+49 89 3229986-239
Berlin, Germany
franziska.boenisch@fu-berlin.de

Franziska Boenisch

Ph.D. Candidate (Computer Science)

GitHub: fraboeni
LinkedIn: fraboeni
https://franziska-boenisch.de/

Academic and Research Experience

Research Associate **09 2019 — present**
Fraunhofer AISEC, Berlin, Germany

- Research on differential privacy, and privacy quantification and metrics in machine learning models
- Project management, project acquisition in public domain and industry, grant writing, student advising

Ph.D. Research Intern **07 2021 — 03 2022**
Vector Institute for Artificial Intelligence, Toronto, Canada

- Research on privacy attacks against federated learning
- Research on privacy attacks in various domains, and differential privacy

Student assistant at the BioRobotics Lab **02 2018 — 01 2019**
Freie University, Berlin, Germany

- Implementation of an object tracking for honey bee trajectories in Matlab
- Collaboration in different research papers in the field of bio robotics and self-driving autonomous cars

Undergraduate Research Intern **08 2016 — 09 2016**
Chung Cheng University, Chiayi, Taiwan

- Supported by the DAAD RISE-Scholarship
- Implementation of neural networks for food image classification

Student assistant at the Data Analytics Lab **02 2016 — 07 2016**
Fraunhofer FOKUS, Berlin, Germany

- Prototype development and implementation of demonstrators in the field of predictive maintenance
- Implementation of applications with Apache Spark and Apache Flink

Education

Ph.D. Candidate **03 2020 — present**
Freie University Berlin, Germany

- Research focus: Privacy Attacks against Machine Learning Models
- Advisors: Prof. Dr. Marian Margraf, Prof. Dr. Nicolas Papernot

M.Sc. Computer Science **10 2017 — 07 2019**
Freie University Berlin *(Final Grade: 1,0)*

- Thesis: "Differential Privacy: General Survey and Analysis of Practicability in the Context of Machine Learning"
- Advisor: Prof. Dr. Marian Margraf

Exchange Student **02 2019 — 07 2019**
Technical University Eindhoven, Netherlands *(Average 8.3/10)*

- Supported by the ERASMUS-Scholarship
- Relevant coursework: Artificial Intelligence, Statistics, Recommender Systems

B.Sc. Computer Science **04 2014 — 04 2017**
Freie University Berlin *(Final Grade: 1,2)*

- Thesis: "Feature Engineering and Probabilistic Tracking on Honey Bee Trajectories"
- Advisor: Prof. Dr. Tim Landgraf

Industry Internships

Undergraduate Intern **09 2015 — 02 2016**
Data Analytics and Infrastructures at Takeaway.com (Lieferando.de), Berlin, Germany

- Development of an ML classifier for prediction of allergens and additives from food descriptions
- Support in business analytic

Prizes and Honors

Fraunhofer TALENTA Start Scholarship, *Fraunhofer Society* 01 2020 — 12 2021
3^{rd} prize: Forum Junge Spitzenforscher, *German Industrial Research Foundation* 11 2020
German National Merit Foundation Scholarship, *Studienstiftung des deutschen Volkes* 04 2015 — 07 2019
Grace Hopper Celebration Travel Scholarship, *Hasso-Plattner-Institute* 09 2018
Taalunie Zomercursus Nederlands Scholarship, *Taalunie* 08 2018
DAAD RISE Research Scholarship, *DAAD (German Academic Exchange Service)* 08 2016 — 09 2016
Kulturweit Scholarship, *DAAD (German Academic Exchange Service)* 02 2013 — 02 2014
German Association of Mathematicians Higher Education Entrance Prize, *DMV (German Mathematical Society)* 07 2012

Teaching

Seminar *Trustworthy Machine Learning*, *Freie University Berlin* Summer 2022
Software Project *Privacy Evaluation of Machine Learning Models*, *Freie University Berlin* Summer 2021
Teaching Assistant in *Security Protocols and Infrastructures*, *Freie University Berlin* Winter 2020
Seminar *Machine Learning and IT-Security*, *Freie University Berlin* Summer 2020
Seminar *Hello brand new data world*, *University of Bayreuth* Summer 2020
Teaching Assistant in *Security Protocols and Infrastructures*, *Freie University Berlin* Winter 2019
Lecture *ProInformatik VI: Python Programming for Female Students*, *Freie University Berlin* Summer 2018
Girl's Day Workshop *Program your own App*, *Freie University Berlin* Spring 2016, 2017, 2018

Publications

[1] Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, and Nicolas Papernot. When the curious abandon honesty: Federated learning is not private. *arXiv preprint arXiv:2112.02918*, 2021.

[2] Anvith Thudi, Ilia Shumailov, Franziska Boenisch, and Nicolas Papernot. Bounding membership inference. 2021. https://openreview.net/pdf?id=Mh40mAxxAUz.

[3] Franziska Boenisch, Reinhard Munz, Marcel Tiepelt, Simon Hanisch, Christiane Kuhn, and Paul Francis. Side-channel attacks on query-based data anonymization. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1254–1265, 2021.

[4] Franziska Boenisch. A systematic review on model watermarking for neural networks. *Frontiers in Big Data*, 4, 2021.

[5] Peter Sörries, Claudia Müller-Birn, Katrin Glinka, Franziska Boenisch, Marian Margraf, Sabine Sayegh-Jodehl, and Matthias Rose. Privacy needs reflection: Conceptional design rationales for privacy-preserving explanation user interfaces. *Mensch und Computer 2021-Workshopband*, 2021.

[6] Franziska Boenisch, Verena Battis, Nicolas Buchmann, and Maija Poikela. "I never thought about securing my machine learning systems": A study of security and privacy awareness of machine learning practitioners. In *Mensch und Computer 2021*, pages 520–546. 2021.

[7] Franziska Boenisch, Philip Sperl, and Konstantin Böttinger. Gradient masking and the underestimated robustness threats of differential privacy in deep learning. *arXiv preprint arXiv:2105.07985*, 2021.

[8] Christopher Mühl and Franziska Boenisch. Personalized pate: Differential privacy for machine learning with individual privacy guarantees. *arXiv preprint arXiv:2202.10517*, 2022.

[9] Tabea Kossen, Manuel Alexander Hirzel, Vince Istvan Madai, Franziska Boenisch, Anja Hennemuth, Kristian Hildebrand, Sebastian Pokutta, Kartikey Sharma, Adam Hilbert, Jan Sobesky, et al. Towards sharing brain images: Differentially private tof-mra images with segmentation labels using generative adversarial networks. *Frontiers in Artificial Intelligence*, page 85.

[10] Franziska Boenisch, Benjamin Rosemann, Benjamin Wild, David Dormagen, Fernando Wario, and Tim Landgraf. Tracking all members of a honey bee colony over their lifetime using learned models of correspondence. *Frontiers in Robotics and AI*, 5:35, 2018.

Students

Current Students

M. Nest	*(Practical Design of Privacy Attacks in Machine Learning)*	Master
I. Fendel	*(Membership Inference Attacks against Deep Neural Networks)*	Undergraduate
A. Meszaros	*(Taxonomy of Privacy Attacks in Machine Learning)*	Undergraduate

Past Students

M. Krüger	*(Application and Evaluation of Differential Privacy in Health Data Classification Tasks)*	Undergraduate	link to thesis
O. Bouanani	*(Neural Network Architectural Choices for Privacy)*	Undergraduate	link to thesis
C. Mühl	*(Personalizing Private Aggregation of Teacher Ensembles)*	Master	link to thesis
T. Känel	*(Practical Evaluation of Neural Network Watermarking Approaches)*	Undergraduate	link to thesis
D. Wang	*(Evaluating and Adapting Existing NN Watermarking Approaches to Online Learning)*	Undergraduate	link to thesis
D. Sosnovchyk	*(Evaluating Privacy of Synthetic Data Through Metrics)*	Undergraduate	link to thesis
W. Gu	*(Differential Private Synthetic Data Generation)*	Undergraduate	link to thesis
J. Ihrig	*(Privacy Quantification Methods for Private Aggregation of Teacher Ensembles)*	Master	link to thesis

Services and Volunteering

Organizer of Workshop Trustworthy AI in Science and Society at Informatik2022 conference	01 2022 — 09 2022
Reviewer for IEEE Symposium on Security and Privacy (IEEE S&P), ICLR PAIR2Struct Workshop	01 2022 — present
CyberMentor: Online mentoring for female high school students in computer science	03 2021 — present
Open Source Project: General Data Anonymity Score	09 2019 — 12 2020
MINToring: Mentoring of female high school students in computer science *Freie University Berlin*	04 2015 — 01 2019
Organizer of Summer School *ProInformatik VI: Python Programming for Female Students* *Freie University Berlin*	07 2019
Student Assistant of the Women's Representative (Physics Department), *Freie University Berlin*	01 2017 — 01 2018
Deputy Representative of Students in the Central Women's Council, *Freie University Berlin*	01 2016 — 12 2017
Kulturweit Voluntary Service, *German Consulate School Izmir, Turkey*	02 2013 — 02 2014
Student Representative, *Rückert High School, Berlin*	09 2010 — 07 2012