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 (j Jerome.francois@inria.fr), Abdelkader Lahmadi (Abdelkader.lahmadi@loria.fr) and Isabelle Chrisment (Isabelle.chrisment@inria.fr)

Mission confiée
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 the Internet in 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 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 comprised and managed as a unique entity; each part of it is 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 demonstrate that IoT can be affected by naïve weaknesses [1,6]. At Inria, we even demonstrated how simple and cheap it can 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).

Principales activités
Project description
The goal of this PhD is to automatically prevent the intrusions by identifying IoT devices, extract relevant information about their vulnerabilities and assess the overall risk. We can thus summarize the global process as follow: (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 techniques around topology discovery. There exist dedicated techniques for IoT [11]. 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.
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:


Compétences

**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

**Avantages**

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 5 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


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