



Offre n°2020-02966

Ingénieur F/H Vérification formelle du protocole de vote électronique Belenios

Type de contrat : CDD

Contrat renouvelable : Oui

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Ingénieur scientifique contractuel

Niveau d'expérience souhaité : Jusqu'à 3 ans

Contexte et atouts du poste

Les équipes Pesto et Caramba développent un système de vote électronique, Belenios, qui assure à la fois la vérifiabilité du scrutin et le secret du vote. Ce système est utilisé chaque année dans plusieurs centaines d'élections. Des premières analyses de sécurité ont été effectuées sur ce protocole mais il n'a jamais bénéficié d'une modélisation formelle complète comme cela pu être le cas d'autres protocoles comme celui de Neuchâtel ou CHVote.

Mission confiée

Missions :

Avec l'aide de Véronique Cortier, la personne recrutée sera amenée à modéliser le protocole Belenios le plus finement possible (en prenant en compte tous les acteurs) et pour un maximum de propriétés. La vérifiabilité et le secret du vote seront bien entendu considérées mais si le temps le permet, nous étudierons comment modéliser et prouver des propriétés comme la résolution de disputes. Pour l'ensemble du modèle, l'outil ProVerif sera utilisé.

Principales activités

Principales activités (5 maximum) :

- modélisation formelle du protocole en ProVerif
- rédaction d'un rapport justifiant les choix de modélisation

Compétences

Compétences techniques et niveau requis : Master en informatique, avec une spécialisation en vérification formelle.

Langues : Français ou Anglais

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 (après 6 mois d'ancienneté) 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

Rémunération selon diplôme et expérience à partir de 2562€ brut mensuel.

Informations générales

- **Thème/Domaine** : Sécurité et confidentialité
Système & réseaux (BAP E)
- **Ville** : Villers lès Nancy
- **Centre Inria** : [Centre Inria de l'Université de Lorraine](#)
- **Date de prise de fonction souhaitée** : 2020-10-01
- **Durée de contrat** : 2 mois
- **Date limite pour postuler** : 2020-09-30

Contacts

- **Équipe Inria** : [PESTO](#)
- **Recruteur** :
Cortier Véronique / veronique.cortier@loria.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

Des compétences solides en vérification formelle de protocoles cryptographiques sont nécessaires pour ce poste. Ainsi, le candidat devra être déjà familier des outils type ProVerif, Tamarin, Scyther, Avispa, Maude-NPA ou équivalent et avoir réalisé des modélisations de protocoles à l'aide de ces outils. La connaissance d'un seul de ces outils est suffisante car elle permettra au candidat de se former rapidement à l'outil ProVerif.

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.