Offre n°2022-05116

Post-Doctoral Research Visit F/M Correlation and Prediction models over Distributed Internet Security Sensors

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-Doctorant

Niveau d'expérience souhaité : Jeune diplômé

Contexte et atouts du poste

Each year, Inria launches a recruitment campaign for Postdoctoral (postdoc) positions, and a limited number of slots is reserved for the International Relation Department in order to support Inria international collaborations.

This year, projects to strengthen partnership with University of Waterloo are eligible.

The postdoc contract will have a duration of**12 to 24 months**. The default start date is November 1st, 2022and not later than January, 1st 2023. The Post-Doc will be recruited by one of the Inria centers in France but it is recommended that the time is shared between France and Canada.

This position is proposed by the RESIST team of the Inria Nancy Grand Est research lab in collaboration with the research team of Prof. Boutaba at the University of Waterloo in Canada. The offered position is located in Nancy but several mobility periods will be planned in Waterloo, Canada.

Mission confiée

Candidates for postdoctoral positions are recruited after the end of their PhD or after a first post-doctoral period: for the candidates who obtained their PhD in the Northern hemisphere, the date of the defence shall be later than 1 September 2020; in the Southern hemisphere, later than 1 April 2020.

In order to encourage mobility, the post-doctorate must take place in a scientific environment that is truly different from that of the PhD (and, if applicable, from the job held since the PhD); particular attention is thus paid to French or international candidates who obtained their doctorate abroad.

Principales activités

Predicting future cyber threats with reasonable lead-time and accuracy can give security practitioners sufficient time to prepare for upcoming major attacks. For example, these practitioners can increase network provisioning to deal with an upcoming major denial-of-service attack or purchase security insurance. These preventive measures can stop future attacks or at least reduce their impact.

Several predictions models have already been proposed as reviewed in [1]. In this paper, beyond the survey, the authors highlight three main levels with an increasing difficulty to have accurate models (perception, comprehension and projection) and that the models can benefit from the integration of multiple sources of data, possibly external and exogenous.

In this project, we aim at analyzing the correlations between two large-scale network security sensors but of different nature: a network telescope and a central repository of distributed IDSs (Intrusion Detection System) logs. On one hand, a network telescope or a darknet is an entire IP subnet collecting incoming traffic without sending any reply. It is thus completely passive and known to be efficient to monitor large scale network threats such as scans or DDoS attacks [2]. On the other hand, IDSs monitor real user traffic and emit alerts when suspect activities are detected. They are also passive but monitor real activities (including benign ones) and inspect complete connections.

Each type of sensor brings its own value individually and we are interested to assess how an external source of data such as network telescope can improve machine learning models to predict the next alerts an IDS would emit.

To achieve our goal, we continuously collect network telescope data at Inria in France and Zeek IDS logs at the University of Waterloo in Canada. The latter serves as a central repository for many institutions in Canada. Although in [9] the darknet was colocated with the real servers, our setup considers two independent vantage points. While the telescope cannot observe complex attacks or full attacks (single direction traffic as it is a sink hole), it can monitor large phenomena with a global impact on the Internet. We can thus expect that observations done in the darknet and in real attacks observed from the IDSs present correlations. Besides, an interesting research question is also to evaluate if the activity on a real network and its evolution in terms of alerts (from IDS logs) can be observed through a darknet located in another country.

The postdoctoral researcher will thus address the following research questions:

- What is the level of correlation between network telescope data and IDS logs?
- Can we predict darknet observations by considering alerts from IDS logs? The objective is to define a machine-learning model (for example using LSTM) over time series of darknet data (number of packets, number of packets per TCP port...) and include as inputs data from the IDS logs. An underlying question is how to represent these logs in a meaningful manner. Embedding techniques (e.g. autoencoders) will be considered.
- Can we refine the IDS alerts using darknet data? While the IDS logs can present uncertain data or false alerts, the objective is to refine the outputs of the IDS. This supposes to predict the impact of darknet observations into the attacks targeting networks protected by the IDSs.

1-2 research visits in the University of Waterloo in Canada will be planned for each year (between 1-2 months each) with the aim to refine the defined approaches and perfrom evaluations with local scientific experts. The first visit will be also helpful to discover and learn to use the platform in Waterloo.

[1] M. Husák, J. Komárková, E. Bou-Harb and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640-660, Firstquarter 2019, doi: 10.1109/COMST.2018.2871866.

[2] Coudriau, M., Lahmadi, A., & Francois, J. (2016, December). Topological analysis and visualisation of network monitoring data: Darknet case study. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.

[3] Richter, P., & Berger, A. (2019, October). Scanning the scanners: Sensing the internet from a massively distributed network telescope. In Proceedings of the Internet Measurement Conference (pp. 144-157).

Compétences

- Required knowledge: networking, network security, machine learning and their relative tools (tshark, scikit-learn, pandas, dask...)
- Languages: Shell, python and others are appreciated
- Fluent in english (writing and oral communication)

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

2653€ gross/month

Informations générales

- **Thème/Domaine :** Réseaux et télécommunications
  Système & réseaux (BAP E)
- **Ville :** Villers lès Nancy
- **Centre Inria :** Centre Inria de l'Université de Lorraine
- **Date de prise de fonction souhaitée :** 2022-11-01
- **Durée de contrat :** 2 ans
- **Date limite pour postuler :** 2022-07-17

Contacts

- **Équipe Inria :** RESIST
- **Recruteur :**
  François Jerome / jerome.francois@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 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 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 200 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.

L'essentiel pour réussir

Instruction to apply:

- Applications for the Inria International Relations Department reserved post-docs must be submitted through this platform jobs.inria.fr **before July 15, 2021** with the following documents:
- Completed summary sheet to be uploaded here:https://mybox.inria.fr/d/0012f24ad5484cfd8307/
- Research project including subject title, research program, work plan and planned visits, duration (between 12 and 24 months) and the desired starting date (default start date is November 1st, 2022 and not later than January, 1st 2023).
- Detailed CV with a description of the PhD and a complete list of publications with the two most significant ones highlighted.
- Motivation letter from the candidate.
- 2 letters of recommendation.
- Letters of support from the host Inria research team and from the host international partner.
- Copy of passport.

For more information:

Main scientific advisor: jerome.francois@inria.fr

Another contact: Feel free to contact postdoc-dri@inria.fr

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.

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.