# Master 2 internship

# Introducing security counter-measures at binary-level

## 1 Introduction and context

Code-reuse attacks hijack the intended control-flow of a running application to produce a malicious effect using constructs (gadgets) presents within the application's code, executed in an arbitrary, attacker-controlled order. In contrast with previous attacks such as shellcodes, CRAs do not require code injection and restrictions on code execution have no effect against them, for it only uses legitimate code to reach a malicious effect [1]. In order to defend against such attacks, solutions based on hardening binaries exists [2]. They however have drawbacks in term of performance and limits in terms of security coverage [3]. In order to overcome these limitations, we propose novel protections to be applied at binary-level, and to be enforced by at micro-architecture-level, specifically on CVA6 RISC-V cores. Our solutions [4] aim at providing reliable runtime security with minimal cost, as we target embedded critical systems such as avionics, space or Industrial Control Systems.

## 2 Objectives of the internship

As part of the Sec-V project, we propose the development of the software part of the counter-measures against CRAs that were designed and already implemented at $\mu$-architecture level. Concretely, the intern will need to inject additional instructions within the binary when detecting specific patterns.

In order to do so, the intern will need to:

- Understand the principles of Code Reuse Attacks and their counter-measures;
- Acquire a deep understanding of the compilation process;
- Extend the compiler (LLVM or GCC) so it could support and generate the new instructions.

## 3 Expected intern profile

We expect a Master 2/Last year engineering school student in software field with the following skills and interests:

Mandatory:

- Knowledge and practice of C code ;
- Basic knowledge in µ-architecture ;
- Interest in security ;
- Interest in research ;

- Strong understanding of English.

Appreciated additional skills:

- Experience with compiler modification ;
- RISC-V architecture ;
- Good writing capacity / experience in scientific publication;
- Cross-compilation experience.

## 4 Consortium Description

The SEC-V project brings together a consortium of researchers and engineers from academic laboratories IETR, LS2N, IRISA and research teams from Thales DIS and TRT.

The intern will be part of a distributed research team consisting in both academics and industrials, actively working on cybersecurity. This internship will be supervised in the IETR laboratory, a member of the SEC-V project, by Professor Sébastien Pillement and PhD student Téo Bitton, as well as Thales Engineer Olivier Gilles. Expertise in compilation will be available to support his work. The intern will also have the opportunity to contribute to a scientific article, and generally to collaborate to the scientific process.

You may be required to collaborate with other consortium stakeholders and take part in associated project meetings.

As integration into the IETR laboratory requires access to a restricted secure area, we ask you to take into account the time required to review your profile if you wish to apply (the process can take up to two months).

## 5 To apply

Send a detailed CV, a motivation letter and your master transcript supporting your application.


- **Pr. Sébastien Pillement**, sebastien.pillement@univ-nantes.fr ,
- **Olivier Gilles**, olivier.gilles@thalesgroup.com ,


## References


[1] Loıc Buckwell et al. “Execution at RISC: Stealth JOP Attacks on RISC-V Applications”. In: *European Symposium on Research in Computer Security*. Springer. 2023, pp. 377–391.

[2] Martín Abadi et al. “Control-flow integrity principles, implementations, and applications”. In: *ACM Transactions on Information and System Security (TISSEC)* 13.1 (2009), pp. 1–40.

[3] Nathan Burow et al. “Control-flow integrity: Precision, security, and performance”. In: *ACM Computing Surveys (CSUR)* 50.1 (2017), pp. 1–33.

[4] Téo Biton et al. “Call Rewinding: Efficient Backward Edge Protection”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025.1 (2025), pp. 227–250.