



Offre n°2025-08654

**Doctorant F/H [Campagne Allocation
Région 2025] Génération Automatique de
Chaînes d'Attaque pour la Détection et la
Prévention des Vulnérabilités Logicielles
(F/H)**

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

Le centre Inria de l'Université de Lille, créé en 2008, emploie 360 personnes dont 305 scientifiques répartis dans 15 équipes de recherche. Reconnu pour sa forte implication dans le développement socio-économique de la région des Hauts-De-France, le centre Inria de l'Université de Lille entretient des relations étroites avec les grandes entreprises et les PME. En favorisant les synergies entre chercheurs et industriels, Inria participe au transfert de compétences et d'expertise dans le domaine des technologies numériques et donne accès au meilleur de la recherche européenne et internationale au bénéfice de l'innovation et des entreprises, notamment dans la région.

Depuis plus de 10 ans, le centre Inria de l'Université de Lille est situé au cœur de l'écosystème universitaire et scientifique lillois, ainsi qu'au cœur de la Frenchtech, avec un showroom technologique basé avenue de Bretagne à Lille, sur le site d'excellence économique EuraTechnologies dédié aux technologies de l'information et de la communication (TIC).

Contexte et atouts du poste

Dans le cadre d'un partenariat (vous pouvez choisir entre)

- non pertinent

L'objectif est de concevoir des méthodes, des techniques et des outils qui permettront la prévention des attaques de désérialisation dans les applications.

Des déplacements réguliers sont prévus pour ce poste ? Non

Mission confiée

Missions :

La personne recrutée sera amenée à : (1) développer une approche modulaire d'analyse de failles logicielles, (2) construire un outil dédié à la génération automatique des chaînes d'attaque via le fuzzing et la mutation et (3) étudier l'historique et la sémantique des changements de code pour la compréhension des attaques. Les prototypes seront développés en langage Pharo.

Pour une meilleure connaissance du sujet de recherche proposé :

Un état de l'art, une bibliographie, des références scientifiques sont disponibles à l'URL suivante, n'hésitez à pas à vous y connecter : <https://www.inria.fr/fr/evref>.

Collaboration :

La personne recrutée sera en lien avec les membres de l'équipe EVREF qui ont des compétences en analyse et qualité logicielle pour répondre aux défis définis dans cette thèse.

Responsabilités :

La personne recrutée a la charge de :

- Conduire des recherches originales en lien avec la problématique de détection des failles de sécurité dans le cadre de cette thèse.
- Effectuer une veille scientifique afin de se tenir informé des avancées dans le domaine d'analyse logicielle pour la détection des vulnérabilités.
- Réaliser des simulations et des analyses des attaques logicielles existantes afin de définir leurs comportements.
- Rédiger des articles scientifiques et présenter ses travaux lors de conférences nationales et internationales.
- Collaborer avec d'autres chercheurs de l'équipe EVREF et participer aux réunions de l'équipe et du groupe de travail GL au laboratoire.
- Participer aux réunions et activités de l'équipe (notamment les Sprints et présentations dans l'équipe EVREF)
- Rédiger et défendre sa thèse devant un jury à l'issue du travail de recherche.

Pilotage/Management :

La personne recrutée aura la responsabilité de :

- Gérer son projet de recherche en planifiant les différentes étapes de son sujet de thèse et en respectant les échéances.
- Coordonner les collaborations avec les autres chercheurs du domaine de sécurité logicielle et du partenaire industriel Berger-Levrault.
- Animer des réunions de suivi hebdomadaires avec les encadrants.
- Valoriser ses travaux en contribuant à la rédaction de livrables et de papiers scientifiques.

Principales activités

Principales activités :

- étude de l'état de l'art à propos des attaques logicielles, les techniques d'analyse statique/dynamique et du fuzzing
- analyse des attaques existantes et extraction de leurs comportements
- définition d'un modèle des attaques
- conception et évaluation d'une approche outillée de détection et de prévention des chaînes d'attaques (en utilisant le langage Pharo (www.pharo.org))
- rédaction des livrables et des rapports

Activités complémentaires :

- validation de l'approche proposée en analysant des attaques existantes et en se référant aux catalogues et bases de données des attaques (Mitre, NVD, etc.)
- expérimentation qualitative/quantitative du prototype développé
- diffusion des résultats devant des communautés du domaine de sécurité au niveau national (journées GDR par exemple) et international (conférences, journaux, etc.)

Compétences

Compétences techniques et niveau requis : programmation Objet, analyse statique de code

Langues : Français, anglais

Compétences relationnelles :

- Capacité à travailler en équipe : collaboration et interactions avec les membres de l'équipe EVREF et avec les chercheurs des groupes de travail en Génie Logiciel
- Facilité en communication orale et écrite : présenter ses travaux en réunions, conférences et articles.

- Adaptabilité et écoute active : intégrer les retours des encadrants et des collègues pour faire évoluer la recherche.
- Capacité à vulgariser les résultats obtenus à différents publics.
- Echanges avec des chercheurs du partenaire industriel Berger-Levrault.

Compétences additionnelles appréciées : capacité à organiser des journées thématiques autour de la sécurité logicielle au niveau de l'équipe et du laboratoire d'accueil.

Avantages

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

Rémunération

2200 € bruts mensuels entre octobre et décembre 2025

2300 € bruts mensuels à partir du 1er janvier 2026

Informations générales

- **Thème/Domaine** : Programmation distribuée et génie logiciel
Ingénierie logicielle (BAP E)
- **Ville** : Villeneuve d'Ascq
- **Centre Inria** : [Centre Inria de l'Université de Lille](#)
- **Date de prise de fonction souhaitée** : 2025-10-01
- **Durée de contrat** : 3 ans
- **Date limite pour postuler** : 2025-04-20

Contacts

- **Équipe Inria** : [EVREF](#)

- **Directeur de thèse :**
Polito Guillermo / Guillermo.Polito@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

Vous pouvez donner là, un portrait à "gros traits" du (de la) collaborateur(trice) attendu(e) : ce que vous voyez comme nécessaire et suffisant et qui peut associer :

- Expérience solide en analyse de code et en programmation.
- Bonne connaissance des méthodologies de recherche en sécurité logicielle.
- Maîtrise des langages de programmation Objet. Une connaissance du langage Pharo est valorisée pour ce poste.
- Une expérience en recherche (via un stage de recherche ou un projet de master, ou une publication scientifique) est un plus.
- Bon niveau en anglais.

Cette rubrique permet de compléter et alléger (réduire) la liste plus formelle des compétences :

- Esprit analytique et rigoureux.
- Autonomie et capacité à prendre des initiatives.
- Bonnes compétences en communication écrite et orale en anglais et en français.
- Aptitude au travail en équipe et aux collaborations avec des chercheurs du domaine et du consortium industriel du langage de programmation Pharo (<https://consortium.pharo.org>).
- Curiosité scientifique et motivation pour la recherche.

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

Merci d'envoyer votre CV et lettre de motivation.

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.