# Offer #2020-02964

# PhD Position F/M AI-guided assessment of IoT security

**Contract type :** Fixed-term contract

**Level of qualifications required :** Graduate degree or equivalent

**Fonction :** PhD Position

## Context

### 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 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 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. The PhD candidate will thus have the opportunity to be part of a whole team working on IoT security (mainly 2 researchers, 2 engineers) 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), Abdelkader Lahmadi (abdelkader.lahmadi@loria.fr) and Isabelle Chrisment (isabelle.chrisment@inria.fr)

## Assignment

### 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 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 [1,6]. 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 [2].

Therefore, security is paramount of importance. In last decade, many IoT architectures have been proposed, such as the reference model IoT-A [3], 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 [13] 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).

## Main activities

### Project description

The goal of this PhD is to automatically prevent the intrusions by identifying IoT devices, extract relevant information about their vulnerabilities and asses 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 documentations (3) evaluation of the overall risk.

While there is room for improvement in step (1), we will mainly rely on state-of-the-art technique around topology discovery and fingerprinting. There exist dedicated techniques for IoT [9]. The PhD candidate 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.

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. The PhD candidate will thus have the opportunity to be part of a whole team working on IoT security (mainly 2 researchers, 2 engineers) and to use our dedicated Iot platform including numerous devices from different brands and using different protocols for validation purposes.

- **Bibliography:**

[1] Manos Antonakakis *et. al*, Understanding the Mirai Botnet, USENIX Security, 2017

[2] L. Rouch *et. Al,* A Universal Controller to Take Over a Z-Wave Network, Black Hat Europe, 2017

[3] Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob van Kranenburg, Sebastian Lange, Stefan Meissner (eds), “Enabling Things to Talk”, Designing IoT solutions with the IoT Architectural Reference Model, Springer, 2013

[4] J. François *et. al,* PTF: Passive Temporal Fingerprinting, IFIP/IEEE International Symposium on Integrated Network Management (IM), 2011

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

[6] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84, 2017.

[7] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, Sasu Tarkoma: IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. ICDCS 2017:

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015.

[9] IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, 2017

[10] P. Stenetorp, S. Pyysalo, G. TopiÂ □c, T. Ohta, S. Ananiadou, and J. Tsujii, BRAT : a web-based tool for NLP-assisted text annotation in Demonstrations, 13th Conf. of the European Chapter of the Association for Computational Linguistics. Association for Computational Linguistics, 2012.

[11] https://prodi.gy/, Radically efficient machine teaching. An annotation tool powered by active learning.

[12] B. Goertzel, M. Ikl, I. F. Goertzel, and A. Heljakka, Probabilistic Logic Networks: A Comprehen-

sive Framework for Uncertain Inference. Springer, 2008.

[13] J. Wallen. “Five nightmarish attacks that show the risks of IoT security”. ZDNet June 2017. Available at: http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/

[14] https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

## Skills

### Required qualifications

– Required qualification: PhD diploma in computer science

– Good expertise in networking, security, machine learning, logic and stochastic modeling

– Knowledge in NLP method will be appreciated

– Computer skills: familiar with Linux, Scala/Python programming,

## 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

Salary: 1982€ gross/month for 1st and 2nd year. 2085€ gross/month for 3rd year.

Monthly salary after taxes : around 1596,05€ for 1st and 2nd year. 1678,99€ for 3rd year. (medical insurance included).

## 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 :** 2021-01-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2020-10-31

## Contacts

- **Inria Team :** RESIST
- **PhD Supervisor :**
  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.

## The keys to success

### Application deadline

### October 31th, 2020 (Midnight Paris time)

### How to apply

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

Applications are to be sent as soon as possible.

**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.