Offer #2024-07661

Post-Doctoral Research Visit F/M Accurate detection and modelling of Advanced Persistent Threats in ICS using Machine-Learning techniques

**Contract type:** Fixed-term contract

**Level of qualifications required:** PhD or equivalent

**Fonction:** Post-Doctoral Research Visit

**Context**

Every year Inria International Relations Department has a few postdoctoral positions in order to support Inria international collaborations.

The postdoctoral contract will have a duration of 12 to 24 months. The default start date is November 1st, 2024 and not later than January, 1st 2025. The postdoctoral fellow will be recruited by one of the Inria Centres in France but it is recommended that the time is shared between France and the partner's country (please note that the postdoctoral fellow has to start his/her contract being in France and that the visits have to respect Inria rules for missions).

**Assignment**

Candidates for postdoctoral positions are recruited after the end of their Ph.D. or after a first post-doctoral period: for the candidates who obtained their PhD in the Northern hemisphere, the date of the Ph.D. defense shall be later than September 1, 2022; in the Southern hemisphere, later than April 1, 2022.

In order to encourage mobility, the postdoctoral position must take place in a scientific environment that is truly different from the one of the Ph.D. (and, if applicable, from the position held since the Ph.D.); particular attention is thus paid to French or international candidates who obtained their doctorate abroad.

**Main activities**

Resist team at Inria Nancy and the University of Abomey-Calvi (UAC) have started in 2024 an associate team focusing on the cyber security of Industrial Control Systems. These systems refer to specialized computer systems and networks that manage and control industrial processes. ICS are employed in various industries, including manufacturing, energy production, transportation, etc. They are fundamental in monitoring and regulating industrial processes, ensuring efficiency, safety, and reliability. They include Supervisory Control and Data Acquisition (SCADA) systems, a type of ICS that collects data from sensors remotely and provides a human-machine interface for operators to make real-time decisions. For instance, Benin has initiated projects to modernize the Electrical grid of the “Société Béninoise d’Énergie Electrique (SBEE)”. For this, Benin has built “a National Distribution Control Center (Dispatching)” for the intelligent management of its electrical grid. Indeed, the National Distribution Control Center is a modern infrastructure based on SCADA system allowing real-time monitoring and control of the power distribution network and data collection. This SCADA Electrical grid supervision system enables the analysis of data collected on the Electrical grid to make remote decisions in real time and detect breakdowns to intervene remotely. The smart grid’s optimal and secure data management has become an significant challenge for the Beninese government. This associated team project and the research that will be conducted will be of great help to meet the challenges of securing and analyzing threats of the communication systems widely deployed in such smart grids.

A vast literature exists regarding the detection and analysis of Advanced Persistent Threat (APT) in ICS. However, these approaches are still missing enough detection accuracy and they still fail in operational environments by raising a high number of false positives. This is mainly due to the heterogeneity of these environments with a large number of legacy systems and proprietary applications. For instance, in such environments, many safety processes are deployed and may raise alerts by intrusion detection systems since they have irregular behavior when activating for instance an emergency command to stop the industrial system. In addition, false positive alerts may be issued due to device failure or dysfunction.

The objective of this Postdoc work is to build more accurate and very low positive rate detection systems for ICS while considering advanced threats that usually have low activity profiles. We will leverage Machine Learning (ML) techniques, in particular, deep learning algorithms over Graph Neural Networks (GNN) to better contextualize observed alerts and to check whether they are really due to an attack, a failure, or an unobserved legitimate action. We will rely on publicly available datasets in the literature and on our own ones for building and evaluating these models.
Skills

Machine Learning, Cyber security, some knowledge on Industrial Control Systems will be benefit.

Deadline for application: June 2, 2024.

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

2788€ 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: 2024-11-01
- Duration of contract: 12 months
- Deadline to apply: 2024-06-02

Contacts

- Inria Team: RESIST
- Recruiter: Lahmadi Abdelkader / abdelkader.lahmadi@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.

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.