**2021-04036 - Scientific Engineer on AI-guided security assessment of 5G IoT Networks**

**Type de contrat :** CDD  
**Contrat renouvelable :** Oui  
**Niveau de diplôme exigé :** Bac + 5 ou équivalent  
**Fonction :** Ingénieur scientifique contractuel

**Contexte et atouts du poste**

The Fifth Generation (5G) mobile networks coupled with Internet of Things (IoT) can provide innovative services for a wide range of users: smart-home, -transport, -health, -city... Providing new IoT services have required first the development of new functionalities with as underlining goals to have more power- and compute- efficient devices which can embed various sensors. Obviously, IoT also supposes a full infrastructure to guarantee the efficiency of communications and processing of information. The embedded devices are thus completed by access points, routers, servers, etc. At the higher levels services are developed and provided to the users. This ecosystem is very rich and cannot be controlled by a unique entity, e.g. services are often developed by third parties, manufacturer of embed devices are different to those providing connectivity... As a result, such a complex system is naturally a source of potential threats and real cases recently demonstrates that IoT can be affected by naïve weaknesses. At Inria, we even demonstrated how simple and cheap can it be take over the control of a Z-Wave home installation in a silent manner.

Therefore, security is paramount of importance. In last decade, many IoT architectures have been proposed, such as the reference model IoT-A, including security modules. However, as highlighted before, security cannot be guaranteed without failure or by-design and this is all the more true with evolving ecosystems such as IoT, with now the emerging trend of using fog-based architecture rather than well-established cloud models. Therefore, vulnerabilities related to IoT are now documented and can be exploited. Looking at the last years, major attacks including the Mirai botnet, Cold in Finland, Brickerbot and the botnet barrage are proofs of the real security concerns that are brought.

There is thus a clear need to automate the security of IoT that can adapt in real-time to the evolving IoT ecosystem (devices appearing, disappearing, configuration changes, updates...). All changes may introduce new threats. Actually, evaluating the security of single device is vital but most of all, considering a set of devices interacting together in their IoT environment is paramount of importance as complex interactions open the way to complex and stealthy attacks. Due to the large number of possible device types, different deployment scenarios and vulnerabilities, manual inspection is impracticable. There is a need for automatically evaluating the security of an IoT system in its globality (rather than just individual devices).

**Mission confiée**

The goal of this work is to automatically evaluate the security of 5G-enabled IoT devices, extract relevant information about their vulnerabilities and asses the overall risk of their usage within 5G environments. We can thus summarize the global process as follows: (1) identification of the IoT deployment through topology discovery and fingerprinting, (2) discovering their vulnerabilities in automated way by relying on AI/ML methods (3) evaluation of the overall risk.

**Principales activités**

The engineer will thus focus on the three steps that can be grouped into two main tasks:

1. Topology discovery and monitoring probes for 5G networks. We can rely on state-of-art tools [9] to extend them with 5G protocols.
2. Vulnerability discovery in IoT devices by developing automated fuzzing tools. We will employ AI/ML techniques to build automated fuzzing processes dedicated to IoT protocols employed in 5G networks.
3. Refine and map the discovered vulnerabilities onto a real deployment of IoT and then derive an overall assessment score of its components.

This work will be achieved in the context of an Inria Project with other partners that aims to evaluate and test 5G technologies before the Olympic Games in Paris 2024.

**Compétences**

- Required qualification: Engineer diploma in computer science
- Good expertise in networking, cybersecurity, machine learning
- Knowledge in NLP method will be appreciated
- Computer skills: familiar with Linux, 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**

Remuneration in regards to professional experiences
Informations générales

- **Thème/Domaine**: Réseaux et télécommunications
  Système & réseaux (BAP E)
- **Ville**: Villers-lès-Nancy
- **Centre Inria**: CRI Nancy - Grand Est
- **Date de prise de fonction souhaitée**: 2021-10-01
- **Durée de contrat**: 12 mois
- **Date limite pour postuler**: 2021-09-30

Contacts

- **Equipe Inria**: RESIST
- **Recruteur**:
  Lahmadi Abdelkader / abdelkader.lahmadi@loria.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 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 180 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.

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 posts 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.