Offre n°2024-08004

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

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region.For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT)

Contexte et atouts du poste

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.

Mission confiée

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

Principales activités

- 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.

Compétences

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.

Avantages

- 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

Informations générales

- **Thème/Domaine :** Sécurité et confidentialité
  Systèmes d'information (BAP E)
- **Ville :** Villeneuve d'Ascq
- **Centre Inria :** Centre Inria de l'Université de Lille
- **Date de prise de fonction souhaitée :** 2024-10-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2024-09-02

Contacts

- **Équipe Inria :** SPIRALS
- **Directeur de thèse :**
  Maurice Clémentine / clementine.maurice@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.