by decreasing fingerprint uniqueness. The goal of this Ph.D. project is to reduce the capacity of
fingerprints, as well as recommender systems to suggest configuration changes that improve privacy
that will allow creating tight-knit groups of users that share the same fingerprint or similar
proof-of-concept tools. We are particularly interested in the use of advanced classification algorithms
approaches to enhance users’ privacy, and is expected to empirically assess theoretical results with
from browser fingerprinting. The Ph.D. student will therefore explore algorithmic and mathematical
developments for over 3 years. These datasets will leverage the study of browser fingerprint diversity and
infrastructure, and associated datasets we collected through the AmIUnique.org website and browser
extensions for over 3 years. These datasets will leverage the study of browser fingerprint diversity and
privacy, security and comfort, as it can be seen by the immense popularity of browser extensions, like
AdBlock and Ghostery, as well as new legislation concerning the use of cookies and tracking
technologies. However, a new threat to privacy that leaves no trace on users’ devices has emerged.
Browser fingerprinting [Eckerseley10, Laperdrix16] exploits modern web technologies, protocols and
APIs to uniquely identify users. The leaked data is stored on remote servers the user has no control
over it. Encryption does little to limit browser fingerprinting as it is performed by the website you
visit: it is not a sniffing nor man-in-the-middle attack. Moreover, browser fingerprinting is becoming
widespread [Englehardt16], and is used to complement or even replace cookies for tracking purposes.
And new research shows it can be used to track people for extended periods of time [Vastel18].
Browser fingerprinting is therefore an important threat to privacy.

Browser fingerprinting techniques evolve with the addition and depreciation of APIs, web standards
and new technologies. To protect users from long term tracking, we need countermeasures that can
easily be maintained to adapt to new fingerprinting vectors. To address as many users as possible, not
only effectiveness but also usability should be an important objective.

https://www.inria.fr/equipes/spirals

Assignment

Assignments:

Positioned in the context of online privacy and web tracking, this Ph.D. topic will focus on developing
effective browser fingerprinting countermeasures. The PhD will benefit from our fingerprint research
infrastructures, and associated datasets we collected through the AmIUnique.org website and browser
extensions for over 3 years. These datasets will leverage the study of browser fingerprint diversity and
the way fingerprints evolve over long periods of time.

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

General Information

- Theme/Domain: Distributed Systems and middleware
- Town/city: Villeneuve d’Ascq
- Inria Center: CRI Lille - Nord Europe
- Starting date: 2018-10-01
- Duration of contract: 3 years
- Deadline to apply: 2018-05-02

Contacts

- Inria Team: SPIRALS
- Recruiter: Rouvoy Romain / roomain.rouvoy@inria.fr

Conditions for application

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.

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.
nowadays and upcoming browser fingerprinting techniques to uniquely identify browsers.

The objectif 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.

**Main activities**

**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".

**Skills**

**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.

**Benefits package**

**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

**Remuneration**

**Remunerating**

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