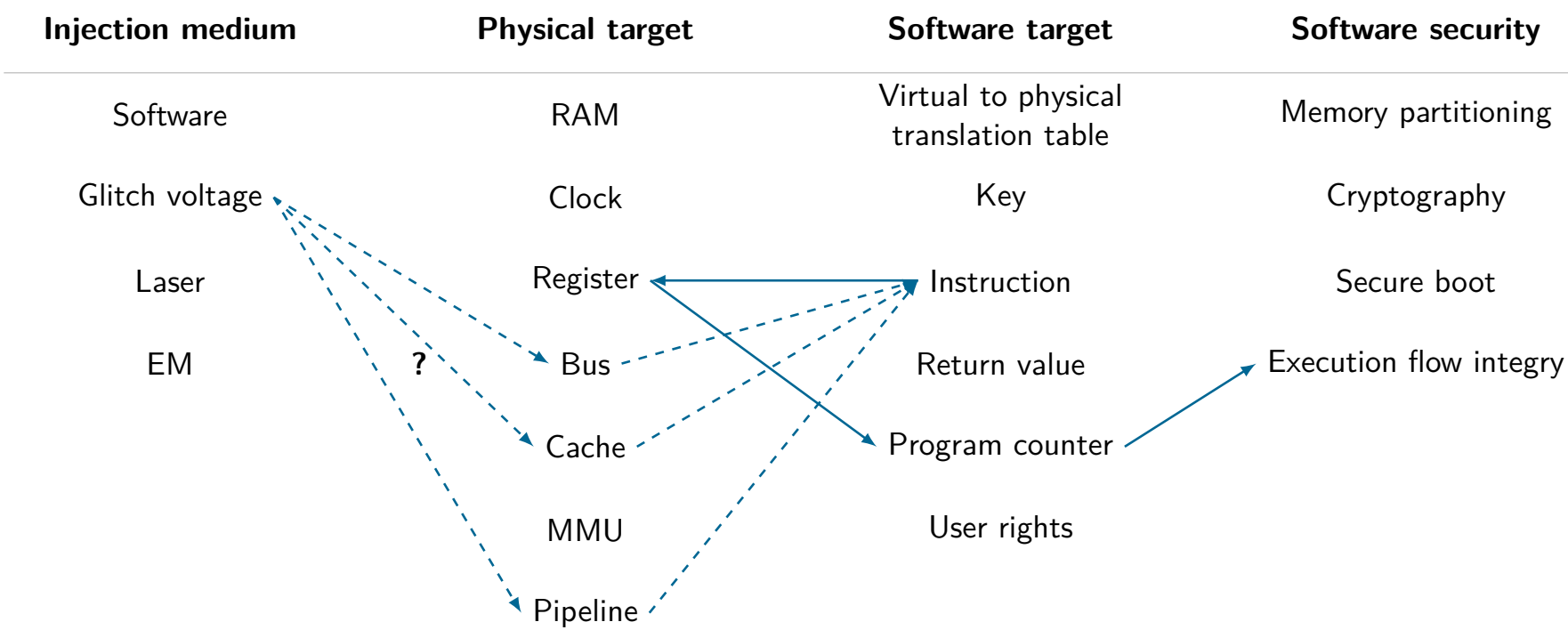
# Known attacks

| 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |



**ClkScrew (2017)** [AS17]

# Known attacks




**Controlling PC on ARM (2016)** [TSW16]

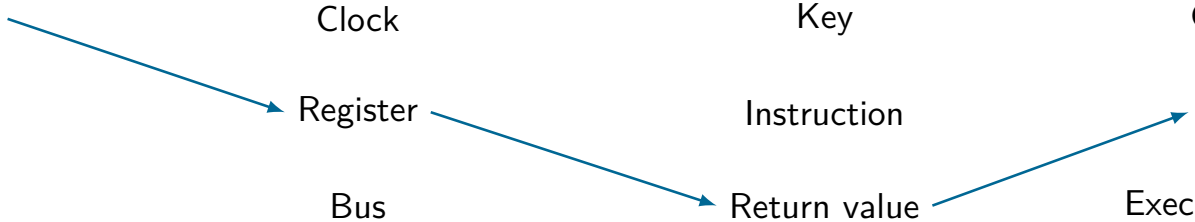
# Known attacks

| 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |

**Attack on PS3**

# Known 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |



**Attack on Xbox 360 (2015)** [Bla15]

# Known 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 |
| | Cache | Program counter | |
| | MMU | User rights | |
| | Pipeline | | |

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

# Conclusion

- Migration of services from Secure Element to Computer on Chip
- Hardware security gap
  - SE is a full trusted environment
  - Computer on chip integrate a software trusted environment
- Invasive/Semi-invasive attacks feel harder on Computer on Chip
- New attack paths

# Questions?

# References


[AS17] Simha Sethumadhavan Adrian Tang and Salvatore Stolfo. *CLKSCREW: Exposing the perils of security-oblivious energy management*. Tech. rep. Columbia University, 2017.

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

[Car17] Pierre Carru. "Attack TrustZone with Rowhammer". In: eshard. 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).

[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.