Jean-Charles Noirot Ferrand

M.S. Student

+1-608-217-5017 | jcnf@cs.wisc.edu | /jean-charles-noirot-ferrand | /jcnf0 | /jcnf.me

Summary

I am a M.S. Student in the School of Computer, Data, and Information Sciences at the University of Wisconsin-Madison. I am a research assistant in the MadS&P research group and advised by Prof. Patrick McDaniel. My research interests are centered around building more secure and trustworthy Machine Learning models. More specifically, my interests focus on foundation models and how they can securely interact with systems.

Education

M.S. in Computer Sciences | University of Wisconsin-Madison — Sep 2023 - Present
- Advisor: Dr. Patrick McDaniel

B.S. and M.S. in General Engineering | Ecole Centrale de Lyon — Sep 2021 - Present
- Multidisciplinary studies : Maths, Physics, Computer Science, Fluid Mechanics, Electrical Engineering, Economics, Management, etc.
- Specialization in Computer Sciences and Mathematics.

B.S. Mathematics and applications | Claude Bernard Lyon 1 University — Sep 2021 - August 2022
- Double degree with Ecole Centrale de Lyon.

Classe préparatoires aux grandes écoles | Lycée Marcelin Berthelot — Sep 2019 - July 2021
- 2-year intensive program preparing for the national competitive exams for entry to the top French Engineering Schools.
- Mathematics and Physics cursus, highest honors.

Experience

Research Assistant | University of Wisconsin-Madison — August 2023 - Present
Madison Security and Privacy Research Group (**MadS&P**)

Research Intern | Ecole Centrale de Lyon — May 2023 - July 2023
Laboratoire d'InfoRmatique en Image et Systèmes d'information (**LIRIS**)

Publications

Workshops/Journals

- Kunyang Li, Kyle Domico, **Jean-Charles Noirot Ferrand**, Patrick McDaniel. "The Efficacy of Transformer-based Adversarial Attacks in Security Domains". In *Workshop on Artificial Intelligence for Cyber (MILCOM 2023)*. 2023. **URL:** https://arxiv.org/abs/2310.11597

Projects

Research Project : Procedural content generation | Machine Learning — 2022-2023
Ecole Centrale de Lyon
- Review of the state-of-the-art procedural content generation : machine learning models such as autoencoders, generative adversarial networks, LSTM, etc.
- Creation and exploitation of a model to generate images using a music and its affect representation.

Study Project : Developing an application for the game Blokus — 2022-2023
Ecole Centrale de Lyon
- Development of an application in C# allowing to play Blokus with players or AI with different difficulties.
- Selected for the school's best study project prize (Francis Leboeuf prize) out of 90 study projects.

Professional Activities

External Reviewer

- ACM Conference on Computer and Communications Security (CCS) - 2024