2020-02463 - Post-Doctoral Research Visit F/M Postdoc Position / AI-guided assessment of IoT security [S]

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

Contexte et atouts du poste

Team

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 European research groups 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 will be achieved in the context of the Inria Project SCUBA that aims at developing a full framework for automated assessment and security of IoT. It is also linked to the activities of the group in the H2020 project SecureIoT (https://secureiot.eu) and with the PhD project of a student focusing on fingerprinting technique for IoT. The postdoc will thus have the opportunity to be part of a whole team working on IoT security (mainly 2 researchers, 2 engineers, 2 PhD students) and to use our dedicated IoT platform including numerous devices from different brands and using different protocols for validation purposes.

Contacts

Jérôme François (jerome.francois@inria.fr) and Abdelkader Lahmadi (abdelkader.lahmadi@loria.fr).

Mission confiée

Scientific context

In last years, Internet-of-Things became a reality with numerous protocols, platforms and devices [8] being developed and used to support the growing deployment of smart* services: smart-home, -transport, -health, -city, ... and even the rather usual rigid systems with Industry 4.0. Providing new services has required first the development of new functionalities with as underlying 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 is 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 naive weaknesses [16]. At Inria, we even demonstrated how simple and cheap it can be to take over the control of a Z-Wave home installation in a silent manner [2].

Therefore, security is paramount of importance. In last decade, many IoT architectures have been proposed, such as the reference model IoT-A [2], 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 [14] and can be exploited. Looking at the last years, major attacks including the Mirai botnet, Cold in Finland, Brickerbot and the botnet barrage [12] 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).

Principales activités

Project description

The goal of this work is to automatically prevent intrusions by identifying IoT devices, extract relevant information about their vulnerabilities and assess the overall risk. We can thus summarize the global process as follows: (1) identification of the IoT deployment through topology discovery and fingerprinting, (2) mapping vulnerability to atomic elements of the IoT deployment based on public documentation (3) evaluation of the overall risk.

While there is room for improvement in step (1), we will mainly rely on state-of-the-art techniques around topology discovery and fingerprinting. There exist dedicated techniques for IoT [9]. The postdoc will thus focus on the three other steps that can be grouped into two main tasks:

1. Consolidation of public vulnerability descriptions with information retrieved in step (1). Actually, most of Cyber-Threat Intelligence databases such as those provided by MITRE (CAPEC, CVE, CWE, ATT&CK...) are far from being complete, in particular in the context of IoT that is emerging. Also, many vulnerabilities are similar but documented in a different manners, as for example regarding their implication in the realization of an exploit.
2. Refine and map the previously built database onto a real deployment of IoT and then derive an overall assessment score of its components.

Informations générales

- Thème/Domaine : Réseaux et télécommunications
- Statistiques (Big data) / (BAP E)
- Ville : Villers-lès-Nancy
- Centre Inria : LR Nancy - Grand Est
- Date de prise de fonction souhaitée : 2020-09-01
- Durée de contrat : 1 an, 6 mois
- Date limite pour postuler : 2020-04-30

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 fait appel à de nombreux talents dans plus d’une quarantaine de métiers différents. 900 personnes 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.

L’essentiel pour réussir

Application deadline

May 31st, 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@loria.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) t. jerome.francois@inria.fr and abdelkader.lahmadi@loria.fr.

Applications are to be sent as soon as possible.
Bibliography


[5] BF Van Dongen et al., The prom framework: A new era in process mining tool support, ICATPN 2005


Compétences

- Required qualification: PhD diploma in computer science
- Good expertise in machine learning, logic and stochastic modeling
- Good knowledge in networking, security
- Skills in NLP method use will be appreciated
- Computer skills: familiar with Linux, Scala/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