Offer #2024-08004

PhD Position F/M PhD position (F/M) "Automated detection of vulnerabilities and exploitation of transient execution attacks"

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

The doctoral project is part of theREV project which is part of thePEPR Cybersécurité. It will be supervised by Clémentine Maurice, CNRS researcher in the Spirals team, and Sébastien Bardin, researcher at CEA-List.

The REV project is a large consortium composed of:EURECOM, CEA LIST and CEA LETI, CentraleSupélec, Inria, CNRS, Université de Lille, Université de Rennes, LAAS-CNRS.

The research will be conducted in theSpirals team.

Assignment

The security and privacy of modern systems and ubiquitous devices such as personal computers, mobile devices and cloud computing environments rely on computations on secret values. In these systems, hardware is often considered as an abstract layer that behaves correctly, executing instructions and giving an output. However, side effects due to software implementation and its execution on actual hardware can cause information leakage from side channels, resulting in critical vulnerabilities impacting both the security and privacy of these systems. More recently, transient execution attacks [Lipp2018, Kocher2019] have shown that exceptions and misprediction events also leave traces in the microarchitecture and can be used to recover secrets. Detection of Spectre gadgets is particularly important for cryptographic libraries and defenses at the software and hardware level have been proposed. However, state-of-the-art detection tools have scalability issues [Guarnieri2020, Daniel2021] and may flag gadgets that are not exploitable. The topic of this PhD is the automated detection of software vulnerabilities that are due to transient execution attacks and their automated exploitation, at scale.

References

[Daniel2021] Lesly-Ann Daniel, Sébastien Bardin, Tamara Rezk: Hunting the Haunter - Efficient Relational Symbolic Execution for Spectre with Haunted RelSE. NDSS 2021

[Guarnieri2020] Marco Guarnieri, Boris Köpf, José F. Morales, Jan Reineke, Andrés Sánchez: Spectector: Principled Detection of Speculative Information Flows. IEEE Symposium on Security and Privacy 2020

[Kocher2019] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom: Spectre Attacks: Exploiting Speculative Execution. IEEE Symposium on Security and Privacy 2019.

[Lipp2018] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg: Meltdown: Reading Kernel Memory from User Space. USENIX Security Symposium 2018

Main activities

- Bibliography on microarchitectural attacks, and gadget detection,
- Propose and implement improvements in gadget detection,
- Propose and implement techniques for automated assessment and exploitation of Spectre vulnerabilities,
- Scientific publications in top international conferences,
- Presentations of the work in national and international conferences, and in project meetings.

Skills

The ideal candidate will have the following skills:

- Good mastery of English
- Good programming skills and supporting tools.
- Relational skills, e.g., working in a team, effective reporting and communication with all involved stakeholders.
- Sound background in computer science, including microarchitecture, security, and program analysis.

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

General Information

- **Theme/Domain :** Security and Confidentiality
  Information system (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2024-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2024-09-02

Contacts

- **Inria Team :** SPIRALS
- **PhD Supervisor :**
  Maurice Clémentine / clementine.maurice@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.