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 documents (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 (3). 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 author(s).

2. Refine and map the previously built database onto a real deployment of IoT and then derive an overall assessment score of its components.

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 documents (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 (3). 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 author(s).

2. Refine and map the previously built database onto a real deployment of IoT and then derive an overall assessment score of its components.
Bibliography


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

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.