RESEARCH CENTRE

Inria Centre at Rennes University

IN PARTNERSHIP WITH:

CentraleSupélec, École normale supérieure de Rennes

2024

ACTIVITY REPORT

Project-Team

SUSHI

SecUrity at the Software-Hardware Interface

IN COLLABORATION WITH: Institut de recherche en informatique et systèmes aléatoires (IRISA)

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Inria

Contents

Project-Team SUSHI

Creation of the Project-Team: 2024 January 01

Keywords

Computer sciences and digital sciences

A1.1.2. – Hardware accelerators (GPGPU, FPGA, etc.)

A1.1.8. – Security of architectures

A1.1.10. – Reconfigurable architectures

A1.1.13. – Virtualization

A2.2.1. – Static analysis

A2.2.5. – Run-time systems

A2.2.6. – GPGPU, FPGA...

A2.2.9. – Security by compilation

A2.4.3. – Proofs

A2.6.1. – Operating systems

A2.6.3. – Virtual machines

A4.1.2. – Hardware attacks

A4.4. – Security of equipment and software

A4.5. – Formal methods for security

A4.9.1. – Intrusion detection

A4.9.3. – Reaction to attacks

Other research topics and application domains

B6.5. – Information systems

B6.6. – Embedded systems

1 Team members, visitors, external collaborators

Faculty Members

- Guillaume Hiet [Team leader, CENTRALESUPELEC, Professor, HDR]
- Alessandro Palumbo [CENTRALESUPELEC, Associate Professor]
- Thomas Rokicki [CENTRALESUPELEC, Associate Professor, from Nov 2024]
- Ruben Salvador Perea [CENTRALESUPELEC, Associate Professor]
- Frédéric Tronel [CENTRALESUPELEC, Associate Professor]
- Yaelle Vinçont [ENS RENNES, Associate Professor, AGPR (Agrégée Préparatrice)]
- Pierre Wilke [CENTRALESUPELEC, Associate Professor]

Post-Doctoral Fellows

- Lorenzo Casalino [CENTRALESUPELEC, Post-Doctoral Fellow, from Oct 2024]
- Quentin Ducasse [CENTRALESUPELEC, Post-Doctoral Fellow, from Oct 2024]

PhD Students

- Matthieu Baty [INRIA, until Sep 2024]
- Zakaria Belkadi [INRIA, from Dec 2024]
- Erwan Fasquel [CENTRALESUPELEC, from May 2024]
- Lionel Hemmerle [CENTRALESUPELEC]
- Eliott Quere [UNIV RENNES, from Oct 2024]

Technical Staff

- Jack Royer [CENTRALESUPELEC, Engineer, from Nov 2024]

Interns and Apprentices

- Adam Bouabdallaoui [CENTRALESUPELEC, Intern, from Mar 2024 until Aug 2024]
- Fabio Daussy [CENTRALESUPELEC, Intern, from May 2024 until Jul 2024]
- Gabriel Desfrene [CENTRALESUPELEC, Intern, from May 2024 until Jul 2024]
- Thibaut Frin [CENTRALESUPELEC, Intern, from Mar 2024 until Aug 2024]
- Joffrey Hauw [CENTRALESUPELEC, Intern, from Jun 2024 until Jul 2024]
- Anna Krasovskaya [CENTRALESUPELEC, Intern, from May 2024 until Jul 2024]
- Seydina Oumar Niang [CENTRALESUPELEC, Intern, until Jun 2024]
- Jack Royer [THALES, Intern, from Apr 2024 until Oct 2024]

Administrative Assistant

- Lydie Mabil [INRIA]

External Collaborator

- Louis Rilling [DGA-MI]

2 Overall objectives

Computer systems (e.g. personal computers, servers, or embedded systems) rely on computing platforms to execute user applications and host user data. These computing platforms are made of different hardware and system software (i.e., low-level software components such as Operating Systems, hypervisors, and firmware) and tend to grow in complexity. Indeed, they must fulfil various objectives: optimizing performance and offering new services while limiting energy consumption. To achieve these goals, they rely on complex interactions between heterogeneous computation units like CPU, hardware accelerators, FPGA, and system software. This trend increases with growing architectural heterogeneity and emerging computing paradigms, which might bring new yet hidden vulnerabilities.

Besides these various objectives, such platforms are critical for user applications and data security. To that end, they form the so-called Trusted Computing Base of computer systems. Consequently, any breach in the TCB will dramatically impact user applications and data. This growing complexity of interactions between software and hardware components raises serious privacy and trust issues in today's computer systems. The main research goal of the SUSHI team is to address these issues by assessing and increasing the security level of existing and future computing platforms at the software/hardware interface.

3 Research program

The goal of the SUSHI team is to thoroughly study and contribute to the security of computing platforms at the software/hardware interface, both from an attack and a defense perspective. We do this by exploring three complementary research axes :

- **Vulnerability identification and security by design.** This axis aims first to identify new vulnerabilities resulting from software/hardware interactions in such complex and heterogeneous platforms and, second, to propose secure-by-design approaches to prevent the exploitation of such vulnerabilities.
- **Reactive security at the host level.** This axis focuses on host-based intrusion detection and reaction by leveraging software/hardware interactions.
- **Formal models and proofs for low-level security.** This axis aims to formally prove the security properties enforced or detected by software/hardware mechanisms.

We propose to decline these research axes on three different levels at the software/hardware interface:

- The hardware architecture and microarchitecture level focuses on the hardware part of the interface, which should provide software with the required services to ensure security;
- The system software level focuses on low-level software, such as OSes or hypervisors, which are heavily tied to hardware interfaces and must use them correctly to achieve security;
- The binary executable analysis and instrumentation level focuses on analysing and modifying binary executables, i.e., sequences of instructions belonging to the ISA.

4 Application domains

We focus on host-based system security but do not consider any specific application or type of system. We are interested in various systems, from tiny IoT devices to high-end workstations or servers. Moreover, we aim to provide trusted software/hardware computing platforms that could be helpful in different application domains such as defence, health, industry, or finance.

5 New software, platforms, open data

5.1 New software

5.1.1 HyperSec

Name: A Dedicated Language for Adaptive Rootkit Detection in Virtual Machines

Keywords: Cybersecurity, Anomaly detection, Security

Functional Description: HyperSec is a domain-specific language allowing virtual machines (VMs) to send programs to an hypervisor. These programs leverage the VM's knowledge of its internal OS structures and enable the hypervisor to detect intrusions. To secure this process, we enforce constraints on the set of programs accepted by the hypervisor to prevent the exploitation of vulnerabilities inside the hypervisor.

Contact: Lionel Hemmerle

5.1.2 koika-sushi

Keywords: Formal methods, Coq, CPU, Cybersecurity

Functional Description: This project is the fork of Kôika maintained by the SUSHI team. Kôika is a rule-based Hardware Design Language embedded within Coq. This fork proposes a framework to verify security properties on Kôika circuits using Coq and SMT solvers.

Release Contributions: - Support for more recent Coq versions - Support for SMT powered proofs - Reorganized codebase - Extended RV processor (moved to its own repository)

News of the Year: Support for more recent Coq versions Support for proofs using the progressive rewriting approach described in our CSF paper Support for SMT powered proofs Reorganized codebase Extended RV processor (moved to its own repository)

URL: https://gitlab.inria.fr/SUSHI-public/FMH/koika

Publication: hal-04118645

Contact: Pierre Wilke

Participants: Pierre Wilke, Matthieu Baty

Partner: EPFL - Ecole Polytechnique Fédérale de Lausanne

5.1.3 COQQTL

Keywords: Formal methods, Coq

Functional Description: Formal semantics in Coq of the FIRRTL intermediate representation of the CHISEL Hardware Description Language.

News of the Year: Creation of the project, definition of the semantics of most of FIRRTL constructs (excluding modules and assertions).

URL: https://gitlab.inria.fr/SUSHI-public/FMH/coqqtl

Contact: Pierre Wilke

Participants: Matthieu Baty, Pierre Wilke

5.1.4 heRVé

Keywords: Formal methods, Coq, CPU

Functional Description: This project is a fork of the 4-stage RISC-V pipeline processor of the Kôika project. The design has been rewritten to add support for exceptions and interrupts.

News of the Year: Redesign and support for exceptions and interrupts

URL: https://gitlab.inria.fr/SUSHI-public/FMH/herve

Contact: Pierre Wilke

Participants: Gabriel Desfrene, Pierre Wilke

Partner: EPFL - Ecole Polytechnique Fédérale de Lausanne

5.2 Open data

ESORICS 2024 artefact

Contributors: Jean-Loup Hatchikian-Houdot and Pierre Wilke

Description: Public artefact of ESORICS 2024 [5], including a leakage simulator, a proof of ONI preservation in Coq and a benchmark of several cryptographic and sorting algorithms

Publications: https://gitlab.inria.fr/scratchs-public/esorics2024-artefact

Contact: Pierre Wilke (pierre.wilke@inria.fr)

6 New results

6.1 Vulnerability identification and security by design

6.1.1 Machine Learning-Based Detection of Hardware Trojans

Participants: Alessandro Palumbo.

Keywords: Hardware Security, Machine Learning, Hardware Trojans, Feature Importance, FPGA, RISC-V.

Hardware Trojans (HTs) pose a significant threat to integrated circuits, particularly in scenarios involving RISC-V cores implemented on FPGAs. These malicious modifications can compromise hardware security by leaking sensitive information, altering functionality, or causing device failures. Traditional detection methods face challenges in accurately identifying HTs due to their diverse forms and behaviors. In [7], a Machine Learning-based methodology is proposed to detect and classify HTs with high accuracy. The methodology combines software features, such as performance counters, with hardware features, including circuit worst negative slack, temperature, and the number of flip-flops, extracted from FPGA designs. These features are used to train Machine Learning models capable of identifying malicious modifications effectively. The approach achieves perfect classification and detection accuracy in distinguishing HTs from legitimate circuitry. Experimental validation is conducted across diverse FPGA setups and benchmarks to evaluate the robustness and practicality of the methodology. This validation demonstrates its suitability for real-world applications, highlighting its potential to enhance the security and reliability of FPGA-based systems by providing a systematic and data-driven solution to HT detection challenges.

6.2 Reactive security at the host level

6.2.1 Time control for stealth analysis sandboxes

Participants: Louis Rilling.

Keywords: Evasive malware, Virtualization, Network simulation, Introspection.

Virtual Machine Introspection (VMI) is used by sandbox-based dynamic malware detection and analysis frameworks to observe malware samples while staying isolated and stealthy. Sandbox detection and evasion techniques based on hypervisor introspection are becoming less of an issue since running server and workstation environments on hypervisors is becoming standard and high-end sandboxes manipulate virtual clocks to mask VM execution pauses caused by VMI. However, the fake network environment around a sandbox VM offers opportunities similar to hypervisor introspection for malware to evade. Malware can evaluate the discrepancy between observed performances and a real, presumed network environment of infected targets. VMI pauses also cause visible network performance glitches. To solve this issue, in [3] with Léo Cosseron, Matthieu Simonin and Martin Quinson from the Magellan team, we propose to extend virtual clock manipulation to synchronize hardware-accelerated virtual machines with a discrete-event network simulator. The experimental evaluation shows that our proposal can counter attempts to infer VMI activity from network timing observations.

6.2.2 Hypervisor extension using a Domain Specific Language to detect rootkits

Participants: Lionel Hemmerlé, Frédéric Tronel, Pierre Wilke, Guillaume Hiet.

Keywords: Virtualization, Introspection, Intrusion Detection System, Rootkits.

Endpoint Detection Reaction (EDR) needs to be protected against attackers who manage to gain access to a high privilege level. We propose using virtual extensions for this purpose: the protected system is placed in a VM, and the EDR is implemented in the hypervisor [8]. This ensures that the EDR remains functional even if the VM is fully compromised. However, in such setup, the EDR loses the operating system abstraction provided by the VM. To reduce this semantic gap, we developed a new language that allows a VM to write and send programs to the hypervisor. Since these programs are produced by the VM, we can legitimately assume they have the necessary knowledge about the internal structure of the VM's operating system. The hypervisor runs these programs to detect intrusions. To secure this process, the hypervisor must enforce strict security constraints to ensure that these programs do not introduce new vulnerabilities. Most tested rootkits could be detected with only an acceptable overhead added to the VM's execution. Furthermore, we demonstrate that this overhead can be further reduced by executing native binaries instead of relying on an interpreter. A paper about these results has been submitted in early 2025 and is under reviewing.

6.3 Formal models and proofs for low-level security

6.3.1 Formal verification of hardware/software security mechanisms

Participants: Guillaume Hiet, Pierre Wilke.

Keywords: Formal Methods, Side-channels.

Constant-time programming is the de facto standard to protect security-sensitive software against cache-based timing attacks. This software countermeasure is effective but may incur a significant

performance overhead and require a substantial rewrite of the code. In [5] we propose a secure cache-locking hardware mechanism which eases the writing of secure code and has little execution overhead. To reason about the security of software, we propose a high-level leakage model such that accesses to locked memory addresses do not generate any observable leakage. To ensure the adequacy of this leakage model, we also propose a concrete hardware leakage model for a RISC-V micro-controller where the secure code may be interrupted, at any time, by some arbitrary malicious code. Using the Observational Non-Interference setting, we show formally that the security of the software model is preserved at the hardware level. We evaluate the effectiveness and performance of this mechanism, notably on block ciphers. We also propose and evaluate a new constant-time sorting algorithm.

6.4 Other topics

6.4.1 Large Language Models and Boolean Artificial Intelligence Functions for Features Analysis

Participants: Alessandro Palumbo.

Keywords: Boolean Artificial Intelligence, Decision Making, Large Language Models.

Analyzing texts describing specific scenarios, could be a complex task that requires both precision and explainability to support decision-making processes effectively. Traditional methods often rely on manual interpretation, which can be time-consuming and subject to inconsistencies. Leveraging advancements in artificial intelligence and hardware acceleration can significantly enhance the speed and reliability of such analyses. In [4], an approach is introduced to provide fast and explainable support in the evaluation of texts that describe specific situations. Using road homicide cases in Italy as a use case, key features are extracted from legal texts through a Machine Learning-based engine. These features, representing critical elements of the described scenario, are subsequently processed using a Boolean function to determine whether the conditions for a crime are met. The methodology contributes to bridging the gap between computational efficiency and data interpretability. This approach demonstrates potential for improving decision-making, with lightweight function implementations, providing insights that are both rapid and aligned with predefined criteria

6.4.2 Efficient signal processing for low-delay embedded systems

Participants: Ruben Salvador.

Negative Group Delay (NGD) is a concept not widely explored in embedded digital signal processing systems. In this work [2] we introduce a novel methodology for implementing NGD using second-order Finite Impulse Response (FIR) filter. We include synthesis results that prove the viability of using FIR filters for NGD functions under specific conditions, which involve considering asymmetry coefficients in the time domain. The synthesized results demonstrate the desired time-advance values relative to the input signal frequency, and it is observed that as the normalized advanced-time increases, the normalized frequency also increases. We then design, simulate and test FIR-based NGD parameters before building an FPGA-based proof-of-concept implementation for embedded systems. The experimental results show how the frequency responses of the NGD function at baseband frequency correlate well with the theoretical hypothesis, supporting our analysis and validating our methodology. NGD time-domain characterization was conducted using a sampling frequency of 1 MHz and Gaussian and sinc input signal waveforms. The calculated and experimental results are in excellent agreement, showing a desired time advance of 6 and an average cross-correlation of 98%. The NGD principle presented in this paper is potentially useful for group delay correction processes and signal pure delay reduction in embedded digital signal processing systems.

6.4.3 Design of on-board heterogeneous embedded systems for space applications

Participants: Ruben Salvador.

High-performance on-board payload data processing has become more interesting with the development of radiation-hardened multiprocessor System-on-chip (MPSoC). As recent space-qualified MPSoCs include Arm Central Processing Units (CPUs) and Field Programmable Gate Arrays (FPGAs), an efficient design method is required to deal with complex heterogeneous embedded systems. Both data bit-width (data accuracy) and processing performance are important in astronomy, thus the design methodology should concern application-specific Multi-Objective Optimization Problems (MOOPs). To assist in the design phase of such systems, we propose [6] to combine the roofline performance model with Design Space Exploration (DSE) of hardware/software designs as a methodology. We use High-Level Synthesis (HLS) for FPGA design to configure different hardware architectures based on C/C++ and pragmas. We develop a benchmark for payload data processing on Arm CPUs and embedded FPGA on a heterogeneous MPSoC by adapting open-source libraries for one of the most commonly used algorithms to provide validated libraries to payload teams. The benchmark takes as constraints the SVOM ECLAIRs payload requirements, and as input data the CCSDS test images, executes applications, and verifies output data. We chose an AMD-Xilinx Zynq UltraScale+ evaluation board and the two-Dimensional Fast Fourier Transform (2-D FFT) as a DSE use case. We designed the benchmark on an Arm Cortex-A53 in bare-metal and an embedded FPGA based on Vitis HLS. The results show a customized roofline model with the hardware/software design. The implemented design has 1.6-55 times faster performance compared to the payload execution time requirement. Based on the proposed roofline model and the DSE results, future payload teams can study the trade-off between execution time and area efficiency to select the most suitable implementation.

7 Bilateral contracts and grants with industry

7.1 Bilateral Grants with Industry

7.1.1 ANSSI:

Participants: Matthieu Baty, Pierre Wilke, Guillaume Hiet.

Matthieu Baty started his PhD in October 2020 in the context of a collaboration between Inria and the ANSSI. In this project, we want to formally specify the hardware-based security mechanisms of RISC-V processors to prove that they satisfy a well-defined security policy. In particular, we would like to use the Coq proof assistant to specify and verify the processor formally. We also aim to extract an HDL description of that certified processor that could be used to synthesize the processor on an FPGA board.

7.1.2 ANSSI:

Participants: Zakaria Belkadi, Louis Rilling, Frédéric Tronel.

Zakaria Belkadi started his PhD in October 2024 in the context of a collaboration between Inria and the ANSSI. In this project, we explore using types in operating system source code as a means to get assurance on security properties. With the rise of memory-safe languages for system programming like Rust, type-based techniques in operating system sources have recently started being investigated to assure functional correctness. With security properties, considering the whole program at once instead of individual functions or modules is an additional challenge.

7.1.3 DGA:

Participants: Jack Royer, Frédéric Tronel.

Jack Royer started his research engineer position in November 2024, thanks to a grant from DGA. In this project, we are interested in deobfuscating binaries protected by anti-debugging technical measures. We will start developing tools that target the deobfuscation of binary code protected by anti-debugging techniques. To our knowledge, this last technique has received very little attention in the scientific literature. It is based on the fact that on most operating systems, a process can only be debugged by a single other process (the one that usually acts as the debugger). Based on this property, anti-debugging techniques aim to make it impossible to dynamically analyse a protected program. Based on this property, the program to be protected is launched through a tracer process that will drive the traced process (the one executing the code to be protected).

7.1.4 DGA:

Participants: Quentin Ducasse, Guillaume Hiet.

Quentin Ducasse started his PostDoc position in October 2024 thanks to a grant from DGA. This project aims to propose an intrusion detection approach for hybrid applications by distributing the detection process across different monitors dedicated to each execution unit while minimizing the performance impact on the monitored system and ensuring the protection of the monitors. We propose to use heterogeneous applications developed with High-Level Synthesis (HLS) for platforms utilizing FPGA SoCs (e.g., Xilinx UltraScale+). The implementation involves integrating the monitor generation process into Xilinx's HLS tool based on the LLVM compiler. This approach allows for the insertion of compiler passes capable of analyzing and modifying the intermediate code generated by the compiler.

8 Partnerships and cooperations

8.1 International research visitors

8.1.1 Visits of international scientists

Other international visits to the team

Roberto Boris Martinez

Status: PhD Student

Institution of origin: University of Madrid

Country: Spain

Dates: 25/11/2024 - 25/02/2025

Context of the visit: PhD internship: "Detection of Hardware Threats in Microprocessors Using Probabilistic Data Structures"

Mobility program/type of mobility: research stay

Most cybersecurity strategies for preventing vulnerabilities have focused on software in recent years. However, with the increasing trend of remote manufacturing of microprocessors, different threats have been hidden within the hardware architecture. Probabilistic data structures have proven effective alternatives for preventing and detecting cybersecurity vulnerabilities by optimizing resource usage. This

visit aims to establish collaborative work on this topic with professors Pedro Reviriego Vasallo from the Universidad Politécnica de Madrid and David Larrabeiti López from the Universidad Carlos III de Madrid. By welcoming their PhD student, Roberto Boris Martínez Aguilar from Universidad Carlos III de Madrid, we hope to benefit from their expertise in probabilistic data structures, cybersecurity, and networking. This collaboration aims to continue our research with different strategies and applications and contribute to future research projects at an international level.

Christophe Hauser

Status: researcher (invited Professor)

Institution of origin: Dartmouth College

Country: USA

Dates: 01/06/2024 - 30/06/2024

Context of the visit: Visiting Professor (CentraleSupélec grant).

Mobility program/type of mobility: research stay

During his visit, Christophe Hauser collaborated with Frédéric Tronel and Yaëlle Vinçont to study static and dynamic analysis of binary programs. The objective is to reason about security vulnerabilities at scale in commodity software and embedded firmware, for which current state-of-the-art tools are imprecise and/or unscalable. Furthermore, this first visit was a way to initiate more intensive collaborations in the following years, such as PhD co-advisories and/or student exchange with Dartmouth College.

Volker Stolz

Status: researcher (invited Professor)

Institution of origin: HVL (Bergen)

Country: Norway

Dates: 02/09/2024 - 26/09/2024

Context of the visit: Short-Term Scientific Mission Grant (COST Action CA20111).

Mobility program/type of mobility: research stay

During the visit, we make use of the specialised hardware (ARM-based SoCs) available in SUSHI to use the low-level processor trace mechanism to obtain execution traces of sample programs, and their concrete experience on this platform. These traces are in a highly compressed binary format. Decoded traces can be used to monitor some of the security properties of running applications. At CentraleSupélec, we have established a lab setup with the necessary components to run example programs and obtain program traces on ZCU4 boards. The infrastructure is accessible to lab-researchers and remotely. Volker Stolz then had sessions with Matthieu Baty, Guillaume Hiet, and Pierre Wilke, gaining insights into using Kôika to specify hardware so that future work could be split between the Norwegian and the French partners.

8.1.2 Visits to international teams

Research stays abroad

Participants: Guillaume Hiet, Quentin Ducasse.

Visited institution: HVL (Bergen) and University of Oslo

Country: Norway

Dates: 27/11/2024 - 5/12/2024

Context of the visit: Visiting Researcher

Mobility program/type of mobility: research stay

Thanks to a grant from DGA, Guillaume Hiet and Quentin Ducasse visited Professor Volker Stolz to continue and strengthen the SUSHI team's and HVL's collaboration on using hardware trace mechanisms to detect security intrusions. This visit was also an opportunity to present the team's work to HVL and the University of Oslo.

Participants: Alessandro Palumbo.

Visited institution: International Computer Science Institute, UC Berkeley

Country: USA

Dates: 06/04/2024 - 28/06/2024

Context of the visit: Visiting Researcher

Mobility program/type of mobility: research stay

Thanks to the NGI Enrichers 2023 grant, a research project was conducted at the International Computer Science Institute (ICSI) in Berkeley, California, focusing on hardware security. During the period from April to June 2024, Alessandro Palumbo worked to pose the basis to develop a programmable hardware module integrated into microprocessor-based systems to detect Microarchitectural Side-Channel Attacks (MSCAs). The project utilized Machine Learning-based anomaly detection techniques. The methodology involved integrating a Security Checker between the microprocessor and main memory. This experience at ICSI also facilitated interdisciplinary collaborations. It contributed to identifying innovative approaches to tackle emerging challenges in hardware security, data privacy and machine learning computation in decision-making processes.

Visited institution: Politecnico di Milano, University of Rome Tor Vergata

Country: Italy

Dates: 13-14/11/2024, 16-17/12/2024

Context of the visit: Visiting Researcher

Mobility program/type of mobility: research stay

Alessandro Palumbo had research meetings at the Politecnico di Milano on 13-14/11/2024 and at the University of Rome Tor Vergata on 16-17/12/2024 for his Boost Mobility project. Such a project aims to build a research team to apply for further (more significant) grants (i.e., ERCs).

8.2 National initiatives

8.2.1 PEPR Cybersécurité: projet SECUREVAL (2022-2028)

Participants: Frédéric Tronel, Guillaume Hiet, Pierre Wilke, Erwan Fasquel.

The security assessment of digital systems relies on compliance and vulnerability analyses to provide recognized cybersecurity assurances. The SECUREVAL project of PEPR Cybersecurity aims to design new tools around new digital technologies to verify the absence of hardware and software vulnerabilities and achieve the required compliance proofs. These developments are based on a double approach, first theoretical and founded on the French school of symbolic reasoning, then applied and anchored in the practice of tool development and security assessment techniques. In addition, by exploring new methods for security assessments, this project will also allow France to remain at the top of the world in assessment capabilities by anticipating the evolution of international certification schemes. Within this project's framework, our contribution concerns tasks 4.4 Formal analysis and models at the software-hardware boundary (led by Guillaume Hiet) and 3.2 Vulnerability analysis tools in binary codes (led by Frédéric Tronel). Two PhD and one postdoc funded by this project will start between 2023 and 2025.

8.2.2 ANR Project: TrustGW (2021-2025)

Participants: Guillaume Hiet, Frédéric Tronel, Pierre Wilke, Lionnel Hemmerlé.

In the ANR TrustGW project, we consider a system composed of IoT objects connected to a gateway. This gateway is, in turn, connected to one or more cloud servers. The architecture of the gateway, which is at the heart of the project, is heterogeneous (software/hardware), composed of a baseband processor, an application processor, and hardware accelerators implemented on an FPGA. A hypervisor allows sharing of these resources and allocating them to different virtual machines. TrustGW is a collaborative project between the ARCAD team from Lab-STICC, the ASIC team from IETR, and the SUSHI team from IRISA. The project addresses three main challenges: (1) to define a heterogeneous, dynamically configurable and trusted gateway architecture, (2) to propose a trusted hypervisor allowing the deployment of virtual machines on a heterogeneous software-hardware architecture with virtualization of the whole resources and (3) to secure the applications running on the gateway. Within this project's framework, the SUSHI team's contribution focuses mainly on the last challenge, particularly through the PhD of Lionel Hemmerlé (2022-2025). Guillaume Hiet is the director of this PhD, co-supervised by Frédéric Tronel, Pierre Wilke and Jean-Christophe Prévotet. We will also explore hardware-assisted Dynamic Information Flow Tracking approaches for hybrid applications, which offload part of their computation to an FPGA.

8.2.3 ANR Project: ATTILA (2022-2025)

Participants: Ruben Salvador.

ATTILA tackles the interplay between security and Approximate Computing (AxC) in the context of DNN accelerator security. In particular, it studies the threats posed to such accelerators when built using AxC techniques. We build on the hypothesis of hidden side-channel vulnerabilities that might be due to AxC and on the possibility of leveraging AxC itself to create countermeasures. Specifically, the objectives are:

1. to study power/EM side-channel vulnerabilities of approximate DNN accelerators and the impact of AxC on leakage behaviour and SCA resistance;
2. to build more secure implementations leveraging on DSE and Pareto fronts to facilitate trading-off SCA resistance with inference quality for different approximations;

3. to evaluate AxC and intelligent run-time managers as countermeasures that enable self-adaptation through the Pareto front and beyond to render SCA attacks more difficult;

4. to extend current SCA practices for DNN implementations towards more powerful ML-based techniques.

Rubén Salvador is the PI of ATTILA, which runs in collaboration with the ASIC team from IETR. The project employs 1 PhD student directed by Jean-Christophe Prévotet (INSA Rennes/IETR) and co-supervised by Rubén Salvador and Maria Mendez Real (Polytech Nantes/IETR).

8.2.4 CMA project : Train-Cyber-Expert (TCE) (2022-2026)

Participants: Yohann Rio, Frédéric Tronel.

As part of the France 2030 recovery plan, the SUSHI team participates in the Train-Cyber-Expert (TCE) project, funded by the CMA (Competences and Jobs of the Future) call for projects. TCE is a collaborative project involving several academic partners to develop educational resources in the form of digital content and technological platforms, organized into skill blocks, focusing on modularity, reusability, and competency-based pedagogy leading to certifications. We are involved in this project together with the Inria PIRAT team. Our goal is to propose pedagogical resources in the field of system security. We are currently creating a set of lectures about memory attacks and defences based on existing lectures at CentraleSupélec.

8.3 Regional initiatives

8.3.1 CominLabs project: SCRATCHS (2021-2024)

Participants: Pierre Wilke, Guillaume Hiet.

SCRATCHS is a collaboration between researchers in the fields of formal methods (EPICURE, Inria Rennes), security (SUSHI, CentraleSupélec Rennes), and hardware design (Lab-STICC) [9]. Our goal is to co-design a RISC-V processor and a compiler toolchain to ensure by construction that a security-sensitive code is immune to timing side-channel attacks while running at maximal speed. We claim that a co-design is essential for end-to-end security: cooperation between the compiler and hardware is necessary to avoid time leaks due to the micro-architecture with minimal overhead. In the context of this project, Guillaume Hiet is the director of the Ph.D. of Jean-Loup Houdot, co-supervised by Pierre Wilke and Frederic Besson, on security-enhancing compilation against side-channel attacks.

8.3.2 Boost'Europe

Participants: Alessandro Palumbo.

The objective of the Boost Europe project is to meet researchers and professors to exchange ideas and lay the groundwork for building a team to apply for more extensive research grants (i.e., ERCs or Horizon projects) focused on designing machine learning-based techniques directly on the hardware (FPGAs) to ensure the security and reliability of microprocessor-based systems.

9 Dissemination

Participants: Guillaume Hiet, Ruben Salvador, Frédéric Tronel, Louis Rilling, Yaëlle Vinçont, Alessandro Palumbo, Lionel Hemmerle.

9.1 Promoting scientific activities

9.1.1 Scientific events: organisation

General chair, scientific chair

- Guillaume Hiet was the co-chair of the organizing committee of the Journées Nationales du GDR Sécurité informatique in Rennes.
- Louis Rilling is co-organizer of the CREACH LABS SoSySec seminar (Software and Systems Security).

Member of the organizing committees

- Rubén Salvador was Publicity Chair for SAMOS 2024, in Samos, Greece.

9.1.2 Scientific events: selection

Member of the conference program committees

- Guillaume Hiet was part of the program committees of the following conferences: EAI SecureComm 2024, NSS 2024, VERDI@DSN 2024.
- Alessandro Palumbo was part of the program committees of the 2024 4th International Conference on Computer Communication and Artificial Intelligence (CCAI).
- Rubén Salvador was part of the program committees of the following conferences: IEEE ISVLSI, SAMOS, IEEE LASCAS, DASIP. He also served in the program committee of the workshop PARMA-DITAM (within HiPEAC conference).
- Yaëlle Vinçont was part of the program committee for GreHack 2024.
- Rubén Salvador is part of the scientific committee of the CREACH LABS SemSecuElec seminar (security of embedded electronic systems).
- Guillaume Hiet and Louis Rilling are part of the scientific committee of the SoSySec seminar.

Reviewer

- Rubén Salvador served as reviewer for the following conferences: IEEE ISCAS, IEEE ISVLSI, IEEE ETS, IEEE LASCAS, SAMOS, DASIP. He served as reviewer in the following workshops: MAL-IoT (within Computing Frontiers), PARMA-DITAM (within HiPEAC conference).

9.1.3 Journal

Member of the editorial boards

- Rubén Salvador is Associate Editor for the journal IEEE Embedded Systems Letters (from 2022).

Reviewer - reviewing activities

- Guillaume Hiet served as reviewer for IEEE Transactions on Information Forensics & Security
- Alessandro Palumbo served as reviewer for the following journals: Journal of Systems Architecture (JSA), IEEE Transactions on VLSI, IEEE Sensors and the Journal of Supercomputing
- Rubén Salvador served as reviewer for the following journals: Elsevier Computers & Security, Springer Genetic Programming and Evolvable Machines, IEEE Embedded Systems Letters, IEEE Transactions on VLSI and IACR TCHES (as subreviewer)

Member	Licence-level	Master-level	CS	Univ. of Rennes	ENS	Amout (h eqTD)
Guillaume Hiet	✓	✓	✓			312
Ruben Salvador	✓	✓	✓	✓		208
Alessandro Palumbo	✓	✓	✓			95
Yaëlle Vinçont		✓			✓	128
Pierre Wilke	✓	✓	✓			286

Table 1: Summary of teaching effort (eqTD)

9.1.4 Invited talks

- Guillaume Hiet gave an invited talk on *Enhancing Host-Based Security: Leveraging Hardware and Compiler Techniques for Robust Protection* at the AFSecurity seminar (Oslo - November 28th, 2024)
- Alessandro Palumbo gave an invited talk on *Features Analysis of Threats in Microprocessors: Attacks Detection & Mitigation Techniques* at the University of California, Santa Cruz (Santa Cruz - April 25th, 2024)

9.1.5 Leadership within the scientific community

Guillaume Hiet is the co-chair of the Systems, Software and Network Security working group of the GDR Sécurité Informatique.

9.1.6 Scientific expertise

Frédéric Tronel served as a scientific expert for the Vienna Science and Technology Fund (WWTF). He reviewed a proposal to a project call funded by WWTF.

9.1.7 Research administration

Guillaume Hiet was a member of the recruitment committees for an Assistant Professor position at CentraleSupélec.

9.2 Teaching - Supervision - Juries

9.2.1 Teaching

Several team members are involved in initial and continuing education at CentraleSupélec, a French institute of research and higher education in engineering and science, ENS of Rennes and University of Rennes.

In these institutions, Guillaume Hiet is responsible for the new engineering curriculum in Cybersecurity at CentraleSupélec. Yaëlle Vinçont is partly responsible for the "préparation agrégation" (intermediate year leading to the agrégation competitive exam) at ENS. In 2023-2024, Frédéric Tronel was in delegation at Inria.

The teaching duties are summed up in table 1.

9.2.2 Supervision

PhD students of the team:

- Lionel Hemmerlé (in progress), *Conception et implémentation d'un langage dédié à l'introspection de machine virtuelle*, funded by ANR TrustGW, started November 2022, supervised by Guillaume Hiet (25%, director), Pierre Wilke (25%), Frédéric Tronel (25%), and Jean-Christophe Prévotet (25%)
- Matthieu Baty (defended December 10th, 2024), *Formalisation de mécanismes de sécurité pour l'architecture de processeurs RISC-V*, funded by ANSSI, started October 2020, supervised by Guillaume Hiet (37%, director), Pierre Wilke (38%) and Ludovic Mé (25%).

- Zakaria Belkadi (in progress), *Type-based security properties assurance in operating systems*, funded by ANSSI, started December 2024, supervised by Louis Rilling (25%), Frédéric Tronel (25%), Guillaume Hiet (25%, director), and Florence Schadle (25%).
- Erwan Fasquel (in progress), *Fuzzing for automatic vulnerabilities discovery in closed-source operating systems*, funded by PEPR SECUREVAL, started in May 2024, supervised by Frédéric Tronel (50%, director) and Yaëlle Vinçont (50%).
- Eliott Quere (in progress), *Towards Secure FPGA-Accelerated Clouds: Identification, Exploitation and Detection of Remote Side-Channel Leakage Sources*, started October 2024, funded by Univ. of Rennes, supervised by Guillaume Hiet (25%, director), Rubén Salvador (25%), Alessandro Palumbo (25%), and Maria Méndez-Real (25%)

Supervision of PhD students in other teams:

- Jean-Loup Hatchikian-Houdot (defended December 16th, 2024), *Mécanisme de sécurité contre les attaques temporelles via une coopération entre logiciel et matériel embarqué*, funded by Labex CominLabs SCRATCH project, started October 2021, supervised by Guillaume Hiet (25%, director), Pierre Wilke (25%) and Frédéric Besson (50%).
- Seungah Lee (in progress), *Efficient designs of On-Board heterogeneous Embedded Systems for Space Applications*, funded by CNES, started October 2021, supervised by Ruben Salvador (35%), Angeliki Kritikakou (35%), and Emmanuel Casseau (30%, director)
- Léo Cosseron (in progress), *Time-Accurate Network Simulation Interconnecting VMs with Hardware Virtualization Towards Stealth Analysis*, funded by DGA via CREACH LABS, started October 2022, supervised by Louis Rilling (50%), Martin Quinson (25%, director), and Matthieu Simonin (25%).
- Guillaume Lomet (in progress), *Guess What I'm Learning: Side-Channel Analysis of Edge AI Training Accelerators*, , started October 2022, supervised by Ruben Salvador (35%), Olivier Sentieys (30%, codirector), and Cédric Killian (35%, co-director)

9.2.3 Juries

Guillaume Hiet was:

- a reviewer of the PhD thesis of Quentin Forcioli, *Modélisation des micro-architectures pour la sécurité avec la plate-forme gem5*, Institut Polytechnique de Paris, Palaiseau, November 21th, 2024
- a reviewer of the HDR thesis of Damien Couroussé, *Application outillée de contre-mesures contre les attaques matérielles*, Université Grenoble Alpes, Grenoble, August 28th, 2024
- an external member of the PhD committee of Simon Tollec, *Formal Verification of Processor Microarchitecture to Analyze System Security against Fault Attacks*, Université Paris-Saclay, Palaiseau, November 15th, 2024
- an external member of the PhD committee of Nicolas Gaudin, *Partitionnement dynamique à grain fin contre les attaques par canaux auxiliaires en cache*, Université de Bretagne Sud, Lorient, December 18th, 2024
- a member of the PhD committee of Matthieu Baty, *Formalisation de mécanismes de sécurité pour l'architecture RISC-V*, CentraleSupélec, Cesson-Sévigné, December 10th, 2024
- a member of the PhD committee of Jean-Loup Hatchikian-Houdot, *Mécanisme de sécurité contre les attaques temporelles via une coopération entre logiciel et matériel embarqué*, Université de Rennes, Rennes, December 16th, 2024

Pierre Wilke was:

- a member of the PhD committee of Matthieu Baty, *Formalisation de mécanismes de sécurité pour l'architecture RISC-V*, CentraleSupélec, Cesson-Sévigné, December 10th, 2024

- a member of the PhD committee of Jean-Loup Hatchikian-Houdot, *Mécanisme de sécurité contre les attaques temporelles via une coopération entre logiciel et matériel embarqué*, Université de Rennes, Rennes, December 16th, 2024

Rubén Salvador was:

- a member of the PhD committee of Jérémy Guillaume, *Optimizing data leakage exploitation in the context of screaming-channel attacks*, CentraleSupélec, Cesson-Sévigné, September 27th, 2024

9.3 Popularization

9.3.1 Productions (articles, videos, podcasts, serious games, ...)

Pierre Wilke wrote an article in ERCIM News on the SCRATCHS project [9].

9.3.2 Participation in Live events

Frédéric Tronel, Alessandro Palumbo and Lionel Hemmerlé presented the teams activity and gave a demonstration at the European Cyber Week, Rennes, November 19th, 2024.

During the regional final of the national CGénial competition, Frédéric Tronel gave a talk on a historical perspective of cybersecurity and the current threats to an audience of secondary school students who had qualified for the competition's final.

10 Scientific production

10.1 Major publications

[1] H.-H. Jean-Loup, P. Wilke, F. Besson and G. Hiet. 'Formal Hardware/Software Models for Cache Locking Enabling Fast and Secure Code'. In: *ESORICS 2024, 29th European Symposium on Research in Computer Security, Bydgoszcz, Poland, September 16–20, 2024, Proceedings, Part III*. ESORICS 2024 - 29th European Symposium on Research in Computer Security. Vol. 14984. Lecture Notes in Computer Science. Bydgoszcz, Poland: Springer Nature Switzerland, 6th Sept. 2024, pp. 153–173. DOI: 10.1007/978-3-031-70896-1_8. URL: https://hal.science/hal-04804914.

10.2 Publications of the year

International journals

[2] R. Randriatsiferana, J. Lorandel, R. Salvador and C. Moy. 'Novel digital NGD Methodology for FPGA-based Embedded Systems'. In: *IEEE Access* (2024), pp. 1–14. DOI: 10.1109/access.2024.3403033. URL: https://hal.science/hal-04596488 (cit. on p. 7).

International peer-reviewed conferences

[3] L. Cosseron, L. Rilling, M. Simonin and M. Quinson. 'Simulating the Network Environment of Sandboxes to Hide Virtual Machine Introspection Pauses'. In: EuroSec 2024 - 17th European Workshop on Systems Security. Athène, Greece, 22nd Apr. 2024, pp. 1–7. DOI: 10.1145/3642974.3652280. URL: https://inria.hal.science/hal-04537165 (cit. on p. 6).

[4] G. Garzo, S. Ribes and A. Palumbo. 'Opening the Black Box: How Boolean AI can Support Legal Analysis'. In: CCAI 2024 - 4th International Conference on Computer Communication and Artificial Intelligence. Xi'an, China, 24th May 2024, pp. 269–272. DOI: 10.1109/ccai61966.2024.10603017. URL: https://hal.science/hal-04685601 (cit. on p. 7).

[5] J.-L. Hatchikian-Houdot, P. Wilke, F. Besson and G. Hiet. 'Formal Hardware/Software Models for Cache Locking Enabling Fast and Secure Code'. In: *ESORICS 2024, 29th European Symposium on Research in Computer Security, Bydgoszcz, Poland, September 16–20, 2024, Proceedings, Part III*. ESORICS 2024 - 29th European Symposium on Research in Computer Security. Vol. 14984. Lecture Notes in Computer Science. Bydgoszcz, Poland: Springer Nature Switzerland, 6th Sept. 2024, pp. 153–173. DOI: 10.1007/978-3-031-70896-1_8. URL: https://hal.science/hal-04804914 (cit. on pp. 5, 7).

[6] S. LEE, E. Casseau, A. Kritikakou, O. Sentieys, R. Salvador and J. Galizzi. 'On-board Payload Data Processing Combined with the Roofline Model for Hardware/Software Design'. In: AeroConf 2024 - IEEE Aerospace Conference. Big Sky, Montana, United States, 2024, pp. 1–12. DOI: 10.1109/AERO58975.2024.10521057. URL: https://inria.hal.science/hal-04423185 (cit. on p. 8).

[7] S. Ribes, F. Malatesta, G. Garzo and A. Palumbo. 'Machine Learning-Based Classification of Hardware Trojans in FPGAs Implementing RISC-V Cores'. In: ICISSP 2024 - 10th International Conference on Information Systems Security and Privacy. Rome, Italy, 2024, pp. 1–8. DOI: 10.5220/0012324200003648. URL: https://hal.science/hal-04685628 (cit. on p. 5).

Reports & preprints

[8] L. Hemmerlé, G. .-. Hiet, F. Tronel, P. Wilke and J.-C. Prévotet. *An XVisor extension using a Domain Specific Language to detect Rootkits in Virtual Machines*. 10th Jan. 2025. URL: https://hal.science/hal-04879065 (cit. on p. 6).

Scientific popularization

[9] F. Besson, C. Le Du and P. Wilke. 'Side-Channel Resistant Applications through Co-designed Hardware/ Software: the SCRATCHS Project'. In: *ERCIM News*. Special theme: Software Security October 2024.139 (2024). URL: https://inria.hal.science/hal-04894615 (cit. on pp. 13, 17).