Dr. sc. ETH Zürich
David M. Sommer

Privacy and Security

- Born: May 1990 in Zürich
- Swiss and Italian Citizenship
- Languages:
  - Swiss-German: native
  - High-German: fluent
  - English: fluent
  - French: CEFR B1+
- Erdős number: 4

Skills

Data Protection and Data Privacy 5+ yrs.

data protection and anonymization methods, differential privacy, data regulation

Software Development 9+ yrs.

proficient: C, C++, Python. familiar: Java, JavaScript, Bash, R, MATLAB, ..

Cyber Security 4+ yrs.

secure protocols, secure systems, malware detection

Big Data/ Data Science/ Machine Learning 4+ yrs.

Tensorflow, Torch, scikit-learn, algorithms, applied statistics, applications, theory

System Adminstration 6+ yrs.

Linux server administration, networking, firewalls, OS-security

Web development 4+ yrs.

hml, css, WordPress, webserver, Ajax, JavaScript, tracking-technologies

Biography

I was always fascinated by complex systems and the abilty to tweak them. Inspired by computers, I taught myself to write programms early and I am running my own servers since then. After my highschool diploma (Swiss *Matura*), I studied Physics which gifted me with a deep and intuitive understanding of mathematical structures. During my studies, I worked on several projects as a programmer and system administrator, always focusing on IT-security. This passion was extended to data privacy and protection whit my PhD at ETH Zürich. Together with my engagement for civil rights, I acquired a strong technical background in IT-security and data protection combined with elaborate communication-skills.

Work experience

PhD at ETH Zürich **11/2015 - 10/2021**

System Security Group (Prof. Srdjan Capkun)
Department of Computer Science, ETH Zürich

Next to actively contributing to world-leading research, I also hold talks at conferences, assist in teaching, design exams, supervise student-theses, and peer-review academic publications.

Key-words: Anonymous communication protocols, privacy-preserving data processing, data protection protocols, differential privacy, Intel SGX, secure system design, secure authentication, security protocols, machine learning, security and privacy of machine learning

Visits abroad for research collaborations:

- Princeton University, USA, (Prof. Prateek Mittal) 02/2020 - 03/2020
  Department of Electrical Engineering.
- National University of Singapore, (Prof. Reza Shokri) 01/2018
  Data Privacy and Trustworthy Machine Learning Research Lab.

Attended summer schools

- Summer School on real-world crypto and privacy, twice 2016 & 2019
  Šhibenik, Croatia

Privacy Consultant for Sedimentum AG **12/2020 - today**

Sedimentum AG, Zug

Sedimentum AG provides a solution to alert clinical care-takers of health-care institutions about dangerous incidents of their stationized patients while complying with the strict medical privacy law of Switzerland. I counsel Sedimentum AG in the development of their lawful, privacy-preserving incident-detection and care-taker alarming protocol.

Engagement for Civil Rights **2017 - today**

Switzerland

Engagement in projects together with NGOs, mostly regarding digital transformation, sovereignty, and surveillance.

Activities include (not exhaustive):

- NGO "Digitale Gesellschaft Schweiz" 2020 - today
  Active Member
- Event series "Digitale Selbstverteidigung Basel" 2018 - today
  Co-chair Organisational Committee (Mitglied im Organisationskomitee)
- Organising "Reclaim Democracy Congress 2020" (Switzerland) 2017 - 2020
  Chair Sub-Committee with focus "Digital Transformation"
- Lange Nacht der Kritik Basel 2018 & 2019 2018 - 2019
  Editorial Board Member (Mitglied im Organisationskomitee)

Education

08/2013 - 05/2015

M.Sc. ETH in Physics

ETH Zürich

Specialised in computational and theoretical solid state physics.

Master's thesis: "Competitive and Random Fragmentation of Trees.".

Semester thesis: "Probability Density Function Estimation: Bayesian Approach."

08/2010 - 07/2013

B.Sc. ETH in Physics

ETH Zürich

Participated in "Astrowoche 2013," measuring light polarization patterns of celestial nebulae.

08/2006 – 12/2009

Swiss Matura (highschool)

Gymnasium Münchenstein

Math ▪ Physics ▪ Chemistry

Participated in world championship for Robotic Soccer ("Robocup" 2009 in Graz).

Thesis (Maturarbeit): Programming an automated Sudoku solver.

Interests

- Guitarist
- DIY
- Electronics
- Reading
- Cooking
- Travel

Contact

david_sommer@breitband.ch

github.com/sommerda

Internship: Private ML Team at Apple Inc. **03/2020 - 07/2020**

Private Machine Learning Team
Apple Cambridge, UK

Development and implementation of a privacy-preserving (differentially private) statistics aggregation protocol within the paradigm of federated learning, that ensures personal data remains on the initial smart devices only.

Mandatory Army Service in Switzerland **2010 - 2017**

EKF-Rekrutenschule in Jassbach, then Bern

While in service, I worked as a developer in IT-security and analysis, together with civil employees at the headquarters in Bern to which I returned annually for the regular repetition courses (WK).

Freelance-Developer for Security Systems **2011 - 2016**

Sommer Securities (Self-Employed)

While studying for my Bachelor's degree, I worked as an independent developer improving security systems for multiple companies, including *armasuisse*.

IT-Administration for Dr. Med. C. Hollenstein **2008 - 2016**

Office in Laufen, Baselland (Switzerland)

For over 8 years, I maintained the small but heterogeneous IT-Infrastructure of the doctor office of Dr. med. Hollenstein in Laufen (BL).

Publications

- David Sommer, Lukas Abfalterer, Sheila Zingg, Esfandiar Mohammadi. "Learning Numeric Optimal Differentially Private Truncated Additive Mechanisms." *arXiv preprint*
- David Sommer*, Liwei Song*, Sameer Wagh, Prateek Mittal. "Towards Probabilistic Verification of Machine Unlearning." *arXiv preprint*
- David Sommer*, Moritz Schneider, Jannik Gut, Srdjan Capkun. "Cyber-Risks in Paper Voting." *arXiv preprint*
- David Sommer*, Sebastian Meiser, and Esfandiar Mohammadi. "Privacy Loss Classes: The Central Limit Theorem in Differential Privacy." In: *Proceedings on Privacy Enhancing Technologies Issue 2 (PoPETS)*, 2019
- David Sommer*, Aritra Dhar*, Esfandiar Mohammadi, Srdjan Capkun, Daniel Ronzani "Deniable Upload and Download via Passive Participation." In: *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2019
- Elizabeth Stobert*, Elizabeta Cavar, Luka Malisa, and David Sommer. "Teaching Authentication in High Schools: Challenges and Lessons Learned." In: *USENIX Workshop on Advances in Security Education (ASE '17). USENIX Association*, 2017
- Sinisa Matetic*, Mansoor Ahmed, Kari Kostiainen, Aritra Dhar, David Sommer, Arthur Gervais, Ari Juels, Srdjan Capkun "ROTE: Rollback Protection for Trusted Execution." In: *26th USENIX Security Symposium*, 2017
- Luka Malisa*, Kari Kostiainen, Thomas Knell, David Sommer, Srdjan Capkun "Hacking in the Blind: (Almost) Invisible Runtime User Interface Attacks." In: *Conference on Cryptographic Hardware and Embedded Systems (CHES)*, 2017

Teaching

I contributed to the following lectures at ETH Zürich:

- *Programmieren und Problemlösen* (TA)
  Grading project presentations and tutoring for programming beginners (Python).
  Spring-Semester (SS) 2021
- *Informatik für Mathematiker und Physiker* (C++ Introduction) (TA)
  Tutoring C++ to a group of 20-30 students per semester.
  Autumn-Semester (AS) 2016, AS 2017, AS 2018, AS 2019, AS 2020
- *Introduction to Machine Learning* (TA)
  Moderating / Answering questions in Moodle for 900+ Students, designing Exam.
  SS 2019
- *Design of Digital Circuits* (TA)
  Designing and supervising labs for developing digital circuits, designing Exams.
  SS 2016, SS 2017, SS 2018

Scientific Service

- Member Editorial Board 2021
  Privacy Enhancing Technologies Symposium (PoPETS) 4.21
- External Reviewer 2019
  ACM Computer and Communications Security 2019 (CCS'19)
- External Reviewer 2018
  ACM Computer and Communications Security 2018 (CCS'18)

Academic Talks

This list only includes academic talks and is not exhaustive:

- Princeton University, Princeton, USA 02/2020
  The Privacy Loss Distribution and its Privacy Loss Class: The Central Limit Theorem in Differential Privacy and Other Insights.
- PETS '19, Stockholm, Sweden 07/2019
  Privacy Loss Classes: The Central Limit Theorem in Differential Privacy.
- NSDI '19, Boston, USA 02/2019
  Deniable Upload and Download via Passive Participation.
- ZISC Lunch Seminar, Zürich, Switzerland 12/2017
  CoverUp: Privacy Through "Forced" Participation in Anonymous Communication Networks.

Awards

- Finalist CSAW'19 HackML 2019
  Top-level competition held by New York University Center for Cybersecurity.
- Top-5 Finalist Spark Award by ETH Zürich 2017
  Top-5 most promising inventions which was registered for a patent in 2016.

Supervised Student-Theses

- Nadja Aoutouf, Semester Thesis, ETH Zürich 10/2020 – 03/2021
  Learning Differential Privacy Mechanisms with High-Dimensional Input.
- Pascal Küng, Bachelor's Thesis, ETH Zürich 09/2020 – 02/2021
  Privacy Leakage in Data Normalization.

- Matthias Niederberger, Master's Thesis, ETH Zürich 10/2019 – 05/2020
  Variational Autoencoder Knowledge Transfer.
- Sheila Zingg, Bachelor's Thesis, ETH Zürich 01/2019 – 7/2019
  Numerically Approximating Optimal Noise in Differential Privacy.
- Vincent Stettler, Master's Thesis, ETH Zürich 11/2018 – 05/2019
  Privacy-Preserving Data-Synthesis.
- Jannik Gut, Bachelor's Thesis, ETH Zürich 09/2018 – 03/2019
  Transferring Voting Results from Municipalities to the State Level.
- Daniel Fischmann, Bachelor's Thesis, ETH Zürich 10/2017 – 04/2018
  Comparison and Feasibility Evaluation of an Information-Theoretic Lower Privacy Bound.
- Luca Ardüser, Master's Thesis, ETH Zürich 10/2017 – 04/2018
  Fair Testing and Exchange of Machine Learning Models Between Distrusting Parties.
- Alexander Meier, Master's Thesis, ETH Zürich 12/2016 – 06/2017
  A Framework for Intention Hiding Proxy Service based on Forced Participation.
- David Bimmler, Bachelor's Thesis, ETH Zürich 03/2016 – 09/2016
  Exploring Cellular Hand-off as an Approach to Mobile Positioning.