Szilvia Lestyán

Research Interests

Mathematician with a Ph.D. in Computer Science, a passion for Ethical AI, interested in the interconnectedness of biases of the mind and machine learning, moral agency in AI, and the ethical dimensions of biases.

Education

2022 **Ph. D. in Computer Science**
CrySyS Lab. Department of Networked Systems and Services
Budapest University of Technology and Economics, Budapest, Hungary
Thesis: *Privacy of Vehicular Time Series Data*
Advisors: Dr. Gergely Biczók, Dr. Gergely Ács
Summary: Devised methods of *re-identification* of drivers and *reverse engineering* of signals in car electronics data with *machine learning* methods; *anonymization* of location data of vehicles using *differential privacy* and deep learning models, analyzing it with several utility measures.

2016 **M. Sc. in Applied Mathematics**
Eötvös Loránd University, Budapest, Hungary

2013 **B. Sc. in Mathematics**
Eötvös Loránd University, Budapest, Hungary

Professional Appointments

2024 - **Postdoctoral Researcher**
INED, Paris, France
The goal of the project is to anonymize and measure the vulnerability of survey datasets with attention to ethical considerations and privacy questions.

2023 **Postdoctoral Researcher**
Comète**,** Inria Saclay, France
Participated in projects concerning: **membership inference attacks;** local **differential privacy**, **causal discovery** algorithms. Developed a good understanding of problems and solutions in: **causality**, **fairness, ethical AI.** **Orrganization of 2nd Ethical AI workshop.**

2017 -2022 **Research Assistant**
Budapest University of Technology and Economics, Budapest, Hungary,
Participated in 5+ research projects mainly focused on **security and privacy** applications or security and privacy in ML. **Taught** 2 full courses of security and privacy in machine learning and assisted in 4 other classes (11 courses in total)**. Tutored** 20+ students for independent projects.

2014 -2017 **Privacy Consultant**

Areus Infokommunikációs Zrt., Budapest, Hungary,
Designed, implemented and tested **data anonymization** solutions for banks and companies.

Publications

Binkyte R., Pinzón C., Lestyán Sz., Jung K., H. Arcolezi H., Palamidessi C., Causal Discovery Under Local Privacy, Causal Learning and Reasoning, CLEAR, 2024

Gazdag A., Lestyán Sz, Remeli M., Acs G., Biczók G., Holczer T., Privacy Pitfalls of Releasing In-Vehicle Network Data, Vehicular Communications, Elsevier, 2023

Lestyán Sz.,Acs G., Biczók G. In Search of Lost Utility: Private Location Data, Proceedings on Privacy Enhancing Technologies, 2022 **(A-ranked)**

Acs G., Lestyán Sz., Biczók G. Privacy of Aggregated Mobility Data. In: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg, 2021

Remeli M., Lestyán Sz., Acs G., Biczók G., Automatic Driver Identification from In-Vehicle Network Log. IEEE Intelligent Transportation Systems Conference (ITSC), 2019

Lestyán Sz., Acs G., Biczók G., Szalay Zs., Extracting vehicle sensor signals from CAN logs for driver re-identification; Proceedings of the 5th International Conference on Information Systems Security and Privacy, 2019

Lestyán Sz., Privacy Preserving Data Aggregation over Multi-hop Networks; Infocommunications Journal, pp. 7-15, December 2016, Volume VIII, Number 4, ISSN 2061-2079

Lestyán Sz., Privacy Preserving Distributed Maximum and Maximal Clique Algorithms; Vocal - Optimization Conference, Advanced Algorithms, Esztergom, 2016

Csiszárik A., Lestyán Sz., Lukács A., Efficient Apriori Based Algorithms for Privacy Preserving Frequent Itemset Mining; Cognitive Infocommunications (CogInfoCom), 2014

Talks

What can we learn from cognitive biases? - Talk on Workshop @ Comète on Ethical AI, Saclay, France 2022

Open discussions about research for high school girls, online, Hungary, 2020

Introduction of Privacy and Security Poblems - Talk on Girls` day at Budapest University of Technology and Economics, Hungary, 2017-2021

Introduction to Adversarial Examples - Talk on WITSEC Day (Women in IT Security), 2020

Differential Privacy in Practice - Talk on WITSEC Day (Women in IT Security), 2019

Panel Discussion on AI - ITBN (Day of IT Security), 2018

Research Experience

2024 - **Postdoctoral Researcher**
INED, Paris, France

2023 **Postdoctoral Researcher**
Comète, Inria Saclay, France

Projects:

ERC HYPATIA
Investigating the:
- application of quantitative information flow on measuring the power and bias of membership inference attacks;
- the trade-off between membership inference attacks, fairness and accuracy in a personalized federated learning setting;
- the effect of local and metric differential privacy on causal discovery algorithms.

2020-2022 **Research Assistant**
Budapest University of Technology and Economics, Budapest, Hungary

Projects:

2022 Artificial Intelligence National Laboratory
Investigating deep learning feature extraction techniques for data anonymization

2019 - 2022 FIKP - Artificial Intelligence for Smart Cities 2019-2022
Designing and implementing location data anonymization techniques with Differential Privacy and deep learning techniques

2018 - 2019 SECREDAS
Designing re-identification attacks for vehicular time series data

2018 EIT Digital
Investigating the re-identification of drivers using vehicular data using machine learning techniques

2017 -2019 EFOP 362
Investigating the in-vehicle Controller Area Network (CAN) protocol for reverse engineering using machine learning techniques

Teaching Experience

Machine Learning Security - planned and led a reading seminar together with Dr. Gergely Acs, where students processed academic papers on various subjects on security and privacy in ML, such as adversarial examples attacks and defenses, membership attacks, certified defenses etc.

Privacy-Preserving Technologies - held several lectures on anonymization techniques, such as anonymization of tabular data, location data and differential privacy

Introduction to Security – held lectures and small exercises on adversarial examples

Coding and Security - led laboratory exercises on the topic of cryptography, security and media encoding technologies

IT Security Laboratory - created exercises and led classes on Linux access security

In the course of 5 and a half years I had **supervised** 20+ students in their independent project exercises, topics included mostly adversarial examples and privacy problems. Many students continued their topic to a diploma project where I was their thesis advisor.

Languages

Hungarian - Native

English - Fully proficient (C2)

French – Intermediate-Advanced (B2-C1)

Russian – Conversational (B1)

Hobbies

Hiking, mountaineering – climbed several 3000+ meters high mountains in Europe, also some 4000+ meters, such as the Mont Blanc, Grand Paradiso, attempted Elbrus in Russia. Also completed several long trail hikes, such as the GR20 (200km), Tour de Mont Blanc (180km), Larapinta in the Australian outback (230km), the Kungsleden in Sweden (480km) and the Alta Via 2 in Italy (170km).