Jonathan Evertz

Machine Learning Security & Software Engineering

Researcher and PhD candidate at CISPA Helmholtz Center for Information Security with distinct team-oriented social skills. High interest in artificial intelligence and (adversarial) machine learning.

jonathan.evertz@rub.de

Bochum, Germany

jevertz.me

linkedin.com/in/jevertz

github.com/LostOxygen

SKILLS

Python | PyTorch | Object Oriented Programming | Large Language Models | Prompt Engineering | Tensorflow | OpenCV | Java | C++ | Systems Security

LANGUAGES

German
Native Proficiency

English
Full Professional Proficiency

Japanese
Elementary Proficiency

INTERESTS

Artificial Intelligence & Machine Learning | Linux | Arduino & RPI | Scientific Research | Swimming | Hiking | Photography | Cooking

EDUCATION

Master's Degree in Applied Computer Science
Ruhr University Bochum

04/2021 - 03/2024 — *Bochum, Germany*

Thesis

- Attacks and Defenses against the Confidentiality of Large Language Models *(Grade 0.7 / A+)*

Graduate Exchange Student
University of Tsukuba

10/2022 - 04/2023 — *Tsukuba, Japan*

Projects

- Organizing the international *CollaboTICS* workshop between Japan, France and Germany
- Received PROMOS scholarship from the German Academic Exchange Service (DAAD)

Bachelor's Degree in Applied Computer Science
Ruhr University Bochum

10/2017 - 03/2021 — *Bochum, Germany*

Thesis

- Data Poisoning based on Adversarial Attacks using Non-Robust Features *(Grade: 0.7 / A+)*

EXPERIENCES (EXCERPT)

PhD Student and Researcher
CISPA Helmholtz Center for Information Security

04/2024 - Present — *Saarbrücken, Germany*

Focus

- Machine learning security research in the domain of large language models

Research Assistant with Bachelor Degree
Horst Görtz Institute (Ruhr University Bochum) / CASA Cluster of Excellence

04/2021 - 03/2024 — *Bochum, Germany*

Tasks

- Adversarial machine learning research against deep neural networks for classification or large language models
- Deep learning based de-obfuscation methods using graph neural network

Student Assistant
Max-Planck Institute for Cybersecurity and Privacy

09/2020 - 03/2021 — *Bochum, Germany*

Tasks

- Hardware reversing of deep learning cores on Xilinx FPGA's to develop adversarial attacks on hardware level

Student Assistant
Chair of Production Systems (Ruhr University Bochum)

12/2018 - 08/2020 — *Bochum, Germany*

Tasks

- Development and optimization of open source software to automate the cabling process of switch cabinets in assembly lines using Raspberry Pi's and the OpenCV framework

VOLUNTEER EXPERIENCE

German Lifeguard Association (03/2009 - Present)
Lifeguard