Andrea Siposova

✉ siposova.andrea@gmail.com ☎ +972 52 968 2068 ☎ +43 699 1823 6066 siposova-andrea in andreasiposova

Data Scientist with 6+ years of experience, specializing in AI security and privacy-preserving machine learning. My experience includes designing and executing complex experiments, and deriving insights for improving model security and data confidentiality. Proven ability in project management and collaboration with cross-functional teams to advance research and development initiatives. Holding a Master's degree in Data Science from Vienna University of Technology, with a thesis in the field of machine learning security.

Professional Experience

Machine Learning Researcher

Vienna, Austria

SBA Research Machine Learning and Data Management Group

Oct 2019 - April 2024

- Conducted systematic empirical studies to assess and enhance AI security and data confidentiality.
- Designed experiments evaluating trade-offs between attack and defense utility, model effectiveness and robustness.
- Developed 4 defense applications to integrate in a federated learning framework used across 3+ research projects.
- Authored 6+ reports and articles detailing the methodologies, results, and implications in machine learning security and adversarial ML, supporting both internal knowledge sharing and external publications. Contributed to project proposals.

Research Project Manager

Vienna, Austria

SBA Research Machine Learning and Data Management Group

October 2021 - April 2024

- Led a €800K climate research project over 2.5 years focusing on landslide risk assessment.
- Coordinated a multidisciplinary team of 15 experts resulting in solutions for landslide detection and susceptibility modeling.
- Led a technical work package on data harmonization and model fusion, increased the change detection precision by 18%, efficiency by ~20%.
- Contributed to the development of a data management workflow in the field of geo-sciences.
- Organized a workshop on data management strategies to equip stakeholders in enhancing reproducibility, and data reliability.
- Held focus groups to assess domain experts' needs and gather feedback for development.

Security Researcher

Vienna, Austria

Vienna University of Technology Data Science Group, Institute Of Information Systems Engineering

December 2023 - March 2024

European Defense Fund project focusing on Cyber Situational Awareness

- Conducted security assessments of federated learning systems to identify vulnerabilities and enhance data confidentiality.
- Designed proof-of-concept of defenses to safeguard sensitive data in a federated learning environment.
- Collaborated with partners in an international consortium consisting of 17 organizations from 11 countries.

Machine Learning Tutor

Vienna, Austria

Vienna University of Technology

September 2020 - January 2023

- Developed and structured comprehensive machine learning assignments, actively collaborating with faculty members.
- Conducted thorough assessment of over 500 student projects providing constructive feedback.

Machine Learning Researcher

Vienna, Austria

Vienna University of Economics and Business Research Institute for Computational Methods

September 2020 - January 2023

- Contributed to the development of object detection and image segmentation approaches.
- Played a key role in project management, overseeing the project timeline, deliverables, and resource allocation.
- Contributed to project reporting by ensuring accurate and timely documentation of research activities.

Research Intern

Vienna, Austria

ONDEWO

October 2017 - January 2018

- Collaborated on the development of a deep learning model for a conversational chatbot.
- Assisted in data preprocessing activities, participated in model building.
- Performed an analysis of model outcomes and documented the development process and findings.

Education

Master of Science (Dipl.Ing. / MSc.) - **Data Science**

Vienna, Austria

Vienna University of Technology

2019 - 2023

Diploma Thesis: Data Exfiltration Attacks and Defenses in Neural Networks

DOI: 10.34726/hss.2023.92803

- Simulated data exfiltration attacks on neural networks through intentional memorization in white-box and black-box scenarios.
- Conducted in-depth evaluation of attack effectiveness regarding various attack hyperparameters and evaluated attack vs. defense vs. model utility trade-offs.
- Designed and applied defense mechanisms, enhancing neural network security and robustness against exfiltration threats.
- Introduced a taxonomy of data exfiltration attacks in machine learning.

Thesis & Defensio grade: 100%, Coursework grade average: 89%

Bachelor of Science (BSc.) - **Information Systems**

Vienna, Austria

Vienna University of Economics and Business

2015 - 2018

Specializations: Data Science, Business Information Systems

Skills

Technical Skills:

Programming and Scripting: Python, R, SQL
Libraries: numpy, pandas, PyTorch, Tensorflow, scikit-learn, ONNX, matplotlib, seaborn
Versioning & Containerization: Git, Docker
Data Science Tools: Weights&Biases, MLFlow, Anaconda, Jupyter
Other: Linux, Latex, MS Office

Languages:

Slovak	-	native
English	-	full proficiency
German	-	full proficiency
Czech	-	full proficiency
Hebrew	-	intermediate proficiency

Articles

- **Advancing Data Management In Mountain Hazard Research: Strategies For Ensuring Data Quality And Enhancing Modeling Capabilities** Waltersdorfer, L., Siposova, A., Schlögl, M., Mayer, R., 2024. Interpraevent 2024, Vienna, Austria. Link.

- **Adopting FAIR data management practices in mountain hazard research: Strategies for ensuring data quality for landslide susceptibility modeling,** Waltersdorfer L., Siposova A., Schlögl, M., Mayer, R., EGU General Assembly 2024, Vienna, Austria. EGU24-18951, DOI: 10.5194/egusphere-egu24-18951

- **Datenexfiltration mit Hilfe von Modellen des maschinellen Lernens,** Siposova A., 2024, OCG Journal, Austrian Computer Society, 01:20-21. Link.

- **Supporting Landslide Disaster Risk Reduction Using Data-driven Methods** Siposova, A., Mayer, R., Schlögl, M. and Lampert, J., 2023. ERCIM NEWS-European Research Consortium for Informatics and Mathematics, 135:10-11. Link.

- **gAia: predicting landslides based on consolidated inventory data–bridging needs and limitations.** Lampert, J., Wernhart, S., Avian, M., Schlögl, M., Seewald, M., Jung, M.O., Kastner, R., Mayer, R. and Siposova, A., 2022, November. In Disaster Research Days 2022. 43-45. Link.

- **Generalized sparse convolutional neural networks for semantic segmentation of point clouds derived from tri-stereo satellite imagery.** Bachhofner, S., Loghin, A.M., Otepka, J., Pfeifer, N., Hornacek, M., Siposova, A., Schmidinger, N., Hornik, K., Schiller, N., Kähler, O. and Hochreiter, R., 2020. Remote Sensing, 12(8), p.1289. DOI: 10.3390/rs12081289