



ESR Project title: Distributed intrusion detection system in a constrained edge context [ESR11]

Contact names: Alexis OLIVÉREAU (alexis.olivereau@cea.fr)

Institution: CEA List, Paris, France

Application deadline: May 31, 2021

ESR Project Description:

This project deals with the detection of security attacks at the network edge via distributed and resource constrained processors. The objectives are: (1) To design a Distributed intrusion detection system suited to network topologies made up of constrained objects and capable of operating on these objects; (2) To adapt the system dynamically according to detected attack or resource constraints, while achieving energy efficiency an high performance, i.e., a low false positive rate, the capability to detect weak signals, real-time operation, etc.; (3) To investigate techniques to obtain an overview of the monitored topologies by collecting data from all detection nodes; (4) To investigate techniques to enhance the detection capability of all system components.

Expected Results:

To develop an adaptable distributed detection system, based on a SDN (Software Defined Networking) architecture, able to change the detection strategy according to resource constraints and/or knowledge on the attack risks; (2) To define policies allowing Part B - Page 27 of 69 the detection primitives to be adapted to the detection system status and constraints; (3) To highlight and develop innovative techniques to increase detection efficiency in a distributed system made up of constrained objects and of more powerful ones.

Supervision and Mobility Program:

Once hired, the candidate:

- will work at CEA List, performing full-time research under the supervision of Alexis OLIVÉREAU.
- will be enrolled in the PhD program at Telecom Sud Paris, under the supervision of Dr. Mireille SARKISS.
- will additionally pursue two secondments at CTTC and NBL, for a respective duration of 5 and 5 months.

Required, Preferred and Desired Prerequisites/Skills:¹

- **Required:** At the time of recruitment, the applicant must not have lived in France for more than 12 months in the previous 36 months (3 years).

¹ **Required**, means mandatory to pass the eligibility check. **Preferred**, means highly welcome and recommended. **Desired**, means additional, not strictly needed, but still very much appreciated.



- **Required:** No more than 4 years spent in research/work activities after the achievement of the MS degree.
- **Preferred:** A Master's degree in Telecommunications, Computer Science, Data Science or equivalent.
- **Preferred:** Excellent knowledge of IP-based networking and IoT
- **Preferred:** Excellent knowledge of key cybersecurity topics & trends in the field of IP-based networking
- **Preferred:** good skills in the Python programming language
- **Preferred:** good skills in machine learning
- **Preferred:** good skills in practical IP network setup and configuration
- **Preferred:** Very good communication skills in oral and written English
- **Preferred:** Open-mindedness, strong integration skills and team spirit
- **Desired:** good skills in the C programming language
- **Desired:** previous training MS-level training on machine learning techniques
- **Desired:** previous experience in implementation for embedded platforms