Postdoctoral fellowship: Formal Methods for Software/Hardware Security

Pierre Wilke and Guillaume Hiet
pierre.wilke@centralesupelec.fr
guillaume.hiet@centralesupelec.fr
SUSHI team, CentraleSupélec Rennes, France

Start date: Fall 2025

The security of applications eventually depends on the security of all the abstraction layers upon which they are built. Formal methods allow for high confidence in such systems and have been successfully applied to prove *functional* properties at various levels: at the compiler (e.g., CompCert [12]), OS (seL4 [11], CertiKOS [8]), and hardware level (e.g. Kami [6], Kôika [5]).

Formal methods can also be applied to security properties to prove the absence of certain classes of vulnerabilities. Such approaches are mandatory for high assurance levels (e.g., EAL6-7 in the Common Criteria, ISO/IEC 15408). One of the challenges is considering the different attacker models and their implications at each layer of the software/hardware stack.

Researchers in the Inria SUSHI group have been using formal methods to prove *security* properties at the software/hardware interface: at the compiler [3, 14, 4], OS [7], and hardware level [13, 2, 10].

We seek a postdoc candidate to conduct research using formal methods to prove security at various software/hardware interface levels. A nonexhaustive list of topics that could be explored would be

- proofs mixing compiler (e.g., CompCert) and hardware support to enforce CFI
- proving security of RISC-V enclaves
- proving that our hardware implementation of a RISC-V processor correctly implements the RISC-V ISA (e.g., with SAIL [1])
- stating and proving software/hardware contracts [9]
- proofs mixing OS and hardware support for isolation

Research environment The work will be part of the PEPR SECUREVAL project funded by France 2030, which aims to improve the tools provided to security evaluators.

The postdoc will be part of the Inria SUSHI team in the IRISA laboratory and will be hosted at CentraleSupélec Rennes, France.

Application Please send your application to Pierre Wilke and Guillaume Hiet. Your application should contain a resume, a link to your Ph.D. thesis or the presumed defense date, and recommendation letters.

The candidate should have a strong background with formal methods in general and proof assistants in particular. Knowledge and experience with computer security, compilers, operating systems, or hardware design languages are welcome.

Salary: gross salary 3000-3200€ (before taxes), depending on previous experience.

Benefits package

- Social security coverage
- Subsidized meals
- Partial reimbursement of public transport costs
- Paid holidays leave
- Accommodation facilities available on campus
- Access to vocational training, social, cultural, and sports facilities and activities

References

[1] Alasdair Armstrong et al. "ISA Semantics for ARMv8-A, RISC-V, and CHERI-MIPS". In: *Proceedings of the 46th ACM SIGPLAN Symposium on Principles of Programming Languages*. Proc. ACM Program. Lang. 3, POPL, Article 71. Jan. 2019. DOI: 10.1145/3290384.

[2] Matthieu Baty et al. "A Generic Framework to Develop and Verify Security Mechanisms at the Microarchitectural Level: Application to Control-Flow Integrity". In: *36th IEEE Computer Security Foundations Symposium, CSF 2023, Dubrovnik, Croatia, July 10-14, 2023*. IEEE, 2023, pp. 372–387.

[3] Frédéric Besson, Sandrine Blazy, and Pierre Wilke. "CompCertS: A Memory-Aware Verified C Compiler Using a Pointer as Integer Semantics". In: *J. Autom. Reason.* 63.2 (2019), pp. 369–392.

[4] Frédéric Besson et al. "Compiling Sandboxes: Formally Verified Software Fault Isolation". In: *Programming Languages and Systems - 28th European Symposium on Programming, ESOP 2019, Prague, Czech Republic*. Ed. by Luís Caires. Vol. 11423. Lecture Notes in Computer Science. Springer, 2019, pp. 499–524.

[5] Thomas Bourgeat et al. "The essence of Bluespec: a core language for rule-based hardware design". In: *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, London, UK, June 15-20, 2020*. Ed. by Alastair F. Donaldson and Emina Torlak. ACM, 2020, pp. 243–257.

[6] Joonwon Choi et al. "Kami: a platform for high-level parametric hardware specification and its modular verification". In: *Proc. ACM Program. Lang.* 1.ICFP (2017), 24:1–24:30.

[7] Laurent Georget et al. "Information Flow Tracking for Linux Handling Concurrent System Calls and Shared Memory". In: *Software Engineering and Formal Methods - 15th International Conference, SEFM 2017, Trento, Italy, September 4-8, 2017, Proceedings*. Ed. by Alessandro Cimatti and Marjan Sirjani. Vol. 10469. Lecture Notes in Computer Science. Springer, 2017, pp. 1–16.

[8] Ronghui Gu et al. "CertiKOS: An Extensible Architecture for Building Certified Concurrent OS Kernels". In: *12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016, Savannah, GA, USA, November 2-4, 2016*. Ed. by Kimberly Keeton and Timothy Roscoe. USENIX Association, 2016, pp. 653–669.

[9] Marco Guarnieri et al. "Hardware-Software Contracts for Secure Speculation". In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 1868–1883. DOI: 10.1109/SP40001.2021.00036. URL: https://doi.org/10.1109/SP40001.2021.00036.

[10] Jean-Loup Hatchikian-Houdot et al. "Formal Hardware/Software Models for Cache Locking Enabling Fast and Secure Code". In: *Computer Security - ESORICS 2024 - 29th European Symposium on Research in Computer Security, Bydgoszcz, Poland, September 16-20, 2024, Proceedings, Part III*. Ed. by Joaquín García-Alfaro et al. Vol. 14984. Lecture Notes in Computer Science. Springer, 2024, pp. 153–173.

[11] Gerwin Klein et al. "seL4: formal verification of an operating-system kernel". In: *Commun. ACM* 53.6 (2010), pp. 107–115.

[12] Xavier Leroy and Sandrine Blazy. "Formal verification of a C-like memory model and its uses for verifying program transformations". In: *Journal of Automated Reasoning* 41.1 (2008), pp. 1–31. URL: http://xavierleroy.org/publi/memory-model-journal.pdf.

[13] Thomas Letan et al. "SpecCert: Specifying and Verifying Hardware-Based Security Enforcement". In: *FM 2016: Formal Methods - 21st International Symposium, Limassol, Cyprus, November 9-11, 2016, Proceedings*. Ed. by John S. Fitzgerald et al. Vol. 9995. Lecture Notes in Computer Science. 2016, pp. 496–512.

[14] Yuting Wang et al. "CompCertELF: verified separate compilation of C programs into ELF object files". In: *Proc. ACM Program. Lang.* 4.OOPSLA (2020), 197:1–197:28.