2023-06014 - Post-Doctoral Research Visit F/M Explainable and Extensible Machine Learning-driven Intrusion Detection System

Type de contrat : CDD
Niveau de diplôme exigé : Thèse ou équivalent
Fonction : Post-Doctorant
Niveau d'expérience souhaité : Jeune diplômé

A propos du centre ou de la direction fonctionnelle

The Inria Centre at Rennes University is one of Inria's eight centres and has more than thirty research teams. The Inria CentRE is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Contexte et atouts du poste

Inria CIDRE team (https://team.inria.fr/cidre/) is hiring one postdoctoral researcher at Rennes with a strong background on the research and practices of Machine Learning-driven Cyber Security. This project will be collaborated with Inria RESIST team ant Nancy (https://team.inria.fr/resist/). This post-doctoral position is part of the ANR PEPR Superviz project, in which Inria is responsible for on AI-driven intrusion detection / classification

Previous practices of Machine Learning (ML)-driven intrusion detection systems (IDS) suffer from two bottlenecks. First of all, the attack behaviors evolve persistently. New attack techniques / campaigns emerge and may change drastically the malicious payloads that recorded in the data, e.g., system logs or network traffics. Such change over malicious behaviors can lead to failure of Machine Learning-driven intrusion detection. Second, beyond evaluating the detection accuracy, it is interesting to understand the decision logics learned by the intrusion detection model. Current practices of ML-based intrusion detection methods depend heavily on black-box prediction models. It is therefore difficult to the owner of IDS to assess and identify potential bias in the detection output.

Therefore, the goal of this post-doctoral position is twofold. We will first focus on developping fast and adaptive ML methods that can detect and update the model to cope with the variation of attack behaviors. Furthermore, we expect the trained detection model to be interpretable. It can evaluate the informativeness of attributes in security reports. It can reveal the causal relationship between these raw attributes and the detection and classification results.

The post-doc researcher will be hosted at Rennes and may be required to travel to work with RESIST team regularly. Travel expenses will be covered within the limits of the scale in force.

Mission confiée

Assignments :
With the help of the researchers at CIDRE and RESIST team, the recruited person will be taken to conduct research in two perspectives. We aim first to provide transferable ML-based intrusion detection systems. In this study, the ML-based intrusion detection model should be designed to be easily adapted to different network traffic data sources without relearning from scratch. For example, we first train an intrusion detection model using network traffics from some attack campaigns from CIC-IDS-2018 [1]. After that, we want to identify the optimal hyperparameters or the optimal detection model using a few network flows of the other attack campaigns of the same dataset. The adapted model should achieve accurate detection over the other attack campaigns during test. In this sense, the designed ML-based detection model can be flexibly reused without the intense retraining cost in different network intrusion detection applications. Potential Machine Learning methodologies, e.g. meta learning [2] or transfer learning [3], could be useful to achieve fast adaption of the intrusion detection methods across different data sources, or across the drift of attack behaviours.

In a further step, we will also focus on providing interpretable intrusion detection algorithms. The expected ML-driven intrusion detection model should automatically discover malicious payload signatures and attack behaviors from network traffic data. These ML-generated signatures can help understand the process of stealth attacks, such as APT attacks, and make the decision of ML-based detection models more reliable compared to black box ML models. In this respect, we plan to explore if the popular examplanable methods, e.g. Shapley value [4] or LIME [5] could be applied to interpret the detection logics and highlight the important attributes of cyber attack behaviours.

[1] https://www.unb.ca/cic/datasets/ids-2018.html

[2] Chelsea Finn, Pieter Abbeel, Sergey Levine (2017). “Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks” arXiv:1703.03400

[3] Jeeyung Kim, Alex Sim, Jinoh Kim, Kesheng Wu, and Jaegyoon Hahm. 2020. Transfer Learning Approach for Botnet Detection Based on Recurrent Variational Autoencoder. In Proceedings of the 3rd International Workshop on Systems and Network Telemetry and Analytics (SNTA '20).

[4] https://shap.readthedocs.io/en/latest/

[5] https://github.com/marcotcr/lime

Informations générales

- **Thème/Domaine :** Représentation et traitement des données et des connaissances
  Statistiques (Big data) (BAP E)
- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2023-06-01
- **Durée de contrat :** 1 an
- **Date limite pour postuler :** 2023-04-30

Contacts

- **Equipe Inria :** CIDRE
- **Recruteur :**
  Han Yufei / yufei.han@inria.fr

A propos d'Inria

Inria est l’institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3500 scientifiques pour relever les défis du numérique, souvent à l’interface d’autres disciplines. L’institut fait appel à de nombreux talents dans plus d’une quarantaine de métiers différents. 900 personnels d’appui à la recherche et à l’innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 180 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.

Consignes pour postuler

Please submit online : your resume, cover letter and letters of recommendation eventually

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.

Collaboration :
The recruited person will be in connection with Tthe members of the Inria team CIDRE and RESIST.

Responsibilities :
The person recruited will be in charge of pursuing and maintaining the contact between the team and help sync up the research progress over the topic with our external collaborators.

Principales activités

Main activities (5 maximum) :

- Co-development of extensible Machine Learning methods to deliver fast adaption of intrusion detection use across different attack behaviours, as well as across different data sources. In this study, we especially focus on network traffic flow-based intrusion detection.
- Preprocessing and measurement study of the proposed methods using publica datasets and network flows collected by the team members
- Development of explanable machine learning approaches to produce interpretations to the detection logics of state-of-the-art Deep Learning-based intrusion detection models.
- Maintaining regular interactions with the team members.
- Writing reports / papers.

Compétences

Technical skills and level required :

- Knowledge in intrusion detection systems. Previous experiences with network flow-based intrusion detection systems will be favored.
- Knowledge in semi-supervised Machine Learning / Meta Learning.
- Proficient in programming in python. Experience with programming using pytorch and GPU platform will be preferred.

Relational skills

- Good communications skills
- Reasonable presentations skills

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Possibility of teleworking (90 days per year) and flexible organization of working hours
- Partial payment of insurance costs

Rémunération

Monthly gross salary amounting to 2746 euros