

ADAM HENAULT

PhD Candidate in Hardware Security

adamhlt.com | contact@adamhlt.com | github.com/adamhlt | [LinkedIn](#) | [Google Scholar](#)

PROFILE

PhD candidate at Lab-STICC (Université Bretagne Sud) working on the detection of software and hardware attacks on embedded systems from on-chip hardware metrics. Background in fault injection, SoC design with LiteX and low-level development (C, C++, VHDL, Verilog, x86 assembly). Main developer of LiteInjector (open-source fault-injection tool) and Damn Vuln IoT SoC. 1st place at the CSAW Embedded Security Challenge 2023.

EDUCATION

PhD in Hardware Security <i>Lab-STICC, Université Bretagne Sud</i> – Thesis: <i>Hardware telemetry for embedded system security</i> . Supervisors: C. Monière, P. Tanguy, V. Lapôtre. Expected defense: late 2027. Funded by the DGA and the Brittany Region.	2024 – 2027 <i>Lorient, France</i>
MSc in Hardware Security (ISC CSSE), with distinction <i>Université Bretagne Sud</i>	2022 – 2024 <i>Lorient, France</i>
BSc in Computer Science <i>Université François Rabelais</i>	2018 – 2021 <i>Tours, France</i>

EXPERIENCE

Doctoral Researcher – Lab-STICC <i>Hardware security</i> – Detecting software and hardware attacks on embedded RISC-V SoCs (CVA6, Linux) from hardware performance counters (HPC). Implemented process-aware HPC filtering (Linux kernel and OpenSBI extensions) and a statistical protocol to evaluate it: up to two orders of magnitude less measurement variability; on a buffer-overflow detection case, the false-positive rate of an SVM dropped from 80.6% to 3.2%.	Oct 2024 – Present <i>Lorient, France</i>
Hardware Developer Intern – ARCAD team, Lab-STICC <i>Secure boot chain for Microchip FPGAs</i> – Designed a secure boot chain using the hardware security features of Microchip PolarFire FPGAs, in collaboration with Thales: reduced the bootloader size (memory footprint) while adding security features.	Jan – Jul 2024 <i>Lorient, France</i>
Hardware Developer Intern – ARCAD team, Lab-STICC <i>Fault emulator for LiteX SoCs</i> – Built a modular fault-injection tool for LiteX SoCs on FPGA, which became LiteInjector.	Apr – Jul 2023 <i>Lorient, France</i>
Software Developer Intern – Geology Department, Université de Tours <i>Software to assess phosphorus surplus</i> – Refactored and extended software computing phosphorus surpluses in soil from an SQL database.	Apr – Jul 2021 <i>Tours, France</i>

PUBLICATIONS AND COMMUNICATIONS

- 2026** – A. Henault, C. Monière, P. Tanguy, V. Lapôtre. *Statistical Analysis of HPC Filtering: Towards Reliable Use in Security*. HS3 2026, 2nd Workshop on Hardware-Supported Software Security, Rome. [PDF] [code]
- 2025** – A. Henault, P. Tanguy, V. Lapôtre. *LiteInjector: A LiteX Extension for Fault Injection*. 28th Euromicro Conf. on Digital System Design (DSD), pp. 443–451, Salerno. [PDF] [code]
- 2024** – A. Henault, P. Tanguy. *Damn Vuln IoT SoC: A Modular Platform To Learn Hardware Bug Exploitation*. Talk, SSTIC 2024, Rennes. [slides] [code]
- 2024–2025** – Posters: BitFlip by DGA at European Cyber Week 2025; GDR SoC2 2025; JAIF 2024, Rennes (LiteInjector).

PROJECTS

LiteInjector <i>Python, Migen, LiteX</i> github.com/labsticc-arcad/LiteInjector – Main developer (supervised by P. Tanguy and V. Lapôtre) of an open-source (BSD-2) bit- and cycle-accurate logical fault emulator for LiteX SoCs on FPGA: 5 fault models, event-based triggers, CLI and Python API. Up to 210× faster than HDL simulation on a Linux-capable RISC-V SoC; 4 case studies (VerifyPIN, PMP bypass).	2023
Damn Vuln IoT SoC <i>LiteX, Verilog, Python</i> github.com/Damn-Vuln-IoT-SoC – Main developer (project led by P. Tanguy) of a modular LiteX-based generator of FPGA SoCs with deliberate hardware vulnerabilities, for teaching, CTFs and HDL analysis tool evaluation.	2022

TECHNICAL SKILLS

Languages : C, C++, Python, Java, VHDL, Verilog, x86 Assembly
Hardware and FPGA : LiteX, Migen, SoC design, FPGA (Vivado, Libero), STM32, bare-metal, FreeRTOS
Hardware security : fault injection and emulation, side-channel attacks (MSc), HPC-based attack detection, secure boot
Software security : reverse engineering, exploit development, Windows internals (open-source tooling on [GitHub](#), 1.5k+ stars)
Tools : Qt, Git, Linux, Ghidra, IDA Pro, GDB, Docker, x64dbg

AWARDS, TEACHING AND LANGUAGES

Award: 1st place (international, team of 3), CSAW Embedded Security Challenge 2023 (hardware CTF).
Teaching: ~142 h in total. Master's (reverse engineering, exploits, defensive programming); Bachelor's year 3 (OS); engineering school year 3 (microprocessors); associate degree year 2 (Python).
Languages: French (native), English (B2).