Informations générales

- **Thème/Domaine :** Systèmes distribués et intergiciels
- **Développement web (BAP E)**
- **Ville :** Villeneuve d’Ascq
- **Centre Inria :** CRI Lille - Nord Europe
- **Date de prise de fonction souhaitée :** 01-10-2018
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 02-05-2018

Contacts

- **Équipe Inria :** SPIRALS
- **Recruteur :** Rouvoy Romain / roumain.rouvoy@inria.fr

Conditions pour postuler

**Instructions to apply:**

Candidates will be treated firstly with a complete file : CV + letter of motivation + one or more letters of recommendation + transcripts from previous years.

**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.
This Ph.D. will address the design and experimentation of collaborative strategies to protect users from browser fingerprinting. The Ph.D. student will therefore explore algorithmic and mathematical approaches to enhance users’ privacy, and is expected to empirically assess theoretical results with proof-of-concept tools. We are particularly interested in the use of advanced classification algorithms that will allow creating tight-knit groups of users that share the same fingerprint or similar fingerprints, as well as recommender systems to suggest configuration changes that improve privacy by decreasing fingerprint uniqueness. The goal of this Ph.D. project is to reduce the capacity of nowadays and upcoming browser fingerprinting techniques to uniquely identify browsers.

The objective of this Ph.D is to define and implement new strategies to protect against browser fingerprinting, in particular by reducing fingerprint uniqueness, while ensuring that the proposed solutions are acceptable by non-technical users.

**Principales activités**

**Main activities**

In order to do so, we propose to apply the following methodology:

1. Evaluate and classify the state of the art of browser fingerprinting techniques, including academic and those found in-the-wild (e.g., by reverse engineering commercial fingerprinting scripts and inferring their tracking strategies);

2. Evaluate the impact of current browser fingerprinting countermeasures. One of the ways to detect the presence of fingerprinting countermeasures is to look at inconsistencies they introduce in the fingerprint. Indeed, when these countermeasures alter attributes to spoof the browser’s identity, they may introduce impossible combination of attributes;

3. Model the distance between fingerprinted attribute values and between browser fingerprints.

4. Build a countermeasure that generates consistent fingerprints, and takes into account the strategies used by fingerprinters. One possible strategy to investigate would be to find users with similar fingerprints, and to apply minimal changes so that altered browser fingerprints look the same to fingerprinters.

5. Analyze the usability and the impact of the proposed countermeasure.

This Ph.D. builds upon our previous work, Blink [Laperdrix15], a countermeasure that relies on virtualization (virtual machines or containers) and random reconfiguration to break fingerprint linkability. Although effective against tracking, Blink’s has overhead has shown to be a deterrent to its use and a new approach is needed. This Ph.D. also benefits from our studies regarding fingerprint statistical analyses [Laperdrix16], as well as advanced machine learning techniques to track browsers over long periods of time [Vastel18].

**References**


[iovation] iovation, " Multifactor Authentication and Online Fraud Prevention Solutions ".

Compétences
Skills

The Ph.D. candidate will develop her/his skills in Web technologies, in particular Javascript. Moreover, the candidate will also develop skills in Python, as well as machine learning and statistical data analysis, among many other technologies.

As is a common practice in the Spirals research team, all source code is expected to be open sourced. The student should publish high-level academic papers, as well as participate in related open source communities. This should assist in the technological transfer from academic prototypes to industry-ready tools.

Avantages sociaux
Benefits

- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Sports facilities
- Flexible working hours

More information about Lille :
http://www.lille3000.eu/portail/
http://www.lillemetropole.fr/mel.html

Rémunération
Remunerating

The gross monthly salary is 1982€ for the 1st and 2nd year and 2085€ for the 3rd year.