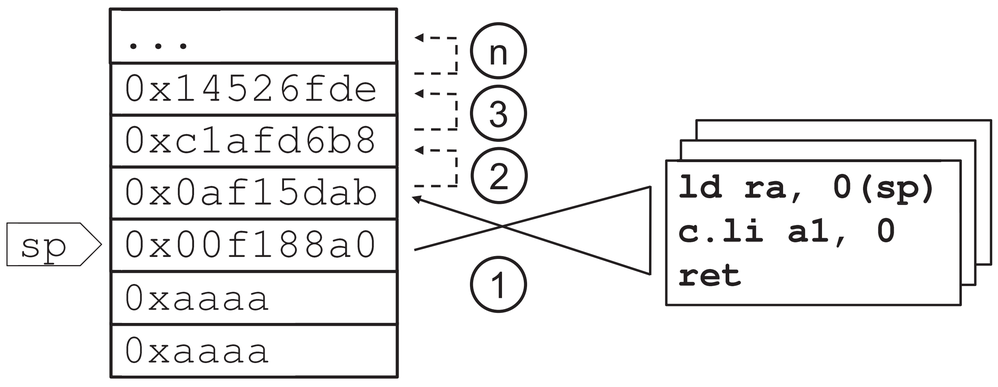
Call Rewinding Towards RISC-V Specification

Téo Biton, Olivier Gilles, Daniel Gracia Pérez, Nikolai Kosmatov, Sébastien Pillement

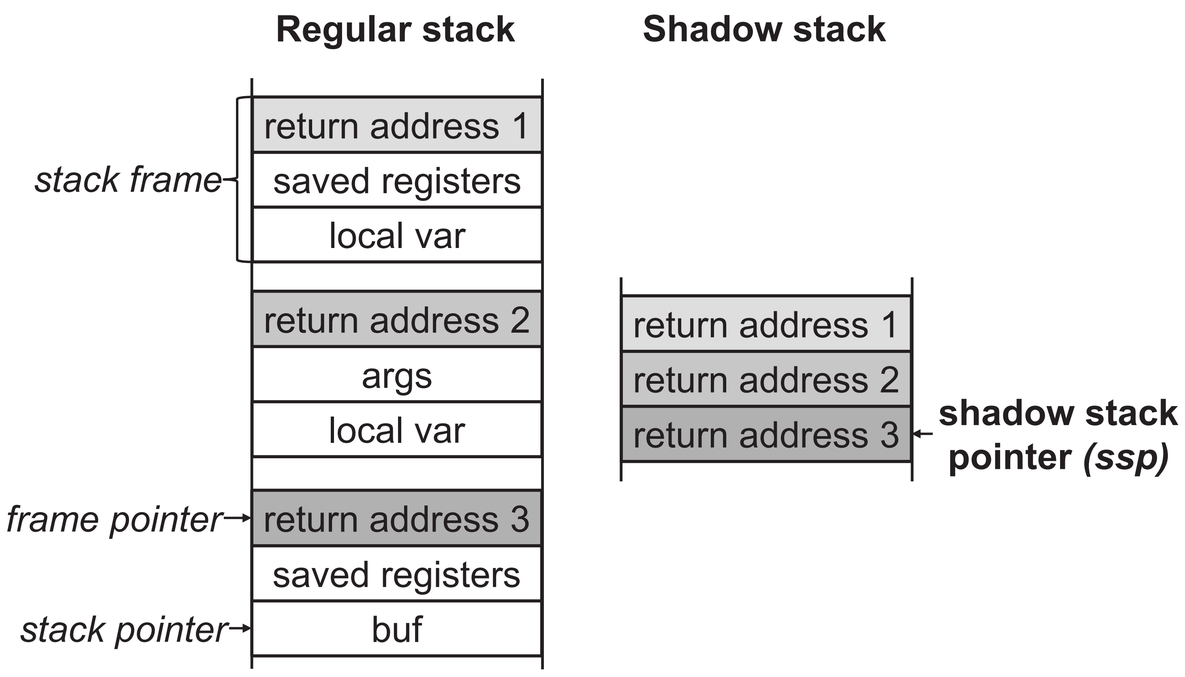
Efficient backward-edge protections on RISC-V

- **Return-oriented programming (ROP)** is a code-reuse attack that overwrites the return address stored in the link register *ra* in order to form a *gadget chain*.
- **Backward-edge protections** verify the integrity of the return address to prevent exploits such as ROP.
- We propose a comparison between RISC-V Shadow Stack extension, **Zicfiss [2]** and previous work, **Call rewinding [1]** evaluated on the open source CV64A6 core.



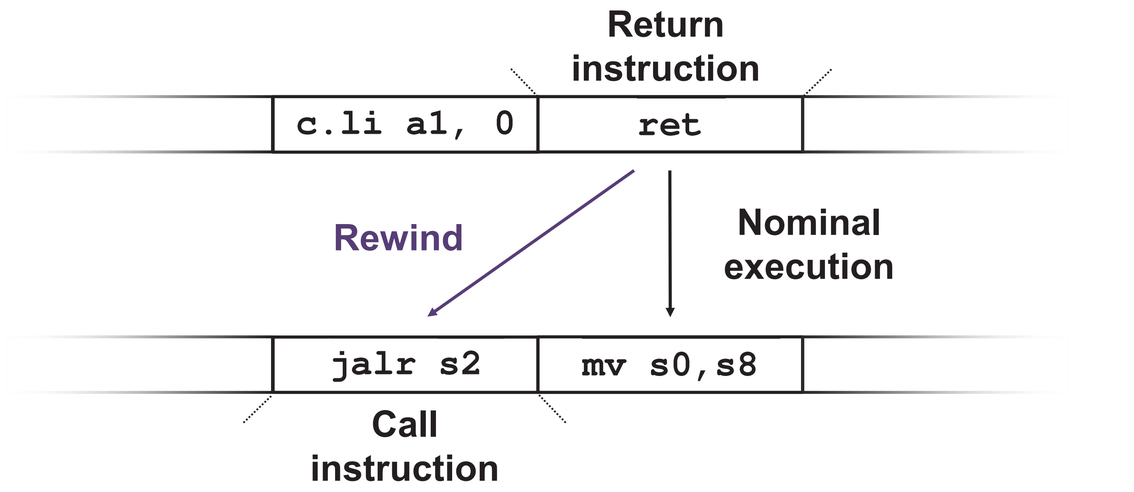
RISC-V Shadow Stack extension *(Zicfiss)*

- The **Zicfiss** extension provides instructions to both load and store the link register in a shadow stack and verify the integrity of the return address.



Call Rewinding

- **Call Rewinding** is a microarchitecture-level mechanism that dynamically detects illegitimate return addresses, by verifying their integrity upon return instructions.



Feature	Call Rewinding	Shadow stacks (Zicfiss)
Security level	Coarse-grained (valid call check)	Fine-grained (exact address match)
Performance	Negligible (~0.12%)	Medium (~1%)
Hardware requirements	Minimal (0.3%)	Minimal (~1%) + memory usage
Integration	No binary modification needed	New instructions
Compatibility	Tightens the ABI (requires *x1* as link register)	Flexible and backward-compatible

Resources

[1] Biton, T., Gilles, O., Gracia Pérez, D., Kosmatov, N., & Pillement, S. (2024). Call Rewinding: Efficient Backward Edge Protection. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(1)*, 227-250.
[2] SS-LP-CFI Task Group. *RISC-V Shadow Stacks and Landing Pads*, Document version 1.0.0, July 2024.

Contacts : Téo BITON teo.biton@thalesgroup.com
Olivier GILLES olivier.gilles@thalesgroup.com
Sébastien PILLEMENT sebastien.pillement@univ-nantes.fr