Enhanced Processor Defence Against Physical and Software Threats by Securing DIFT Against Fault Injection Attacks

PhD Dissertation Defense

William PENSEC

Université Bretagne Sud, UMR 6285, Lab-STICC, Lorient, France

December 19, 2024

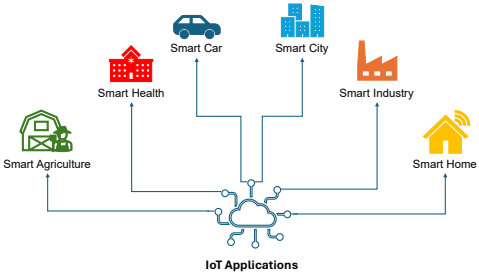
Outline

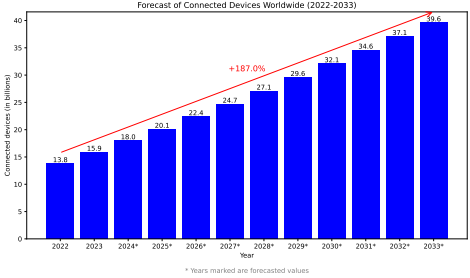
Outline

Context: Embedded Systems and IoT

Internet of Things (IoT)

- Wide range of application
- Fast growing market with exponential usage
- Rely on sensors depending on their use
- Collect and share data
- Manipulation of critical data
- Increasingly vulnerable to multiple threats





Motivations: IoT Under Threats

Threats

- Software threats: malwares, memory overflow attacks, SQL injection, etc
- Network threats: DDoS, Man-In-The-Middle, jamming, etc
- Hardware threats: physical attacks such as reverse engineering, Side-Channel Attacks (SCA), Fault Injection Attacks (FIA)

Motivations: IoT Under Threats

Threats

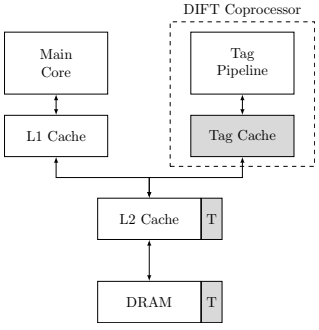
- **Software threats**: malwares, memory overflow attacks, SQL injection, etc
- Network threats: DDoS, man-in-the-middle, jamming, etc
- **Hardware threats**: physical attacks such as reverse engineering, Side-Channel Attacks (SCA), Fault Injection Attacks (FIA)

Software threats: Information Flow Tracking

- Security mechanism
- Protection against software attacks (e.g.: *buffer overflow*, *format string*, *SQL injections*, ...) [1, 2]
- Static or Dynamic
- Software, Hardware or Hybrid
- Hardware DIFT: off-core, off-loading core, in-core

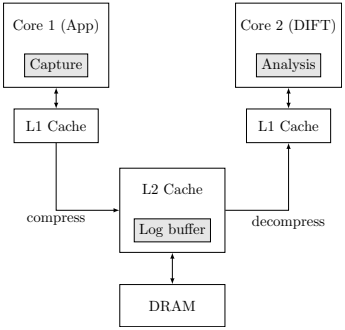
Software threats: Information Flow Tracking

- Security mechanism
- Protection against software attacks (e.g.: *buffer overflow*, *format string*, *SQL injections*, ...) [1, 2]
- Static or Dynamic
- Software, Hardware or Hybrid
- Hardware DIFT: **off-core**, off-loading core, in-core



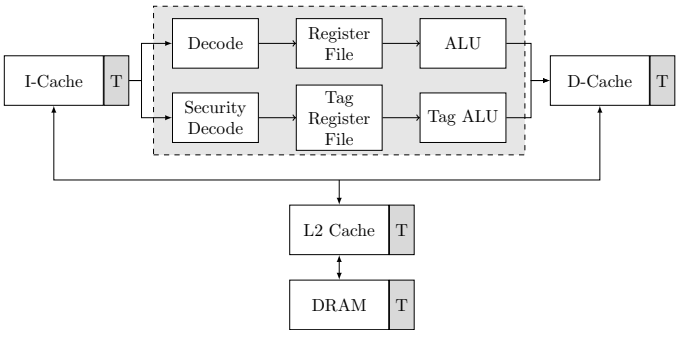
Software threats: Information Flow Tracking

- Security mechanism
- Protection against software attacks (e.g.: *buffer overflow*, *format string*, *SQL injections*, ...) [1, 2]
- Static or Dynamic
- Software, Hardware or Hybrid
- Hardware DIFT: off-core, **off-loading core**, in-core



Software threats: Information Flow Tracking

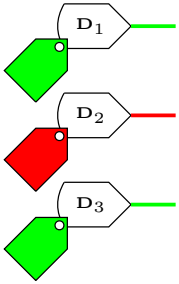
- Security mechanism
- Protection against software attacks (e.g.: *buffer overflow*, *format string*, *SQL injections*, ...) [1, 2]
- Static or Dynamic
- Software, Hardware or Hybrid
- Hardware DIFT: off-core, off-loading core, **in-core**



Dynamic Information Flow Tracking

Three steps

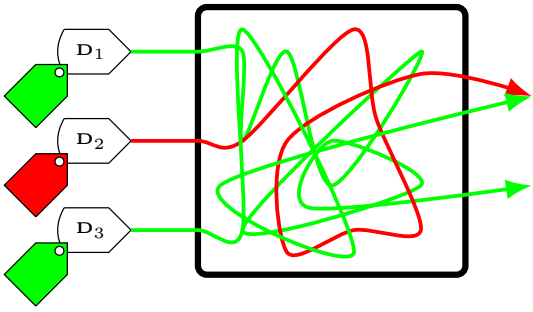
- Tag initialisation
- Tag propagation
- Tag check



Dynamic Information Flow Tracking

Three steps

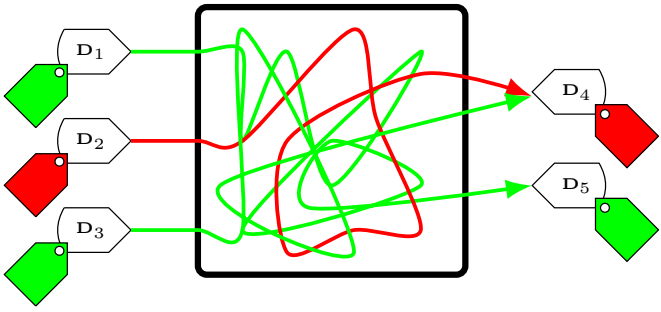
- Tag initialisation
- Tag propagation
- Tag check



Dynamic Information Flow Tracking

Three steps

- Tag initialisation
- Tag propagation
- Tag check

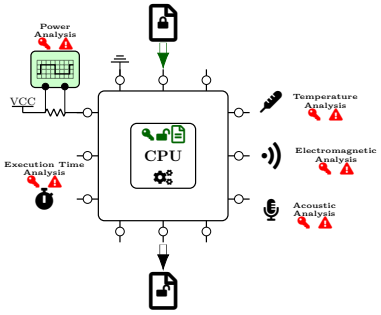


Hardware threats: Physical Attacks

- Reverse Engineering: process of information retrieval from a product by analysing and understanding the design, functionality, and operation of existing hardware
- Side-Channel Attacks: exploit information leakages on the circuit behaviour
- Fault Injection Attacks: involve deliberately introducing one or more fault(s) into the system to observe its behaviour and identify potential vulnerabilities.

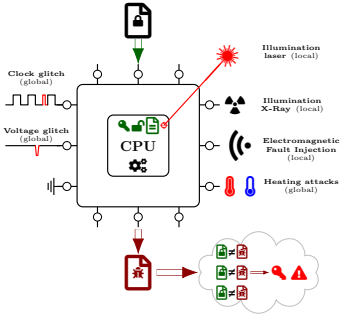
Hardware threats: Physical Attacks

- Reverse Engineering: process of information retrieval from a product by analysing and understanding the design, functionality, and operation of existing hardware
- Side-Channel Attacks: exploit information leakages on the circuit behaviour
- Fault Injection Attacks: involve deliberately introducing one or more fault(s) into the system to observe its behaviour and identify potential vulnerabilities.



Hardware threats: Physical Attacks

- Reverse Engineering: process of information retrieval from a product by analysing and understanding the design, functionality, and operation of existing hardware
- Side-Channel Attacks: exploit information leakages on the circuit behaviour
- Fault Injection Attacks: involve deliberately introducing one or more fault(s) into the system to observe its behaviour and identify potential vulnerabilities.



Issue

How can we maintain maximum protection against software attacks in the presence of physical attacks?

Objectives of this PhD Thesis

Contributions

- Provide a robust security mechanism against software and hardware threats.
- Take into account Fault Injection Attacks
- Propose lightweight countermeasures against FIA
- Take into account constraints, such as area and performance overhead

Outline

D-RI5CY

Vulnerability Assessment

Outline

Introduction

Parity codes

Simple Parity

Hamming Code

SECDED

Outline

Experimental setup

Outline

Conclusion

Perspectives

Publications

Publications

Enhanced Processor Defence Against Physical and Software Threats by Securing DIFT Against Fault Injection Attacks

PhD Dissertation Defense

William PENSEC

Thank you for your attention.

References

References

[1] Christopher Brant et al. “Challenges and Opportunities for Practical and Effective Dynamic Information Flow Tracking”. In: *ACM Computing Surveys* 55.1 (Nov. 2021). ISSN: 0360-0300. DOI: 10.1145/3483790.

[2] Wei Hu, Armaiti Ardeshiricham, and Ryan Kastner. “Hardware Information Flow Tracking”. In: *ACM Computing Surveys* (2021). DOI: 10.1145/3447867.

[3] Transforma Insights; Exploding Topics. *Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033*. Online. Accessed 13 August 2024. 2024. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.