JOB SPECIFICATION
FOR CALL FOR APPLICATIONS

Date of update: February 2020

Job title: Postdoctoral researcher (F/M)

Localisation : Palaiseau

Entity / Service: Télécom SudParis / RST

Position of supervisor: Head of RST department

Categories or professions of agents who can apply: II - R / T

Category and job occupation in IMT: II - P

Category in the public service: A

One year contract renewable

ABOUT TELECOM SUDPARIS

Telecom SudParis is a public graduate school for engineering, which has been recognized on the highest level in the domain of digital technology. The quality of its courses is founded on the scientific excellence of its faculty and on teaching techniques that emphasize project management, innovation and intercultural understanding. Telecom SudParis is part of the Institut Mines-Telecom, the number one group of engineering schools in France, under the supervision of the Minister for Industry. Telecom SudParis with Ecole Polytechnique, ENSTA Paris, ENSAE Paris and Telecom Paris are co-founders of the Institut Polytechnique de Paris, an institute of Science and Technology with an international vocation.
Its assets include: a personalized course, varied opportunities, the no.3 incubator in France, an ICT research center, an international campus shared with Institut Mines-Telecom Business School and over 60 student societies and clubs.

CONTEXT AND OBJECTIVES :

Context:
SPARTA is one of the four pilots, funded by the European Commission, to become the European Cybersecurity Research and Competences Center. In SPARTA, research and innovation projects are articulated within 4 programs, including CAPE (Continuous Assessment in Polymorphic Environments) which deals in particular with the performance assessment of cybersecurity.
In CAPE, Télécom SudParis aims at improving the assessment of cybersecurity measures such as intrusion detection systems (IDS) or security information and event management (SIEM)

systems. We propose a framework to integrate tools and metrics for traffic generation with the purpose to perform diverse tests:

- synthetic legitimate traffic in order to implement a realistic environment when data is unavailable for privacy purposes
- legitimate/malicious trafic bootstrapping from existing traces with the ability to apply diverse transformations to the obtained traffic in order to generate more diverse traffic and augment the dataset size
- synthetic adversarial traffic in order to bypass detection

Objectives:
The main goal is to propose new methods to assess IDS and SIEM solutions that leverage machine/deep learning or not, including methodologies, metrics and existing tools.
The job activities include, but are not limited to:

- state of the art of intrusion detection and alert correlation, and the related assessment methods, with a focus on robustness
- design of metrics to assess the robustness of the proposed model
- assessment methods to evaluate robustness of approaches leveraging generative adversarial networks (GAN) or deep learning, in the face of asymmetric traffic datasets; special focus on legitimate/malicious traffic generation using generative models
- design of a multi-objective optimisation model to evaluate the robustness of IDS and SIEM

ACTIVITIES :

- Development of an IDS/SIEM assessment prototype
- Contribution to research works (security assessment, intrusion detection, traffic generation)
- Interaction with project partners (in SPARTA)
- Supervision of interns

TRAINING AND SKILLS:

Level of training and / or experience required:

- Ph.D in computer science

Essential skills, knowledge and experience:

- machine learning, including deep learning and generative models
- LaTeX
- Python programming
- English proficiency

Advantageous skills, knowledge and experience:

- computer networks
- cyberrsecurity (intrusion detection, alert correlation)
- machine learning reliability and explainability

Abilities and skills:

- Ability to adapt an international workplace
- Ability to work in a team
- Autonomy
- Ability to synthetise the research work in academic publications

TO APPLY:

Please send :

- a motivation letter
- a resume

- recrutements@imtbs-tsp.eu
Or
- Télécom SudParis - HRD - 9 rue Charles Fourier - 91000 EVRY - FRANCE

Contact person: Grégory BLANC, gregory.blanc@telecom-sudparis.eu

Web Site: https://www.telecom-sudparis.eu/

Information of the candidate on the processing of personal data: https://bit.ly/2QeOZhl