

Ludovic Barman

Current location: Lausanne, Switzerland. Willing to relocate.
Languages: Fluent in French/English (C2), B2 in German/Italian
Nationality: Swiss
Year of birth: 1992
Contact: firstname.lastname@protonmail.com



The information below is compressed to fit in one page. The extended version is available at <https://lbarman.ch>

Core skills: Research in security and privacy. General knowledge in networking and applied cryptography. Software development (Web/desktop). Preparing and delivering talks for various audiences. Project management.

Research: My thesis was about assessing the threat stemming from the metadata of encrypted network communications, and building systems (in Go) to protect against it. We built a VPN-like anonymous communication system for LANs and WLANs (similar to Tor, working at a smaller scale but with stronger guarantees), and a large-scale system for anonymous text messaging supporting millions of users and providing differential privacy.

Technologies: Go, Python. Previous experience with Front & Back-end Web development, (Typescript, JS, PHP, HTML/CSS, SQL), Scala, Java. Good knowledge of software development lifecycle (infra, testing, deployment).

Latest publications and projects:

- **Traffic-Analysis of Web Traffic** 2021
- **Rubato: Metadata-Private Messaging for Mobile Devices** 2021
- **Every Byte Matters: Traffic Analysis of Bluetooth Wearable Devices** 2021
L. Barman, A. Dumur, A. Pyrgelis, J-P. Hubaux, in IMWUT'21 (UbiComp)
- **Decentralized Privacy-Preserving Proximity Tracing** 2020
C. Troncoso et al. arXiv
- **PriFi: Low-Latency Metadata Protection for Organizational Networks** 2020
L. Barman, M. Zamani, I. Dacosta, A. Pyreglis, B. Ford, J-P. Hubaux, J. Feigenbaum, in PETS'20
- **Reducing Metadata Leakage from Encrypted Files and Communication** 2019
K. Nikitin, L. Barman, M. Underwood, W. Lueks, B. Ford, J-P. Hubaux, in PETS'19
- **Drand & LeagueOfEntropy.com: Provable Distributed Randomness** 2017
- **PriFi: A Low-Latency [...] Protocol for Local-Area Anonymous Communication** 2016
L. Barman, M. Zamani, I. Dacosta, B. Ford, J-P. Hubaux, J. Feigenbaum, in WPES'16
- **Mirror: Enabling Proofs of Data Replication and Retrievability in the Cloud** 2015
F. Armknecht, L. Barman, J-M. Bohli, G. Karame (NEC Laboratories), in USENIX Security '16
- **Privacy Threats and Practical Solutions for Genetic Risk Tests** 2015
L. Barman, E. Graini, J-L. Raisaro, E. Ayday, J-P. Hubaux, in GenoPri'15

Last positions & experience:

- **Research Intern at Cloudflare, London** 2020
I worked on QUIC, on Website fingerprinting and defenses.
- **Teaching assistant at EPFL** (part of the PhD program) *since 2015*
In particular, for the class "Information Security and Privacy", for which I rebuilt the infrastructure in favor of a more reliable setup with dockers, unit and integration tests, and Continuous Integration.
- **Intern (Master Project) at NEC Laboratories Europe, Heidelberg** 2015
I implemented and benchmarked a research project in Scala, later published at USENIX Security.
- **Committee member at Hacker EPFL** 2014
- **Web Developer at Sunergic SA** 2012-2014
I created a web application for monitoring Siemens solar panels, as well as a web application to enable clients to design a roof (through a graphical wizard) and estimate the expected efficiency and rentability. This application has been used by several partners of Sunergic and Romande Energie.

Education:

- PhD in Security and Privacy, EPFL. My advisors were prof. Jean-Pierre Hubaux and Bryan Ford 2021
- Bachelor + Master in Communications Systems at EPFL, with a 1-year exchange at NUS, Singapore 2015

I maintain a blog about technology/do-it-yourself projects at <https://lbarman.ch>, along with some demos of projects.