Job vacancy #2023-06392

PhD Position F/M Verified Offloading Orchestration of Network Functions at the Edge

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Recently graduated

Context

The offered position is proposed by the RESIST team of the Inria Nancy Grand Est research lab, the French national public institute dedicated to research in digital Science and technology. The team is one of the European research group in network management and is particularly focused on empowering scalability and security of networked systems through a strong coupling between monitoring, analytics and network orchestration.

https://team.inria.fr/resist/

This work is in the context of the HiSec project.The HiSec project is part of the 5G PEPR founded by the ANR, which focuses on cyber-security issues in future networks. These networks have played a key role in service delivery for digital infrastructures. These new networking technologies have also penetrated essential and critical services for our daily lives, such as energy, transportation or healthcare. The pervasive use of digital services and networks to control these critical infrastructures significantly increases the attack surface and the opportunities for attackers. We regularly observe attacks against these infrastructures, leading to successful compromise and very significant impacts. The objective of the HiSec project is thus to handle cybersecurity issues in these environments, and propose new mechanisms to protect these networks and detect attacks, attacks against the networking infrastructure itself, or against the services hosted or the users of the network.

Assignment

Smart objects of 5G/6G networks are exposed to a large variety of attacks. Their protection is challenged by their resource constraints in terms of CPU, memory and energy. Security chains, composed of network functions, such as firewalls, intrusion detection systems and data leakage prevention mechanisms, offer new perspectives to protect these devices using software-defined networking and network function virtualization. However, the complexity and dynamics of these chains require new automation techniques to orchestrate them, more specifically when the security functions are offloaded at the network edge.

The objective of this PhD thesis is to automate and verify the building and off-loading of chains of security functions at the edge level, in the context of 5G/6G networks. Depending on contextual changes, such as new security threats, resource degradations and network failures, the security chains may be subject to different off-loading strategies including the transfer, merging and splitting of network functions and their rules. The approach aims at enabling a high level of automation by formally verifying these strategies to make sure that they do not impact on the performance and the security properties of the orchestrated chains and should take into account the knowledge and experience from the different network edges. Moreover, it is well known that formal methods themselves have an exponential complexity both in terms of running time and in terms of resource consumption, which strongly harden their actual deployment for runtime verification in the network.

Main activities

Several axes are envisioned to cover this issue, first of all we can exploit our knowledge of networking and programmability technologies to design domain specific decision procedures specially optimized for considered use cases. A second axis of research would be the parallelization and distribution of the tasks of verification. Indeed, it is often possible to identify independent parts of the model that can be verified in parallel, leading to a more efficient verification in terms of response time. It would then become possible to design the integration of solvers at different levels into the network architecture to verify the correct properties, while preserving network performances, in particular it could be interesting to consider verification methods relying on partially specified systems in order to work with the highly dynamic nature of most 5G and 6G devices.

The expected results include a state-of-the-art with respect to the topic, the identification of one or several specific use case(s), the specification of the decision problem related to this(these) use case(s), the proof of its(their) class(es) of computational complexity and some related results, the specification and implementation of dedicated decision procedures for solving this problem and some reproducibility packages showing their practical efficiency against baseline approaches, as well as a network architecture integrating these solvers and some reproducibility package showing its practical feasibility.

References

- Schnepf, R. Badonnel, A. Lahmadi, S. Merz. Automated Orchestration of Security Chains Driven by Process Learning. In Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning, Nur Zincir-Heywood, Yixin Diao, Marco Mellia, IEEE Press Series on Networks and Service Management, Wiley-IEEE press, 2021
- N. Schnepf, R. Badonnel, A. Lahmadi, S. Merz. Generation of SDN Policies for Protecting Android Environments based on Automata Learning, In Proc. of the IEEE Network Operations and Management Symposium (IEEE/IFIP NOMS 2018), Taipei, Taiwan
- N. Schnepf, R. Badonnel, A. Lahmadi, S. Merz. Rule-Based Synthesis of Chains of Security Functions for Software-Defined Networks. Electronic Communications of the EASST, 76, (2018)
- N. Schnepf, R. Badonnel, A. Lahmadi, S. Merz. Automated Verification of Security Chains in Software-Defined Networks with Synaptic, In Proc. of the IEEE International Conf. on Network Softwarization (IEEE NetSoft), Bologna, Italy, July 2017

Skills

- Required qualification: Master in Computer Science / Engineering Degree in Computer Science

- Required knowledge: solid knowledge in computer science and networking, Interest for (or experience in) network security, formalization/verification methods

- Languages: programming languages (python, c)

- Fluent in english (writing and oral communication)

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 (after 6 months of employment) 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

Remuneration

2051 gross/month for the 1st and 2nd years. 2158€ gross/month for the 3rd year.

General Information

- **Theme/Domain :** Networks and Telecommunications
  System & Networks (BAP E)
- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2023-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2023-12-31

Contacts

- **Inria Team :** RESIST
- **PhD Supervisor :**
  Badonnel Rémi / remi.badonnel@loria.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.

The keys to success

- Solid knowledge in computer science and networking

- Strong formalization/abstraction skills

- Excellent writing, communication and presentation skills in English

- Ability to travel within Europe

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.