# Fabrício José de Oliveira Ceschin

Federal University of Paraná, Paraná, Brazil
Department of Informatics, Computer Science
Curitiba, PR 82590-300

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

## 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

Ceschin, Fabrício, Gomes, Murilo Heitor, Oliveira, Luiz S., Grégio, André. Machine Learning (In) Security: A Stream of Problems. Pre-Dissertation Project. Abril 2021. Advisors: André Grégio, Heitor Murilo Gomes, and Luiz S. Oliveira.

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* **University of Waikato, School of Computing and Mathematical Sciences**
Visitor PhD Student
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* **University of Florida, Department of Electrical and Computer Engineering**
Visitor PhD Student
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* | Machine Learning Security Evasion Competition (MLSEC) 2021, Attacker's Challenge – 1st Place, Defender's Challenge – 1st Place |
| *Sep 2020* | Machine Learning Security Evasion Competition (MLSEC) 2020, Attacker's Challenge – 1st Place, Defender's Challenge – 2nd Place |
| *Sep 2019* | 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 |

## Selected Publications

Ceschin, Fabrício, Pinage, Felipe, Castilho, Marcos, Menotti, David, Oliveira, Luis S, Gregio, André. The need for speed: An analysis of brazilian malware classifers. IEEE Security Privacy, 16 (6), pp. 31-41, 2018, ISSN: 1540-7993. 10.1109/MSEC.2018.2875369.

Giovanini, Luiz, Ceschin, Fabrício, Silva, Mirela, Chen, Aokun, Kulkarni, Ramchandra, Banda, Sanjay, Lysaght, Madison, Qiao, Heng, Sapountzis, Nikolaos, Sun, Ruimin, Matthews, Brandon, Wu, Dapeng Oliver, Grégio, André, Oliveira, Daniela. Online Binary Models are Promising for Distinguishing Temporally Consistent Computer Usage Profiles. IEEE Transactions on Biometrics, Behavior, and Identity Science. 10.1109/TBIOM.2022.3179206.

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

Ceschin, Fabrício, Botacin, Marcus, Gomes, Heitor Murilo, Pinagé, Felipe, Oliveira, Luiz S., Grégio, André. Fast & Furious: Modelling Malware Detection as Evolving Data Streams. Expert Systems with Applications. https://doi.org/10.1016/j.eswa.2022.118590. August 2022.

Botacin, Marcus; Ceschin, Fabricio; Sun, Ruimin; Oliveira, Daniela; Grégio, André. Challenges and pitfalls in malware research. Computers & Security, pp. 102287, ISSN: 0167-4048. 10.1016/j.cose.2021.102287.

Ceschin, Fabrício, Botacin, Marcus, Lüders, Gabriel, Gomes, Heitor Murilo, Oliveira, Luiz S., Grégio, André. No need to teach new tricks to old malware: Winning an evasion challenge withxor-based adversarial samples. Proceedings of the 3rd Reversing and Offensive-Oriented Trends Symposium, Association for Computing Machinery, Vienna, Austria, ISBN: 9781450377751. 10.1145/3433667.3433669.

Ceschin, Fabrício, Botacin, Marcus, Gomes, Heitor Murilo, Oliveira, Luiz S, Grégio, André. 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, Association for Computing Machinery, Vienna, Austria, 2019, ISBN: 9781450377751. 10.1145/3375894.3375898.

Castanhel, Gabriel R., Heinrich, Tiago, Ceschin, Fabrício, Maziero, Carlos. Taking a Peek: An Evaluation of Anomaly Detection Using System calls for Containers. 2021 IEEE Symposium on Computers and Communications (ISCC). 10.1109/ISCC53001.2021.9631251.