Stefan Trawicki

trawicki.io, London

Professional Experience

Founding Machine Learning Engineer: *Mindgard, October 2021 - Present*

- Deep-tech cybersecurity company currently valued at £10M+ in Canary Wharf, London
- First employee at inception: Launched the company with fellow PhDs, advisor
- Based the company on groundbreaking work conducted during our PhD studies
- Responsibilities: Large contributions to all engineering aspects; backend, frontend
- Specialize in the ML backend with a focus on adversarial machine learning
- Additional Activities: Authored and published articles on adversarial machine learning, providing educational sessions and mentorship on adversarial machine learning techniques

PhD Student, Secure ML Systems: *Lancaster University, 2021 - Present*

- Advisors **Chair Prof. Peter Garraghan** (Lanc.), **Dist. Prof. Neeraj Suri** (Lanc., Mass. @ Amherst)
- Thesis: **Exploring Vulnerabilities, Countermeasures and Practical Application of Adversarial Attacks on Deep Learning Systems**

Publications

Compilation as a Defense: Enhancing DL Model Attack Robustness via Tensor Optimization: *CAMLIS*, 2023

- Developed novel defense against Adversarial Machine Learning (AML) side-channel attacks using tensor optimization techniques, achieving up to 43% reduction in attack effectiveness.
- Explored the implications of tensor optimization for AML defenses and outlined directions for future research.

PINCH: An Adversarial Extraction Attack Framework for Deep Learning Models, 2022/2023

- Developed and deployed PINCH, an automated extraction attack framework to evaluate and analyze extraction attack scenarios across diverse hardware platforms.
- Conducted extensive experimental evaluations on 21 DL model architectures revealing key extraction characteristics, resilience factors, and the potential for further adversarial attacks.

Education

BSc Hons Computer Science, First Class: *Lancaster University, October 2018 - June 2021*

- First year *82.2%,* Second & Third year *80.8%* ***(first class)***

St Nicholas Catholic 6th Form: *September 2016 - June 2018*

- **A-Levels:** BBB in Computer Science, Mathematics and Physics (B in AS Economics)

Honors:

- **5th Highest Degree Score in Cohort (University)**, **Commendation of First Year Achievement (University)**, Best Computer Scientist (6th Form), Best Team/Stand/Presentation: Young Enterprise Regional (6th Form)

Other Experience

Operating Systems and Networking Teaching Assistant: *Lancaster University*

- Operating systems, networking and building big data systems modules.

Decentralised Cloud Gaming Engine- AI Profiling and Integration: *2018*

- Assess practicality of decoupled pathfinding subsystem, contrasting current monolithic engines.
- Complex concepts such as pathfinding, performant serialization, profiling and concurrency.