Offer #2024-08041

PhD Position F/M Moving-target defense driven by artificial intelligence for cloud composite services

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

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 PhD thesis will take place in the context of the TrustInCloudS project. This project is part of the CLOUD PEPR founded by the ANR, and targets the design of new solutions for the major cybersecurity challenges specific to cloud environments, in order to ensure the confidentiality, integrity and availability of data, applications and services. In particular, its main objective is to study and develop new methodologies to strengthen cloud security and implement them over prototyping platforms, in order to contribute to the development a sovereign and trusted cloud. The project is organized in such a way as to work on the one hand on the security of the infrastructures, and on the other hand on the security of the data (in the broad sense) that these infrastructures host. It will carry out scientific actions on these two main themes, with the objective of proposing new methods and tools for securing cloud infrastructures and their data. This theoretical work will lead, when relevant, to prototype implementations to prove the concept, including potential deployment over the shared infrastructures developed in the SLIDES project of the CLOUD

PEPR.

Assignment

Advances in virtualization techniques together with the growing maturity of orchestration languages contribute to the design and deployment of elaborated cloud services. In particular, these services can be easily designed or modified through the composition of multiple elementary services/resources (such as virtual machines) provided by cloud infrastructures. These services are however exposed to a large variety of security attacks. While traditional static defense techniques allow to reduce the attack surface, they also show their limits to counter more advanced and dynamic attacks. Moving-target defense strategies offer new perspectives with that respect, and can be leveraged by artificial intelligence methods to improve their performance, in order to make recognition activities, which can themselves be based on learning, more difficult.

The objective of this PhD thesis is to design and implement new artificial-intelligence-oriented defensive strategies applied to the context of cloud composite services. The proposed methods will define the movements/changes to be operated over time on cloud composite services (which can go from the simple modification of a configuration parameter to the whole redeployment of a cloud service), by taking into account the specificities/properties inherent to cloud computing, such as rapid elasticity, scalability, and on-demand self-service access, and providing guarantees in terms of explainability and verifiability. In particular, these methods should address the dynamicity of these services, whether this dynamicity is external (e.g. threat evolution) or internal (e.g. changes in the configuration of some resources/services). They should also consider the horizontal and vertical dependencies that may exist between different services, particularly in the context of multiple domains. Finally, the implemented solutions should have a limited impact on service performance (cost minimization).

Main activities

Main activities

The different activities performed during this PhD thesis will include :

- the elaboration of a state-of-the-art about moving-targe defense in cloud infrastructures, including the analysis of the different categories of parameters on which a moving target defense strategy can be applied in a cloud composite service context,

- the design of artificial-intelligence-oriented moving-target defense (MTD) strategies for such services, with guarantee in terms of explainability and verifiability. In particular, we could investigate further the coupling of artificial intelligence together with verification techniques.

- the performance evaluation of these strategies, and their integration with other security mechanisms (such as network and service supervision or threat intelligence activities).

References

- Mohamed Oulaaffart, Rémi Badonnel and Olivier Festor "Towards Automating Security Enhancement for Cloud Services." In the Proceeding of IFIP/IEEE International Sympo-
sium on Integrated Network Management (IFIP/IEEE IM), pp 692-696, IEEE, 2021.

- Mohamed Oulaaffart, Rémi Badonnel, Christophe Bianco. "An Automated SMT-based
Security Framework for Supporting Migrations in Cloud Composite Services. " In the Pro-
ceeding of the IEEE/IFIP Network Operations and Management Symposium (IEEE/IFIP
NOMS). pp 1-9, 2022, IEEE.

- Mohamed Oulaaffart, Rémi Badonnel and Olivier Festor "CMSec: A Vulnerability Preven-
tion Tool for Supporting Migrations in Cloud Composite Services. " In the Proceeding of
the IEEE International Conference on Cloud Networking (IEEE CloudNet). pp 1-9, 2022.

- Mohamed Oulaaffart, Rémi Badonnel and Olivier Festor "C3S-TTP: A Trusted Third
Party for Configuration Security in TOSCA-based Cloud Services", Springer Journal of Network and Systems Management, 2024.

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, java/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

2200 € gross/month

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 :** 2025-10-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-08-31

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 abstraction/formalization skills

- Excellent writing, communication and presentation skills in English

- Ability to travel within Europe or more

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.