Thibault MAHO

Chercheur en Machine Learning

CONTACT:

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

RÉSUMÉ

Actuellement doctorant à l'Inria sur le domaine de l'IA et de sa sécurité, je souhaite aujourd'hui les mettre à profit, et sans cesse continuer à les développer.

COMPÉTENCES

- Techniques:
  - Machine Learning (ML)
  - Natural Language Processing
  - Signal Processing
  - ML Security
  - ML Privacy
- Outils:
  - GiT
  - Python
  - HTML / CSS
  - PostgreSQL
  - LaTeX
- Personel:
  - Capacités d'Analyse
  - Curiosité
  - Autonomie
  - Adaptabilité
- Language:
  - Français (Native)
  - Anglais

LOISIRS

- Running (marathon, trail, ultratrail)
- Cyclisme

FORMATION

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

Doctorat sur la Sécurité du Machine Learning

Superviseurs: Teddy FURON and Erwan LE MERRER
Sujet: Input Space Exploration for the security of neural network models
Récompense: Financement par l'école doctorale pour une visite de recherche à l'**Imperial College London, Royaume-Uni.**

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

Diplôme d'ingénieur

Spécialisé en Traitement d'images, Programmation, et Electronique

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

Classe Préparatoire

Spécialisé en Mathématiques et Physiques.

EXPÉRIENCE PROFESSIONNELLE

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

Doctorat sur la Sécurité du Machine Learning

- **De nombreux axes de la sécurité étudiés**: exemple adversaires, transférabilité, empreinte de réseaux, extraction de modèles, ...
- Obtention d'une bourse pour une visite de recherche de **5 mois à l'Imperial College London en 2023**. Résultat: article sur les attaques par transférabilité à ICCV 2023.
- Innovation d'une approche géométrique dans le cadre d'une attaque réaliste, présentée à CVPR 2021.
- Création d'une méthode d'empreintes de modèles utilisant des images non modifiées couplées à la théorie de l'information.
- Enseignement de la théorie de l'information et de la compression d'images et vidéo à l'ESIR, école d'ingénieurs à Rennes, France.
- Présentations de mes travaux dans des **conférences nationales et internationales** (**ICCV, CVPR**, ICIP, ICASSP, GretSI).
- Reviewer pour des conférences et revues internationales, tels que ICASSP, ICIP et T-IFS.

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

Ingénieur R&D en Intelligence Artificielle

Impliqué dans la création et le déploiement de modèles d'apprentissage automatique. Contribution à divers projets en Traitement du Langage Naturel (NLP) et Vision par Ordinateur :

- Développement d'outils de fouille de texte, aboutissant à un moteur de recherche alimenté par des méthodes de k-Nearest Neighbors et de Réseaux Siamois. Création d'un outil de scrapping d'un site web français de droit.
- Classification d'images non supervisée et supervisée avec des données bancaires
- Classification du courrier bancaire avec une combinaison de techniques non supervisées et supervisées. Utilisation du critère BIC pour évaluer le nombre de classes.

Implication totale dans les projets, de la phases de développement initial au lancement en production.

ENSEIGNEMENT

Ecole d'ingénieur ESIR - Rennes (France) ***2021 - 2023***

Cours Magistraux et TD

- Cours sur la Théorie de l'Information, la Compression Image et Vidéo.
- Dispensés à des étudiants en deuxième année d'école d'ingénieur pendant 3 ans.

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

Cours Particuliers et Mentorat

Mentorat pour Lycéens. Cours dispensé en Mathématiques et Science de l'Ingénieur.

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

RÉFÉRENCES

Teddy FURON - teddy.furon@inria.fr

- Directeur de Recherche à l'Inria, Rennes, France in Linkmedia Team
- Chercheur principal de la chaire *Security of AI for Defense Applications* (SAIDA)

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

- Chercheur à l'Inria, Rennes, France in WIDE team
- Dirige le conseil scientifique de la Société Informatique de France

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

- Lecturer à Imperial College London, Royaume-Uni