2019-01357 - Post-Doctoral Research Visit F/M Identifying and Breaking IoT Intrusion Chains [S]

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

Contexte et atouts du poste

Team:
This postdoctoral activity 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 project H2020 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.

Supervision and contact: Jérôme François (jerome.fransois@inria.fr), Abdelkader Lahmadi (abdelkader.lahmadi@loria.fr)

Additional links: RESIST team website (https://team.inria.fr/resist/), J. François’s homepage (http://jeromefra.free.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 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 embeded 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 naive 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 IoTecosystem (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 discovering automatically intrusion chains in IoT environments and automatically break those chains to guarantee the security.

Principales activités

The goal of this work is to automatically prevent the intrusions by first identifying the potential intrusion chains. 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) building intrusion chains (4) break intrusion chains in an optimized manner to limit the impact on the end-users.

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

- 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. There isa lack of a comprehensive integration of all these documents into a unique database. Our proposal is to build a graph-based knowledge base that rely on identified similarities and correlations among all public documents that are human-written. To realize this objective, the postdoc will mainly rely on NLP (Natural Language Processing) techniques and existing annotation tools, such as Brat [10] or Prodigy [11] to build the recognition models. They will allow to classify and group descriptions, that will extend existing (document) relationships.
- Intrusion chain analysis. The objective here is to derive and map the previously built database onto a real deployment of IoT and then derive the intrusion chains. To identify intrusion chains, we propose to model every threat in terms of predicate including pre and post-condition. Logic inference can be thus used. However, as the knowledge graph and its mapping are based on uncertain assumptions (such as similarities), we will also leverage Probabilistic Logic Network [12] (PLN). It allows to...
model causal relations with some uncertainty. Indeed, having a perfect knowledge about dependency among the pre- and postcondition is impossible in our case. Therefore, different solutions could be used for modeling uncertainty. Each event could be quantified as a single probability within a Bayesian models but it is impracticable for precise inference. A more advanced technique is to use a probability distribution but this assumes to know it, which may not be always the case, at least with a high confidence level. PLN comes into the game by being a kind of intermediary solution between single probability- and probability distribution-based models. Once intrusion chains are identified and actually weighted thanks to the previous techniques, all of them can be merged into a single graph that can be mined to precisely identify the best places to cut links to break all single intrusion chains while limiting the number of cut. Rather than focusing on a fixed snapshot at a fixed time, predicting future evolution of the graph (or most probable areas that can be extended) will be considered to break the graph at a point that may also automatically break future intrusion chains “under-construction” (preventive security).

**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 methods will be appreciated
- Computer skills: familiar with Linux, Scala/Python programming

**Language:** English

**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

**Informations générales**

- **Thème/Domaine :** Réseaux et télécommunications
- **Ville :** Villers-lès-Nancy
- **Centre Inria :** CRI Nancy - Grand Est
- **Date de prise de fonction souhaitée :** 2019-10-01
- **Durée de contrat :** 1 an, 4 mois
- **Date limite pour postuler :** 2019-06-05

**Contacts**

- **Equipe Inria :** RESIST
- **Recruteur :** François Jérôme / jerome.francois@inria.fr
A propos d'Inria

Inria, l'institut national de recherche dédié aux sciences du numérique, promeut l'excellence scientifique et le transfert pour avoir le plus grand impact. Il emploie 2400 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3000 scientifiques pour relever les défis des sciences informatiques et mathématiques, souvent à l'interface d'autres disciplines. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 160 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
June 6th, 2018 (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. 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.

Applications are to be sent as soon as possible.

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 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.