DESCRIPTION DE POSTE
POUR APPEL A CANDIDATURE

Date de mise à jour : Février 2020

Intitulé du poste : Post-doctorant en cybersécurité (F/H)

Localisation : Palaiseau

Entité/service : Télécom SudParis / Département Réseaux et Services de Télécom (RST)

Poste du supérieur hiérarchique : Directeur du département RST

Catégories ou métiers des agents pouvant postuler : II - R / T

Catégorie et métier du poste dans le cadre de gestion IMT : II - P

Catégorie dans la fonction publique : A

CDD 12 mois

CONTEXTE ET MISSIONS :

SPARTA [1] est l'un des quatre projets-pilotes financés par la Commission Européenne pour devenir un Centre Européen de Recherche et de Compétences en Cybersécurité, et construire un Réseau de Compétences en Cybersécurité à travers l'Europe.

Dans le projet SPARTA, les projets de recherche et d'innovation sont financés au travers de 4 programmes, dont CAPE (Evaluation continue en environnements polymorphiques) qui s'intéresse en particulier à l'évaluation de la performance de la cybersécurité.
Dans CAPE, Télécom SudParis a pour objectif l'amélioration de l'évaluation des outils de cybersécurité tels que les systèmes de détection d'intrusion (IDS) et les systèmes de gestion d'information de sécurité (SIEM).

Un quadriciel est proposé qui regroupe un ensemble d'outils et un jeu de métriques pour générer différents types de trafic afin de réaliser divers tests :

- trafic légitime synthétique pour fournir un environnement de test réaliste sans menacer l'intimité numérique (privacy)
- trafic légitime/malveillant amorcé à partir de traces existantes avec la capacité d'appliquer diverses transformations au trafic obtenu afin de générer une variété de trafics différents et accroître la taille du jeu de données
- trafic adverse synthétique avec la capacité de contourner la détection

Par ailleurs, l'apprentissage adverse [2] (en particulier, les réseaux génératifs adverses (GAN) [3]) peuvent être exploités pour améliorer le système de sécurité testé, que ce soit ses capacités de détection (IDS) ou de corrélation (SIEM). Nous sommes particulièrement intéressés par la génération de trafic qui puisse applicquer une forte pression sur les systèmes de sécurité étudiés. Les outils existants manquent souvent de réalisme [4].
Le trafic généré doit comporter des caractéristiques soit légitimes ou soit malveillantes. Dans ce dernier cas, il est intéressant d'aller au-delà de la malveillance et d'essayer de tromper le système de sécurité étudié à travers des attaques imitatrices (mimicry) [5]. Pour générer un tel trafic, il est nécessaier de trouver un compromis entre plusieurs métriques concurrentes, parfois difficilement conciliables [6]. En général, l'amélioration des systèmes de sécurité étudiés devra viser à optimiser de multiples objectifs. Pour les IDS et les SIEM, ces objectifs ne sont pas toujours bien pris en compte par les outils d'évaluation [7].

[1] SPARTA; https://sparta.eu/
[2] L. Huang et al.: *Adversarial machine learning*, 4th ACM Workshop on Security and Artificial Intelligence, 2011.
[3] I. Goodfellow et al.: *Generative Adversarial Nets*, Advances in Neural Information Processing Systems 27, 2014.
[4] P.M. Bajan et al.: *Methodology of a network simulation in the context of an evaluation: application to an IDS*, 5th International Conference on Information Systems Security and Privacy, 2019.
[5] J.E. Tapiador & J.E. Clark: *Masquerade mimicry attack detection: A randomised approach*, Computers & Security 30 (5), 2011.
[6] A. Motzek et al.: *Selection of pareto-efficient response plans based on financial and operational assessments*, EURASIP Journal on Information Security 2017 (1), 2017.
[7] S. Axelsson: *The base-rate fallacy and the difficulty of intrusion detection*, ACM Transactions on Information and Systems Security 3 (3), 2000.

ACTIVITES :

Les activités tournent autour de l'évaluation de solutions IDS/SIEM, basés ou non sur l'apprentissage machine ou l'apprentissage profond [8], incluant les méthodologies, métriques et outils existants.

Ces activités incluent mais ne sont pas limitées à :

- état de l'art de la détection d'intrusion et de la corrélation d'alertes et leurs méthodologies d'évaluation, notamment en ce qui concerne la robustess
- conception de métriques évaluant la robustesse du modèle proposé
- méthode d'évaluation évaluant la robustesse des méthodes basés sur les GAN ou sur l'apprentissage profond face à des jeux de données de trafic assymétrique, en particulier utilisant des modèles génératifs pour la génération de trafics légitime et malveillant
- conception d'un modèle d'optimisation conciliant des objectifs multiples afin d'évaluer la robustesse d'un IDS ou d'un SIEM

[8] N. Shone et al.: *A deep learning approach to network intrusion detection*, Transactions on Emerging Topics in Computational Intelligence 2 (1), 2018.

FORMATION ET COMPETENCES :

Niveau de formation et/ou expérience requis :
-Doctorat

Compétences, connaissances et expériences indispensables :

- Connaissances en informatique dans l'un des domaines suivants: sécurité réseau OU intelligence artificielle / apprentissage statistique et une expérience intéressante dans l'autre domaine
- Une expérience à l'international (projet collaboratif) serait un plus

Capacités et aptitudes :
- Esprit d'équipe
- Autonomie
- Confidentialité

POUR CANDIDATER :

Merci de transmettre avant le 13 mars 2020, une lettre de motivation et un CV à :
- recrutements@imtbs-tsp.eu
Ou
- TELECOM SudParis – DRH – 9 rue Charles Fourier – 91000 EVRY

Personne à contacter : Grégory BLANC, gregory.blanc@telecom-sudparis.eu

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

Information du candidat sur le traitement des données personnelles : https://bit.ly/2QeOZhl