Ioan-Tudor Cebere

Email: tudorcebere@gmail.com **GitHub** **Twitter**
Phone: +40746571672 **Personal Webpage** **LinkedIn**

Research interests

Differential Privacy, Machine Learning, Privacy-Preserving Machine Learning, Privacy Enhancing Technologies, Adversarial Machine Learning

Education

Inria Lille, France
PhD in Computer Science 11.2022 – Present
Advisor: Aurélien Bellet.

Ecole Normale Supérieure de Lyon Lyon, France
MSc in Informatique Fondamentale (first class honours) 09.2021 – 07.2022
Advisor: Sonia Ben Mokhtar
Thesis: *Blackbox Membership Inference Attack via Memorization.*

Politehnica University of Bucharest Bucharest, Romania
BSc in Computer Science and Engineering 10.2016 – 07.2020
Supervisor: Matei Popovici
Thesis: *ROS simulator for Reinforcement Learning*

Work experience

Vector Institute, CleverHans Laboratory Toronto, Canada
Research Intern *10.2023 - 02.2024*
The goal of this internship is to better understand the privacy guarantees of differentially private SGD (DP-SGD). While DP-SGD is known to be tight in the standard threat model, we explore how DP-SGD performs in relaxed threat models via auditing and then try to theoretically ground the results, observing enhanced performance in the hidden-state threat model.
Reference: Nicolas Papernot

OpenMined, Syft Library Remote
Core Engineer *02.2020 - 12.2022*
Syft is a library that aims to make machine learning privacy-friendly. I contributed to a wide range of tasks, from improving the performance and security of the distributed learning stack to designing a tensor type that tracks the needed information to perform individual differential privacy using JAX.
Reference: Andrew Trask

Inria Lyon, France

MSc internship *02.2022 - 07.2022*

My thesis topic was to work on adversaries that exploit learning mistakes, turning misclassifications into low-cost membership inference attacks. The novelty of my thesis is that it designs a membership inference attack independent of the underlying target model, removing the need for expensive shadow models. The attack is time-efficient and suitable for privacy hypothesis testing.
Reference: Sonia Ben Mokhtar

UiPath Bucharest, Romania

Machine Learning Engineering intern *06.2019 - 09.2019*

I developed a recommendation system using a MultiVAE architecture for a Collaborative Filtering use case and engineered a document denoising tool for the internal OCR using cycleGANs.

Publications

Syft 0.5: A platform for universally deployable structured transparency
Adam James Hall, Madhava Jay, Tudor Cebere, Bogdan Cebere et al.
Distributed and Private Machine Learning (DPML), ICLR Workshop, 2021.

PyVertical: A Vertical Federated Learning Framework for Multi-headed SplitNN
Daniele Romanini, Adam J. Hall, ..., Tudor Cebere et al.
Distributed and Private Machine Learning (DPML), ICLR Workshop, 2021.

Honors and scholarships

Ampère Scholarship of Excellence 2021
1^{st} place PyTorch Summer Hackaton, Facebook 2020
1^{st} place, Machine Learning for Healthcare Contest, Cognizant 2019

Teaching experience

Undergraduate TA, Politehnica of Bucharest Spring 2020, Spring 2019
Functional and Logic Programming

Undergraduate TA, Politehnica of Bucharest Fall 2020
Formal Languages and Automata

Undergraduate TA, Politehnica of Bucharest Spring 2019
Numerical methods

Talks and tutorials

Syft 0.5: A platform for universally deployable structured transparency
Distributed and Private Machine Learning (DPML), ICLR Workshop, 2021
The Privacy Crisis
Politehnica University of Bucharest, 2022
Privacy Auditing & Privacy Amplifications
Inria Nord, Lille, 2023

Skills

Technologies

Proficient in: Python, PyTorch, JAX, Rust, Linux.
Familiar with: C, C++.

Concepts

Proficient in: Deep Learning, Differential Privacy, Privacy-Preserving ML.
Familiar with: Applied Cryptography, Statistical Learning.

Service and outreach

Reviewer

ICML 2023 (1 paper), NeurIPS 2023

Romanian Open Source Educational 03.2018 – present

Since March 2019 I am the president of ROSEdu, working on a set of projects for the Romanian open source community. Had an impact on over 2000 students by organising courses, talks and workshops, myself training over 200 students.
Reference: Razvan Deaconescu

OpenMined Research 12.2022 – present

Since December 2022, I have been leading the open-source research team of OpenMined, organizing monthly meetings, seminars, and reading groups on the topic of the privacy, security, robustness and fairness of Machine Learning models. I am a strong supporter of open-source communities and we have decided at OpenMined that such a group would benefit all people who would like to get a background in trustworthy machine learning.
Reference: Andrew Trask