

# Jean-Charles Noiroto Ferrand

M.S. STUDENT · COMPUTER SCIENCES

1210 W. Dayton Street, Madison, WI 53706-1613, USA

✉ [jcnf@cs.wisc.edu](mailto:jcnf@cs.wisc.edu) 🏠 <https://jcnf.me> 🎓 Jean-Charles Noiroto Ferrand

## Research Experience

---

### MadS&P - Security and Privacy Research Group at UW-Madison

*UW-Madison*

RESEARCH ASSISTANT

*2022 - Present*

- My research focuses on understanding the robustness of large language models

### LIRIS Laboratory, École Centrale de Lyon

*Centrale Lyon*

RESEARCH INTERNSHIP

*Summer 2023*

- Development of DESCRIPT, a tool for creating and visualizing stroke-based drawings

## Education

---

### University of Wisconsin-Madison

*Madison, WI, USA*

M.S. IN COMPUTER SCIENCES

*2023 - Present*

- Research at the intersection of adversarial machine learning and large language models.
- Advisor: Prof. Patrick McDaniel

### École Centrale de Lyon

*Lyon, France*

DIPLÔME D'INGÉNIEUR (M.S. AND B.S. IN ENGINEERING SCIENCES)

*2021 - Present*

- French Engineering School
- Multidisciplinary studies: Maths, Physics, Computer Science, Fluid Mechanics, Electrical Engineering, Economics, Management, etc.

### Claude Bernard Lyon 1 University

*Lyon, France*

B.S. IN GENERAL MATHEMATICS AND APPLICATIONS

*2021 - 2022*

- Dual degree during the first year at École Centrale de Lyon

### Lycée Marcelin Berthelot

*Saint-Maur-des-Fossés, France*

CLASSE PRÉPARATOIRE AUX GRANDES ÉCOLES (EQUIVALENT TO THE FIRST 2 YEARS OF B.S. IN ENGINEERING SCIENCES)

*2019 - 2021*

- 2-year intensive program preparing for the national competitive exams for entry to the top French Engineering Schools

## Publications

---

### CONFERENCES

- Kunyang Li, Kyle D Domico, **Jean-Charles Noiroto Ferrand**, and Patrick McDaniel. "The Efficacy of Transformer-Based Adversarial Attacks in Security Domains". In: *MILCOM 2023 - Workshop on Artificial Intelligence for Cyber (MILCOM 2023 - Workshop on AI for Cyber)*. Boston, USA, Oct. 2023, p. 6.

## Professional Activities

---

### REVIEWER - CONFERENCES

- 2025 **International Conference on Learning Representations (ICLR)**, External Reviewer
- 2025 **USENIX Security Symposium (USENIX Security)**, External Reviewer
- 2025 **IEEE Symposium on Security and Privacy (IEEE S&P)**, External reviewer
- 2024 **ACM Conference on Computer and Communications Security (ACM CCS)**, External Reviewer

### OTHER SERVICE

- 2024 **UW-Madison New CS Graduate Students Mentoring Program**, Mentor

# Skills

---

## COMPUTING SKILLS

**Languages** C, C#, Bash, Python, Matlab,  $\text{\LaTeX}$ , HTML, CSS, JavaScript, SQL  
**OS** GNU/Linux (Ubuntu), Windows  
**Softwares** Docker, Git, Gitlab

## LANGUAGE SKILLS

**French** Native  
**English** Fluent  
**Spanish** Intermediate  
**Chinese** Beginner