2020-02462 - Post-Doctoral Research Visit F/M
Automated configuration of network security in Industrial Control Systems [5]

Type de contrat : CDD
Contrat renouvelable : Oui
Niveau de diplôme exigé : Thèse ou équivalent
Fonction : Post-Doctorant

Contexte et atouts du poste
The PhD 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 leading 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 also in the scope of a new collaboration between the Inria Nancy Grand Est research lab in France and the Helmholtz Center for Information Security (DfGPA) in Germany.

Mission confiée
Scientific context:
Industrial Control Systems (ICSs) have been used to rely on rigid architectures documented in standards and recommendations such as NIST 800-82 guideline [1]. These cyber-physical systems are composed of very sensitive devices such as PLCs (Programmable Logic Controllers), HMIs (Human Machine Interfaces) and field devices. Nowadays, ICS systems tend to be more integrated into the IT infrastructure of the enterprise network. It brings higher flexibility for maintenance but also for business purposes and reduces the costs and maintenance overhead. In addition, with the advent of smart technologies such as smart grids, smart cities or smart buildings, it is unavoidable to rely solely on a dedicated infrastructure. As a result, ICSs, which are very sensitive by nature to disruption (even unattended normal events) can dramatically suffer from this situation in terms of security and resilience because main principles of isolation or segmentation cannot be guaranteed anymore.

During decades, assuring performance and satisfying Service-Level Agreements (SLAs) in network has been addressed in different manners. In the last decade, the concept of Software-Defined Network (OpenFlow but also data-plane programming) stimulates new proposal since it is now easier to reprogram the network behavior for both QoS [2] and security [3]. It is still therefore natural to see if these evolution can also be beneficial for ICSs.

Principales activités
Objectives
The objective of the postdoctoral fellow is to consider advances in networking technologies such as SDN but also (Network Function Virtualization) to achieve and adapt dynamically the security of ICS. Even if ICS networks are more and more integrated within the regular IT infrastructure, they still host particular applications and services requiring so different security solutions. On one hand, their sensitivity requires very accurate detection. A simple unseen attack may force a full industry production to stop working for hours and the necessity to have manual operations and consequences can be even more dramatic (explosions, fire, flooding...). On the other hand, communications are mostly Machine-to-Machine (M2M) based lowering so the variety and the unpredictability of communication flows making so easier to predict the normality of the latter. Such statement has been recently used in [4] to automatically derive rules to be enforced in a SDN-enabled ICS network. However, it supposes a full understanding of the ICS system to protect.

With the evolution of ICSs highlighted below such as the integration of many IoT devices in smart environments, their complexity makes the full knowledge of normal communications almost impossible. In particular, it may also depend of the state systems or external events even in the case of M2M communications. Therefore, the objective of the postdoc is to propose and evaluate new solutions that will automatically learn profile of M2M communications in a first step by using different techniques (such as machine learning) before transforming them into dynamic SDN policies.

References

Informations générales
- Thème/Domaine : Réseaux et télécommunications
- Système d’erreurs (BAP E)
- Ville : Villers-lès-Nancy
- Centre Inria : CRI Nancy - Grand Est
- Date de prise de fonction souhaitée : 2020-09-01
- Durée de contrat : 1 an, 6 mois
- Date limite pour postuler : 2020-05-31

Contacts
- Equipe Inria : RESIST
- Recruteur : François Jérôme / jerome.francois@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 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3500 scientifiques pour relever les défis du numérique, souvent à l’interface d’autres disciplines. L’institut s’efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l’économie.

L’essentiel pour réussir
Application deadline
May 31th, 2020 (Midnight Paris time)

How to apply
Upload your files on jobs.inria.fr in a single pdf or zip file, and send it as well by email to jerome.francois@inria.fr and abdelkader.lahmadi@inria.fr.

Your file should contain the following documents:
- CV including a description of your research activities (2 pages max) and a short description of what you consider to be your best contributions and why (1 page max and 3 contributions max); the contributions could be theoretical or practical. Web links to the contributions should be provided.
- Include also a brief description of your scientific and career projects, and your scientific positioning regarding the proposed subject.
- The report(s) from your PhD external reviewer(s), if applicable.
- If you haven’t defended yet, the list of expected members of your PhD committee (if known) and the expected date of defense (the defense, not the manuscript submission).
- In addition, at least one recommendation letter from your PhD advisor should be sent directly by their author(s) to jerome.francois@inria.fr and abdelkader.lahmadi@inria.fr.

Applications are to be sent as soon as possible.

Consignes pour postuler
**Compétences**
- Required qualification: PhD diploma in computer science
- Good expertise in networking, security, machine learning/data mining, ICS architectures
- Computer skills: familiar with Linux, network administration tools, C and Python programming

**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 (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

**Rémunération**
Salary: 2653€ gross/month

---

**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.

---

**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.