Polytech network form for PhD Research Grants from the China Scholarship Council

This document describes the PhD subject and supervisor proposed by the French Polytech network of 14 university engineering schools. Please contact the PhD supervisor by email or Skype for further information regarding your application.

Supervisor information	
Family name	ETIEN
First name	Anne
Email	Anne.Etien@polytech-lille.fr
Web reference	http://www.lifl.fr/~etien/
Lab name	CRIStAL
Lab web site	https://www.cristal.univ-lille.fr/
Polytech name	Polytech Lille
University name	University of Lille
Country	France

PhD information	
Title	Designing Fingerprint Resistant Browsers
Main topics regards to CSC list (3 topics at maximum)	Software Security, Privacy, Software Engineering
Required skills in science and	Web programming, Software Engineering

Ph.D. proposal

Designing Fingerprint Resistant Browsers through Automated Configuration Testing

Supervisors

- *Anne* ***Etien*** (Associate professor, HdR, Polytech Lille)
- *Walter* **Rudametkin** (Associate professor, Polytech Lille)
- *Romain* **Rouvoy** (Professor, University of Lille)

Research teams

The Ph.D. student will join the Rmod (https://rmod.inria.fr) and Spirals (https://team.inria.fr/spirals) project-teams between the University of Lille and Inria, within the UMR CRIStAL Laboratory.

Contact : spirals-recrute@inria.fr

Université de Lille UMR CRIStAL Bâtiment M3, Université de Lille 1, 59655 Villeneuve d'Ascq – FRANCE	**Inria Lille - Nord Europe** Parc Scientifique de la Haute Borne 40, avenue Halley - Bat. B, Park Plaza 59650 Villeneuve d'Ascq – FRANCE

Scientific Context

Browsers and web technologies, such as HTML5, are redefining the limits of what web applications can do. At the same time, concerned web users are becoming aware of practices that jeopardize their privacy, security and comfort, as can be seen by the immense popularity of browser extensions like AdBlock and Ghostery, as well as new legislation concerning the use of cookies (e.g. GDPR). 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 collected data is stored on servers the user has no control over it. Encryption does little to limit fingerprinting because it is performed by the website you visit; it is not a sniffing nor man-in-the-middle attack. Moreover, it is becoming widespread [Englehardt16], 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]. This is an important threat to privacy.

Ph.D. Project

Positioned in the context of web security and privacy, this Ph.D. project will focus on numerous issues developers face when attempting to build browsers and browser extensions that respect users' privacy. This Ph.D. will benefit from our browser fingerprints dataset, collected through the AmIUnique.org website and browser extensions for over 4 years. The dataset will enable the study of fingerprints diversity, the way they evolve, as well as the impact of fingerprint countermeasures on collected fingerprints. This Ph.D. will focus on providing developers tools to reduce the fingerprintability of their products.

The objective of this Ph.D. is to provide tools to define and implement new techniques that assist developers in reducing the fingerprintability of their browsers and extensions. The main approach is to automate the testing and configuration processes, in particular to obtain browser fingerprints and calculate short and long-term fingerprintability through statistical analyses and machine learning techniques.

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

1. Evaluate and classify the state of the art of browser fingerprinting ;
2. Evaluate the state of the art of countermeasures used to circumvent browser fingerprinting ;
3. Build a fingerprint collection platform that can be integrated into the development process or a continuous integration server (can be based partly on the AmIUnique.org website) ;
4. Build a platform capable of automatically launching and fingerprinting browsers, such an approach can be based off of Blink [Laperdrix15] ;
5. Propose techniques for exploring browser and browser extension configurations in order to analyse the impact that browser personalization has on fingerprintability ;
6. Build a statistical analysis platform that allows for short-term and long-term fingerprintability analysis of browsers and/or their extensions (such work can be based off of FP-Stalker [Vastel18] and FP-Tester [Vastel18-2]) and provide automated reports through the CI server ;
7. Include the detection and analysis of browser fingerprint inconsistencies, particularly useful for building fingerprinting countermeasures (work can be based on [Vastel18-3]) ;
8. Apply the tools on a real-world browser, preferable Chromium, and use them to reduce it's fingerprint uniqueness (should test popular configurations), as well it's long-term trackability.

Skills Summary

The Ph.D. candidate should have a background in computer science. Knowledge in Web programming is desired. Experience in machine learning and statistical data analysis is a plus.

As is a common practice in the Rmod and Spirals research teams, 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.

Bibliography

[Eckersley10] P. Eckersley. "**How unique is your web browser?**". *Int. Conf. on Privacy Enhancing Technologies* (PETS'10).

[Englehardt16] S. Englehardt and A. Narayanan, "**Online tracking: A 1-million-site measurement and analysis**". *ACM SIGSAC Conf. on Computer and Communications Security* (CCS'16).

[Laperdrix15] P. Laperdrix, W. Rudametkin and B. Baudry. "**Mitigating browser fingerprint tracking: multi-level reconfiguration and diversification**". *Int. Symp. on Software Engineering for Adaptive and Self-Managing Systems* (SEAMS'15). https://hal.inria.fr/hal-01121108

[Laperdrix16] P. Laperdrix, W. Rudametkin, B. Baudry. "**Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints**". *IEEE Symp. on Security and Privacy* (S&P'16). https://hal.inria.fr/hal-01285470

[Vastel18] A. Vastel, P. Laperdrix, W. Rudametkin, R. Rouvoy. "**FP-STALKER: Tracking Browser Fingerprint Evolutions**". *IEEE Symp. on Security and Privacy* (S&P'18). https://hal.inria.fr/hal-01652021

[Vastel18-2] A. Vastel, W. Rudametkin, R. Rouvoy. **"FP-TESTER: Automated Testing of Browser Fingerprint Resilience"**. IWPE 2018 - Int. Workshop on Privacy Engineering, Apr 2018. https://hal.inria.fr/hal-01717158

[Vastel18-3] A. Vastel, P. Laperdrix, W. Rudametkin, R. Rouvoy. **"FP-Scanner: The Privacy Implications of Browser Fingerprint Inconsistencies"**. USENIX Security Symposium, Aug 2018. https://hal.inria.fr/hal-01820197