



2021-03845 - Doctorant F/H Andromak : The next gen on device ANDROID malware protection

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Recently graduated

About the research centre or Inria department

Le centre Inria Rennes - Bretagne Atlantique est un des huit centres d'Inria et compte plus d'une trentaine d'équipes de recherche. Le centre Inria est un acteur majeur et reconnu dans le domaine des sciences numériques. Il est au cœur d'un riche écosystème de R&D et d'innovation : PME fortement innovantes, grands groupes industriels, pôles de compétitivité, acteurs de la recherche et de l'enseignement supérieur, laboratoires d'excellence, institut de recherche technologique

Context

Android est de nos jours l'une des plateformes de premier choix pour propager les menaces de logiciels malveillants. Le taux d'infection sur les appareils Android est en constante augmentation, engendrée par une prolifération spectaculaire de logiciels malveillants.

De nos jours, il n'existe pas de solutions satisfaisantes pour arrêter la prolifération des logiciels malveillants sur les appareils Android. Cela constitue une menace grave pour toute entreprise. Un malware peut interrompre, désactiver des applications, récupérer des informations personnelles, usurper l'identité d'une personne, accéder à des informations sensibles, contrôler toutes les applications s'exécutant sur l'appareil des utilisateurs, et même surfacturer les utilisateurs à leur insu.

Les résultats pourront également être mesurés grâce à l'expérimentation.

Assignment

Le défi de cette thèse est de concevoir une nouvelle génération de protection anti-malware. L'analyse dynamique communément utilisée pour détecter des malware n'est à ce jour pas possible sur Android car cela a : (i) un impact trop important sur les ressources, et (ii) requiert d'avoir des privilèges d'administrateur sur l'appareil, ce qui n'est pas possible sur les périphériques ANDROID du commerce.

Nous souhaitons dans cette thèse adresser le problème sus-mentionné. Nous pensons que l'intégration d'une technique d'analyse dynamique directement sur les appareils ANDROID est la voie à suivre ; elle permet d'arrêter les menaces telles que les variantes de logiciels malveillants encore inconnues dès que possible, c'est-à-dire dès qu'un comportement est détecté comme suspect sans avoir identifié une signature particulière au préalable (c'est-à-dire dans les laboratoires des éditeurs d'antivirus)

Main activities

Notre objectif est donc de promouvoir un nouveau concept d'analyse de code dynamique basé sur l'inspection de code à la volée associé à des concepts de bacs à sable applicatifs basés sur la virtualisation d'application afin de permettre une surveillance efficace sans aucune altération du système d'origine, et sans requérir de privilèges administrateur tout en réduisant au minimum les modifications à appliquer aux applications Android.

La qualité des résultats obtenus se feront grâce à une publication des travaux dans des conférences de top niveau de rang A et A* tels que par exemple : Usenix Security, S&P, ESORICS, NDSS, DSN, EUROSYS, Usenix ATC.

Skills

Compétences techniques et niveau requis : Connaissance approfondie du noyau Linux, Android, ARM et ML

Langues : Anglais oral et écrit courant

Benefits package

- Restauration subventionnée
- Transports publics remboursés partiellement

Remuneration

Rémunération mensuelle brute de 1982 euros les deux premières années et 2085 euros la troisième année

General Information

- **Theme/Domain** : Distributed Systems and middleware
- **Town/city** : Rennes
- **Inria Center** : CRI Rennes - Bretagne Atlantique
- **Starting date** : 2021-09-01
- **Duration of contract** : 3 years, 1 month
- **Deadline to apply** : 2021-08-22

Contacts

- **Inria Team** : WIDE
- **PhD Supervisor** : Bromberg David / david.bromberg@irisa.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Instruction to apply

Merci de déposer en ligne CV, lettre de motivation et éventuelles recommandations

Pour plus d'information, contactez david.bromberg@irisa.fr ou francois.taiani@irisa.fr

Defence Security :

This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :

As part of its diversity policy, all Inria positions are accessible to people with disabilities.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.