Thibault MAHO

Researcher in Machine Learning Security

CONTACT:

Phone: +33 7 70 13 55 36
Mail: thibault.maho@gmail.com
Address: 170 rue de Chateaugiron 35000 Rennes (France)
Website: www.thibaultmaho.com

SUMMARY

Completing PhD in Machine Learning Security, featuring a notable research visit to Imperial College London via a doctoral school grant. Contributions to adversarial attack research highlighted by innovative work on transferability and robustness assessment. Published author and speaker at prestigious international conferences. Proficient in ML model creation and deployment, specializing in NLP and Computer Vision.

SKILLS

- Techniques:
  - Machine Learning
  - Natural Language Processing
  - Signal Processing
  - ML Security
  - ML Privacy
- Tools and Software:
  - GiT
  - Python
  - HTML / CSS
  - PostgreSQL
  - LaTeX
  - JAVA
- Language:
  - French (Native)
  - English

HOBBIES

- Running (marathon, trail, ultratrail)
- Road Cycling

EDUCATION

INRIA - Rennes (France) ***09/2020 - Present***

PhD on the Security of Machine Learning
Supervisors: Teddy FURON and Erwan LE MERRER
Subject: Input Space Exploration for the security of neural network models
Award: **Doctoral school funding granted for a research visit at Imperial College London**, United Kingdom.

Phelma - Grenoble (France) ***09/2014 - 07/2017***

Msc Degree
Msc in Signal and Image Processing, Programming, and Electronics.

Faidherbe - Lille (France) ***09/2012 - 07/2014***

Bsc Degree
Intensive study course preparing for the competitive entrance examinations to the French 'Grandes Écoles' (the top French and highly-selective institutions). Specialized in Mathematics and Physics.

WORK EXPERIENCE

INRIA - Rennes (France) ***09/2020 - Present***

PhD on the Security of Machine Learning

- Secured funding for a **5-month research visit at Imperial College London, collaborating with Seyed Mohsen Moosavi-Dezfooli in 2023**, resulting in a paper defining a new attack scenario for transferable attacks at ICCV 2023.
- Innovated a novel geometrically-based decision-driven black-box attack, highlighted at CVPR 2021.
- Introduction of an equitable assessment approach for evaluating neural network robustness inspired by physic.
- Develop a model fingerprinting technique employing unaltered images and leverage information theory.
- Delivered **lectures on information theory and video image compression** to second-year students at ESIR, an engineering school in Rennes, France.
- Shared insights through presentations at **esteemed national and international conferences** and seminars, such as **ICCV, CVPR**, ICIP, ICASSP, and GretSI.
- Contributed expertise as a **reviewer** for international conferences and journals, including ICASSP, ICIP, and T-IFS.

xBrain - Lille (France) and Menlo Park (US) ***03/2017 - 07/2020***

R&D AI Engineer

Engaged in the creation and deployment of Machine Learning and Deep Learning models. Contributed to diverse projects at the intersection of Natural Language Processing (NLP) and Computer Vision:

- Orchestrated the development of a text mining endeavor, resulting in the establishment of a search engine powered by k-Nearest Neighbors and Siamese Network methodologies. Data was extracted from a French law website.
- Undertook both unsupervised and supervised image classification projects utilizing banking data, showcasing proficiency in handling complex visual data.
- Executed the classification of banking-related mail using a blend of unsupervised and supervised techniques. Employed active learning techniques.

Demonstrated end-to-end project involvement, from initial development to the launch into production.

TEACHING AND MENTORING

ESIR Engineering School - Rennes (France) ***2021 - 2023***

Lecturer

- Lecture on Information Theory and Compression to second-year engineering students.
- Lecture given each year with 20 hours

La Banque Postal, L'envol - Grenoble (France) ***2016 - 2017***

Private Tutoring + Mentor

Mentor for high school students. Courses in Mathematics and Engineering Science

PUBLICATIONS

Thibault Maho, Teddy Furon, Erwan Le Merrer, *FBI: Fingerprinting models with Benign Inputs*, IEEE Transactions on Information Forensics and Security (T-IFS)

Thibault Maho, Seyed-Mohsen Moosavi-Dezfooli, Teddy Furon, *How to choose your best allies for a transferable attack?*, International Conference on Computer Vision (ICCV) 2023

Thibault Maho, Teddy Furon, Erwan Le Merrer, *SurFree: a fast surrogate-free black-box attack*, Computer Vision and Pattern Recognition (CVPR) 2021

Thibault Maho, Teddy Furon, Erwan Le Merrer, *Randomized Smoothing Under Attack: How Good is it in Practice?*, IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2022

REFERENCES

Teddy FURON - teddy.furon@inria.fr

- Director of Research at Inria, Rennes, France in Linkmedia Team
- Principal Investigator of the chair on *Security of AI for Defense Applications* (SAIDA)

Erwan LE MERRER - erwan.le-merrer@inria.fr

- Researcher at Inria, Rennes, France in WIDE team
- Leading the scientific council of the Société Informatique de France

Seyed Mohsen MOOSAVI-DEZFOOLI - seyed.moosavi@imperial.ac.uk

- Lecturer at Imperial College London, United Kingdom