Politecnico di Torino
Dipartimento di Automatica e Informatica
PhD in Computer and Control Engineering
XXXV cycle

Supervisor
*Prof. **Paolo Prinetto***

Vulnerability-Tolerant Architectures for Resource-Constrained Devices

PhD Candidate: *Gianluca Roascio*

1. Context

- **Control-Flow Hijacking Attacks**
- **Embedded Systems**
- **Hardware-based Security**

2. Issues

- **C/C++ languages**: widely used in ES, good degree of low-level control but possible **memory vulnerabilities** for lack of native controls on pointer manipulation;
- Attackers exploit them to **corrupt code pointers** and reach random instructions at will, forcing the system to behave abnormally.

3. Limits of the SOTA Solutions

Control-Flow Integrity (CFI) is a promising defense mechanism based on verifying whether original Control-Flow Graph (CFG) of the program is respected during execution. Anyway:

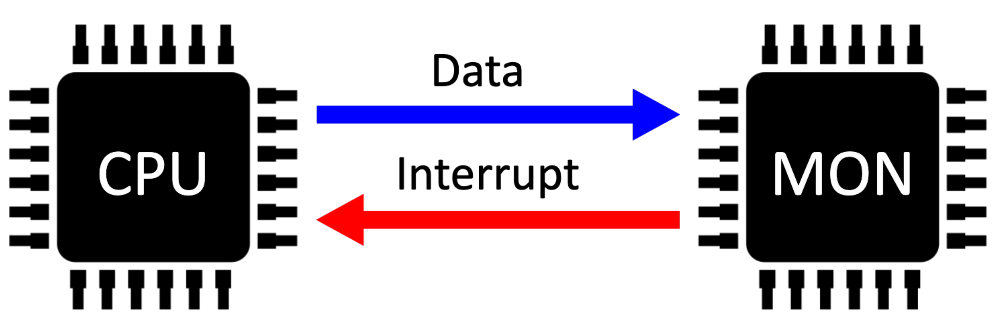
- Original SW-based solutions [1] lack of sufficient isolation and result in **large overhead** in terms of memory footprint and execution time;
- To gain performance, later techniques [2, 3] perform **coarse checks**, e.g., validate branches on all valid destinations, but degrading security;
- In almost all cases, techniques lack a precise strategy to handle **interrupts**, which are by their nature unpredictable through static control-flow analysis [4].

4. Our Approach

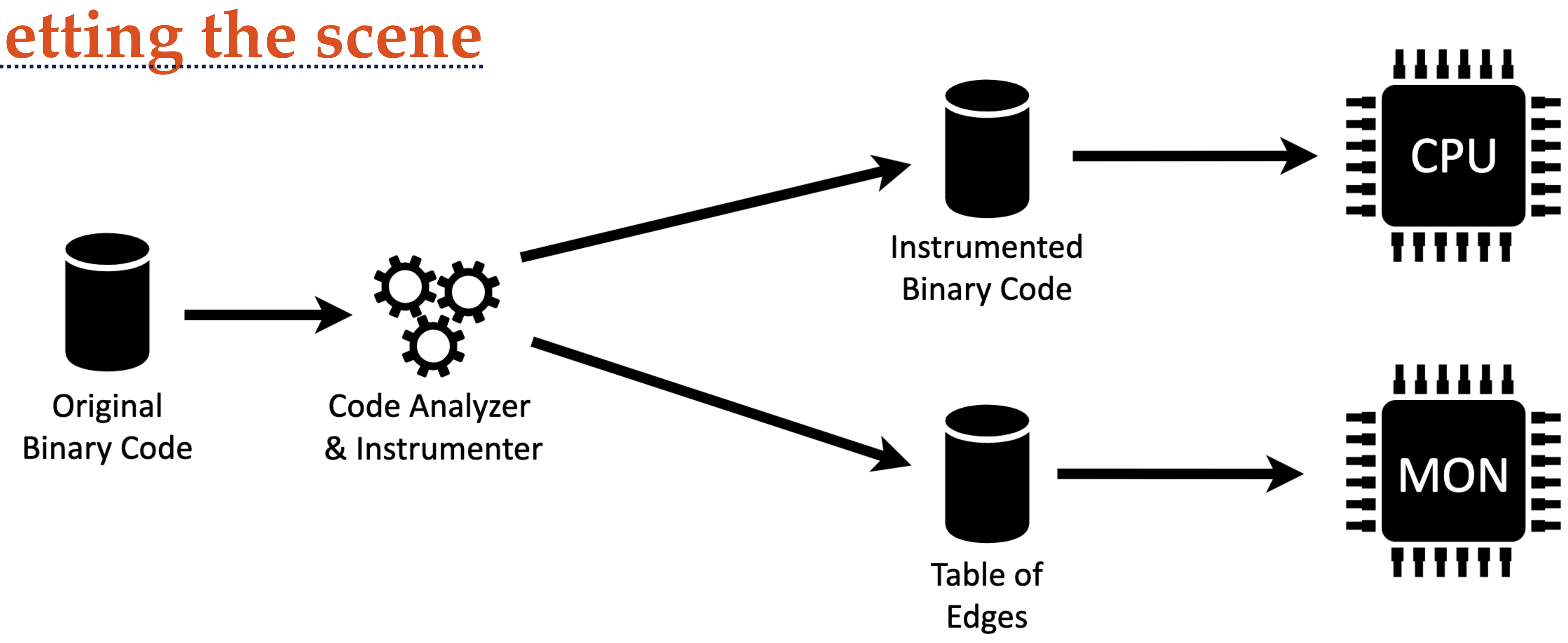
What is protected

- Indirect forward edges
- Backward edges
- Interrupt Service Routines

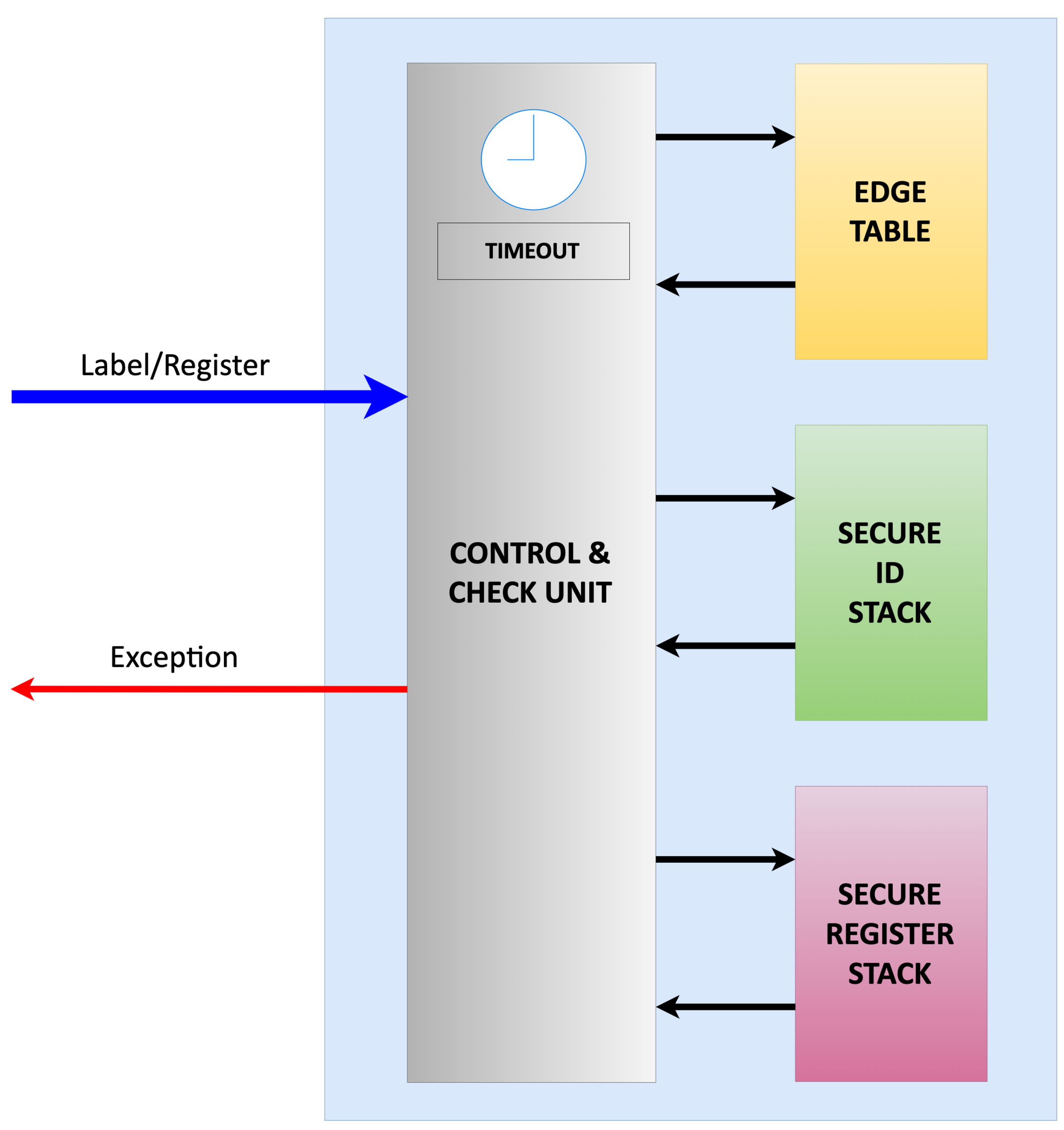
How the protection works



Setting the scene



Monitor structure



5. Experimental Results

- Solution experimented for ARM Cortex-M and 32-bit custom RISC-V processor [6]
- External parallel FPGA for ARM, internal monitor for RISC-V
- ARM: **+17.88%** on code size, **+1.10%** on execution time
- RISC-V: **+0.63%** on code size, **+0.01%** on execution time

6. References

1. M. Abadi, M. Budiu, U´. Erlingsson, and J. Ligatti. Control-flow integrity. In Proceedings of the 12th ACM conference on Computer and communications security, pages 340–353. ACM, 2005.
2. S. Das, Z. Wei, and L. Yang. A fine-grained control flow integrity approach against runtime memory attacks for embedded systems. In IEEE Transactions on Very Large Scale Integration (VLSI) Systems 24.11 (2016): 3193-3207.
3. Zhou, J., Du, Y., Shen, Z., Ma, L., Criswell, J., & Walls, R. J. (2020). Silhouette: Efficient protected shadow stacks for embedded systems. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 1219-1236).
4. N. Maunero, P. Prinetto, and G. Roascio. Cfi: Control flow integrity or control flow interruption?. In Proceedings of the 2019 IEEE East-West Design & Test Symposium (EWDTS). IEEE, 2019.
5. Rajabalipanah, M., Roodsari, M. S., Jahanpeima, Z., Roascio, G., Prinetto, P., & Navabi, Z. AFTAB: A RISC-V Implementation with Configurable Gateways for Security. In Proceedings of the 2021 IEEE East-West Design & Test Symposium (EWDTS) (pp. 1-6). IEEE.