Marc Juárez Miró

Informatics Forum
10 Crichton St
Edinburgh
EH8 9AB
United Kingdom

Email: marc.juarez@ed.ac.uk
Phone: +44 01316502707
Website: mjuarezm.github.io
Google Scholar: Na1MX7EAAAAJ

EDUCATION

PhD — Engineering Science: Electrical Engineering, *summa cum laude*
KU Leuven, 2019

BSc, MSc — Mathematics (BSc) and Computer Engineering (BSc and MSc) dual study program
Universitat Autònoma de Barcelona, 2013

PROFESSIONAL EMPLOYMENT

2022– — University of Edinburgh, School of Informatics
Lecturer in Cyber Security and Privacy

2019-22 — University of Southern California, Department of Computer Science
Postdoctoral Scholar

2013-19 — KU Leuven, Department of Electrical Engineering
Researcher / Teaching Assistant

2018 — International Computer Science Institute (ICSI)
Summer Research Intern

2012-13 — Research Institute on Artificial Intelligence (IIIA-CSIC)
Software Engineer / Research Assistant

RESEARCH AREAS

Privacy; algorithmic fairness; adversarial machine learning; traffic analysis; web tracking

SELECTED PUBLICATIONS

2023 — J. Schoeffer, A. Ritchie, K. Naggita, F. Monachou, J. Finocchiaro, and M. Juarez. "Online Platforms and the Fair Exposure Problem Under Homophily." *37th AAAI Conference on Artificial Intelligence (AAAI'23), Vol. 37, No. 10, pp. 11899-11908.*

2023 — M. Juarez, S Yeom, and M. Fredrikson "Black-Box Audits for Group Distribution Shifts." *AAAI Workshop on Privacy-Preserving Artificial Intelligence. arXiv* (Sep 2022) 2209.03620 [cs.LG]

2022 — M. Juarez, and A. Korolova. "'You Can't Fix What You Can't Measure': Privately Measuring Demographic Performance Disparities in Federated Learning." *In the Proceedings of Machine Learning Research. Vol. 214: Algorithmic Fairness through the Lens of Causality and Privacy (NeurIPS)*, 2017.

2020 — S. Siby, M. Juarez, N. Vallina-Rodriguez, C. Diaz, and C. Troncoso. "Encrypted DNS ⇒ Privacy? A Traffic Analysis Perspective." In the *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, pp. 1–18. IEEE Computer Society.

2019 — P. Sirinam, M. Imani, M. Juarez, and M. Wright. "Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning." In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pp. 1928–1943. ACM.

2018 — R. Jansen, M. Juarez, R. Galvez, T. Elahi, and C. Diaz. "Inside Job: Applying Traffic Fingerprinting to Measure Tor." In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA (pp. 1–15). IEEE Computer Society.

2018 — V. Rimmer, D. Preuveneers, M. Juarez, T. Van Goethem, and W. Joosen. "Automated Website Fingerprinting through Deep Learning." In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA (pp. 1–15). IEEE Computer Society.

2017 G. Cherubin, J. Hayes, and M. Juarez. "Website Fingerprinting Defenses at the Application Layer." *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017(2) 186–203. Sciendo.

2016 M. Juarez, M. Imani, M. Perry, C. Diaz, and M. Wright. "Toward an Efficient Website Fingerprinting Defense." In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, Vol. 2, pp. 27–46. Springer.

2014 M. Juarez, S. Afroz, G. Acar, C. Diaz, and R. Greenstadt. "A Critical Evaluation of Website Fingerprinting Attacks." In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Scottsdale, AZ, pp. 263–274. ACM.

2013 G. Acar, M. Juarez, N. Nikiforakis, C. Diaz, S. Gürses, F. Piessens, and B. Preneel. "FPDetective: Dusting the Web for Fingerprinters." In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pp. 1129–1140. ACM.

PATENTS

2022 M. Juarez and A. Korolova. "Local Differentially Private Mechanisms to Measure Performance Demographic Disparities in Federated Learning" US 18/322,525

AWARDS AND HONORS

2020 SIGSAC Doctoral Dissertation Award, Runner-up.

2018 ACM CCS Best Paper Award finalist.

2018 Award for Outstanding Research in Privacy Enhancing Technologies, Runner-up.

2017 Deep Learning and Security Workshop Outstanding Presentation Award.

2017 ACM CCS Best Paper Award finalist.

2016 ESORICS Outstanding Paper Award.

2015 Award for Outstanding Research in Privacy Enhancing Technologies, Runner-up.

2015 FWO (Research Foundation–Flanders) PhD fellowship.

PROGRAM COMMITTEE MEMBERSHIPS

ACM Conference on Computer and Communications Security (CCS). 2023–Present

AAAI Conference on Artificial Intelligence (AAAI). 2023–Present

Proceedings of the Privacy Enhancing Technologies Symposium (PoPETs). 2018–Present

Financial Cryptography. 2020

GUEST LECTURES

2023 Guest lecture at the INCACrypto Summer School. Online.

2023 Guest lecture at the Summer School on Security and Privacy in the Age of AI. Leuven, Belgium.

2020 Keynote speech at the DPM and CBT workshops. Online.

2019 Guest lecture on Privacy and Machine Learning at the BSC, Brussels, Belgium

2019 Presentation at the International Committee of the Red Cross Workshop, Brussels, Belgium

2017 Invited lecture in the course on Privacy Enhancing Technologies of TU Wien, Vienna, Austria

2017 Seminar at the Computer Communications and Applications Lab, EPFL, Lausanne, Switzerland

2016 Guest lecture at the Secure Application Development course (SecAppDev), Leuven, Belgium

OTHERS

Member of the Tor Research Safety Board. 2020–Present

Scientific Board Member of the Eticas External Algorithmic Audits task force. 2021–Present

Member of the Mechanism Design for Social Good (MD4SG)Working Group. 2020–22