Federal University of Paraná
Computer Science
Brazil

fabricioceschin@gmail.com
Website: https://fabriciojoc.github.io/
LinkedIn: https://linkedin.com/in/fabricioceschin/

Fabrício José de Oliveira Ceschin, PhD Student

Education

Feb 2018 – Dec 2022 **Federal University of Paraná**
PhD, Machine Learning applied to Security
Curitiba, Paraná, Brazil

Feb 2016 – Feb 2018 **Federal University of Paraná**
MS, Machine Learning applied to Security
Curitiba, Paraná, Brazil

Feb 2012 – Dec 2015 **Federal University of Paraná**
BSc, Computer Science
Curitiba, Paraná, Brazil

Thesis

Fabrício Ceschin, David Menotti, André Grégio: *Need for Speed: Analysis of Brazilian Malware Classifiers' Expiration Date*. 02/2018, Degree: Master's Degree, Supervisor: André Grégio and David Menotti.

Research Experience

Feb – Mar 2020 **Visitor PhD Student**
The University of Waikato, School of Computing and Mathematical Sciences
Hamilton, Waikato, New Zealand.

Collaborative research in machine learning applied to cybersecurity, data streams, and development of algorithms for scikit-multiflow library.

May 2019 and Aug 2018 **Visitor PhD Student**
University of Florida, Department of Electrical and Computer Engineering
Gainesville, Florida, United States.

Collaborative research in machine learning applied to cybersecurity.

Professional Experience

Mar 2014 – Feb 2016 **C3SL – Scientific Computing Center and Free Software**
Full Stack Web Developer

May 2013 – Jan 2014 **ECOMP – Junior Computing Company**
Project Advisor

Awards, Grants & Competitions

Sep 2021	Competition: Machine Learning Security Evasion Competition (MLSEC) 2021, Attacker's Challenge – 1st Place, Defender's Challenge – 1st Place
Sep 2020	Competition: Machine Learning Security Evasion Competition (MLSEC) 2020, Attacker's Challenge – 1st Place, Defender's Challenge – 2nd Place
Sep 2019	Competition: Machine Learning Security Evasion Competition (MLSEC) 2019 – 2nd Place
Jan 2019	Grant: Enigma 2019 - Diversity Grant
Aug 2017	Award: Google Research Awards for Latin America

Journal Publications

Fabrício Ceschin, Heitor Murilo Gomes, Marcus Botacin, Albert Bifet, Bernhard Pfahringer, Luiz S. Oliveira, André Grégio. *Machine Learning (In) Security: A Stream of Problems. https://arxiv.org/abs/2010.16045.*

Marcus Botacin, Fabrício Ceschin, Ruimin Sun, Daniela Oliveira, André Grégio. *Challenges and Pitfalls in Malware Research. Computers & Security. Computers & Security, pp. 102287, 2021, ISSN: 0167-4048.*

Marcus Botacin, Fabrício Ceschin, Paulo de Geus, André Grégio. *We Need to Talk About AntiViruses: Challenges & Pitfalls of AV Evaluations. Computers & Security, pp. 101859, 2020, ISSN: 0167-4048.*

Fabrício Ceschin, Felipe Pinage, Marcos Castilho, David Menotti, Luiz S. Oliveira, André Grégio. *The Need for Speed: An Analysis of Brazilian Malware Classifiers. IEEE Security and Privacy Magazine 11/2018; 16(6):31-41., DOI:10.1109/MSEC.2018.2875369.*

Conference Proceedings

Gabriel R. Castanhel, Tiago Heinrich, Fabrício Ceschin, Carlos Maziero. *Taking a Peek: An Evaluation of Anomaly Detection Using System Calls for Containers. 2021 IEEE Symposium on Computers and Communications (ISCC), 2021, pp. 1-6.*

Fabrício Ceschin, Marcus Botacin, Gabriel Lüders, Heitor Murilo Gomes, Luiz S. Oliveira, André Grégio. *No need to teach new tricks to old malware: Winning an evasion challenge with xor-based adversarial samples. Proceedings of the 3rd Reversing and Offensive-Oriented Trends Symposium, Association for Computing Machinery, Vienna, Austria, 2020, ISBN: 9781450377751.*

Fabrício Ceschin, Marcus Botacin, Heitor Murilo Gomes, Luiz S. Oliveira, André Grégio. *Shallow Security: On the Creation of Adversarial Variants to Evade Machine Learning-Based Malware Detectors. Proceedings of the 3rd Reversing and Offensive-Oriented Trends Symposium (ROOTS) 2019. Association for Computing Machinery, Vienna, Austria, 2019, ISBN: 9781450377751.*