Ayoub Benaissa

Algeria

✉ me@ayoub-benaissa.com | ⌂ ayoub-benaissa.com | youben11 | in ayoub-benaissa

Education

Ecole Supérieure en Informatique 08 Mai 1945 — *Sidi Bel Abbès, Algeria*

Master of Science - Computer Science — *Sep 2015 - July 2020*

My master thesis and final project was focused on applying homomorphic encryption in machine learning. We released an open-source library ”TenSEAL” within the OpenMined community to build machine learning models that can process encrypted data. We published our findings in the DPML workshop at ICLR 2021 (see publications).

Malek Ben Nabi — *Blida, Algeria*

Baccalaureate — *Sep 2012 - July 2015*

- **Option:** Technical Mathematics and Electrical Engineering Stream.
- **Rating:** Good, with 15,95 out of 20.

Experience

Zama — *Remote*

Software Engineer — *Mar 2021 - Present*

- Worked on building Concrete: a compiler that converts python programs into their Fully Homomorphic Encryption (FHE) equivalent. My main work was around defining MLIR dialects and lowering passes for the compiler, and implementing the runtime. I also contributed on making a great UX for the compiler frontend.
- Worked on a blockchain library that integrates the fhEVM (run encrypted operations in the blockchain) into different blockchain frameworks.
- Integrated the fhEVM into different blockchain frameworks including Polygon, Avalanche, and Ethermint
- Published developer content including video tutorials and blog posts
- Played a key role in implementing and maintaining our CI/CD pipeline

Apheris — *Remote*

Freelancer — *Oct 2020 - Dec 2020*

- Explored different PET that would fit their solution
- Compared different open-source libraries for SMPC/FHE and built a prototype for weight aggregation

OpenMined — *Remote*

Homomorphic Encryption Team Lead — *Aug 2020 - Feb 2021*

- Lead a team focused on applying homomorphic encryption in machine learning. My main role was to organize discussions and unify our direction as a team.

OpenMined — *Remote*

Core Developer — *Oct 2019 - Aug 2020*

- Worked as part of the crypto team to investigate the use of different privacy-preserving techniques in machine learning.
- Built and maintained TenSEAL, a library for working with tensors that are homomorphically encrypted (see publications).
- Mentored a talented engineer as part of Google Summer of Code to implement the BGV scheme in Python for an internal prototype.
- Made SMPC available through a simple and intuitive API by integrating Facebook CrypTen into PySyft.
- Worked on a library for private-set-intersection during the Covid-19 pandemic (see publications).

Sudo-root — *Algeria*

CTF Player — *Jun 2016 - Dec 2020*

- I participated in several international CTFs competitions with the team. My main role was to reverse engineer binaries (mostly ELF) to find exploitable bugs. I often followup with writing exploits using Python. I also did code reviews to find flaws in crypto implementations, but also broke some encryption schemes due to design weaknesses (that were made on purpose for the challenge). I also helped on other occasions to find vulnerabilities in webapps and medium-size networks.

Realistic Security — *Algiers, Algeria*

DevOps Engineer — *Feb 2019 - Dec 2019*

- My main role was to build a real-world infrastructure as a training lab for penetration testing students.

Docker, INC *Algeria*

DOCKER COMMUNITY LEADER *Aug 2018 - Dec 2020*

- As a Docker Community Leader in Algeria, my main role was to organize meetups around container technologies across the country, and also deliver workshop sessions.

SFIZER GLOBAL SOLUTIONS *Remote*

JUNIOR SOFTWARE ENGINEER *Sep 2018 - Dec 2018*

- I worked on designing and implementing a data analytics platform for clients. My main role in the implementation of the backend with Django, and the deployment of the product with Docker on an AWS.

Realistic Security *Algiers, Algeria*

TRAINEE *Sep 2018*

- I was mainly responsible for the setup of a server with virtualization and the deployment of a bunch of containerized applications.

Projects

TenSEAL

Dec 2019 - Dec 2021

- A library for doing homomorphic encryption operations on tensors. It provides ways for training and evaluating machine learning models on encrypted data.

CrypTen Integration into PySyft

Jan 2020 - July 2020

- Provides a new way for running efficient secure multi-party computation protocols in PySyft to manipulate neural networks on private data.

Malware Revealer

Feb 2019 - Sep 2019

- Malware Revealer is a malware classification framework, designed primarily for malware detection, it contains a modular toolset for feature extraction, as well as pre-trained models and a ready to use web API for making predictions.

Pneumonia Detector

Dec 2018 - Jan 2019

- A trained neural network that can diagnose Pneumonia on chest x-ray, wrapped by an easy to use web application. It was selected as the best healthcare project by Udacity and Facebook during the Deep Learning with Pytorch challenge.

OpenClass

Feb 2018 - June 2018

- OpenClass is a web app that promotes information sharing through organized workshops.

ESI Linux

Feb 2017 - June 2017

- ESI Linux is a Linux distribution made for ESI-SBA (Ecole supérieure en informatique 08 Mai 1945) students particularly, it provides all the necessary tools for their curriculum.

Publications

- TenSEAL: A Library for Encrypted Tensor Operations Using Homomorphic Encryption - ICLR 2021 DPML Workshop
- Asymmetric Private Set Intersection with Applications to Contact Tracing and Private Vertical Federated Machine Learning - NeurIPS 2020 PPML Workshop
- Syft 0.5: A Platform for Universally Deployable Structured Transparency - ICLR 2021 DPML Workshop

Certifications

LFD121: Developing Secure Software

THE LINUX FOUNDATION *Sep 2024*

Certified in Cybersecurity

ISC2 *Jul 2024*

Deep Learning Specialization

DeepLearning.AI on Coursera *Oct 2020*

CCNA Cyber Ops

Cisco *Oct 2018 - Oct 2021*

Machine Learning

Coursera *Sep 2018*

Deep Learning Nanodegree

Udacity *Apr 2019*

Deep Reinforcement Learning Nanodegree

Udacity *Nov 2019*

Skills

Machine Learning	Scikit-Learn, PyTorch
DevOps	Docker, Ansible
Programming Languages	Python, C/C++, Golang, Rust, X86 Assembly
Others	Git, MLIR, OpenTelemetry, KVM, Reverse Engineering (ELF and APK)
Languages	Arabic (Native), French (Fluent), English (Proficient)

Courses

- Algorithms, Object Oriented Programming, Language Theory and Compilation;
- Mathematical Analysis, Linear Algebra, Statistics;
- Embedded Systems, Electronics, Digital Logic, Computer Architecture and Organization;
- Operating Systems, Computer Networks, Relational Databases, Cryptography, Cyber Security;
- Software Engineering, Distributed Systems;
- Machine Learning, Deep Learning.

Awards

Community Leader Award

DockerCon 2020

Docker Community Leader Award *May 2020*

CSAW'19 CTF

Second place for "Sudo_root" at the Cyber Security Awareness Week, New York University Abu Dhabi. *Nov 2019*

HITB Abu Dhabi standoff 2019

Fourth place for "Sudo_root" at Hack in The Box Abu Dhabi Standoff competition. *Oct 2019*

Arab Regional CTF 2019

Second place for "Sudo_root" at the annual Arab Regional Capture the Flag competition organized by CyberTalents. *Sep 2019*

SecuriNets CTF

Third place for "Sudo_root" at the annual SecuriNets qualification Capture the Flag competition. *Mar 2019*

Deep Learning with Pytorch Challenge

Our project ”Pneumonia Detector” got selected by Udacity and Facebook as the best healthcare project. *Jan 2019*

Hacklab CTF

Fourth place for “Sudo_root” at the Hacklab Capture the Flag competition, ESGI Paris. *Mar 2018*

CSAW’17 CTF

Third place for “Sudo_root” at the Cyber Security Awareness Week, New York University Abu Dhabi. *Nov 2017*

Himayatic CTF

First for “Sudo_root” at the Himayatic Capture the Flag competition. *Oct 2017*

Major League Hacking - Local Hack Day

First place at the AutoBot13 programming competition organized by the Major League Hacking Local Hack Day. *Dec 2016*

Activities

- Participating in CTF competitions to learn and practice different skills related to cyber-security
- Since 2016, I have been an instructor at workshops on Docker, Machine Learning, Python Programming, Linux Binary Analysis and Exploitation, Cryptography and others.