RESEARCH GROUP PRIVACY-ENHANCING TECHNOLOGIES

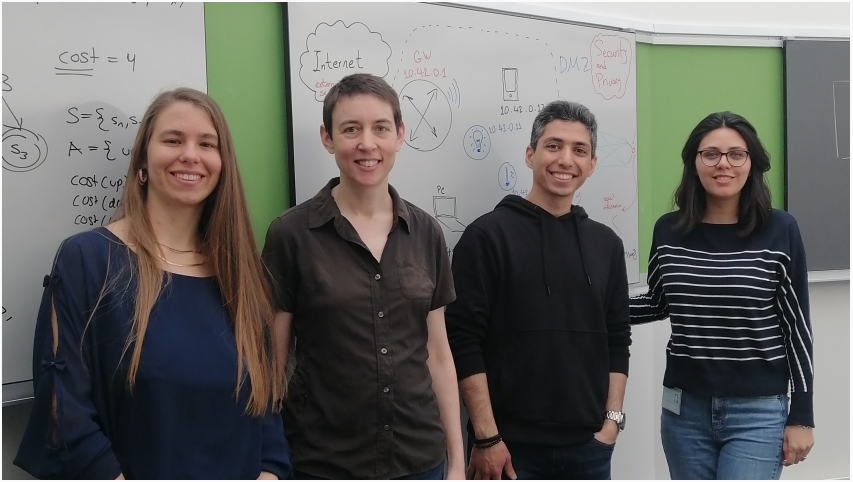
BACHELOR THESES

Isabel Wagner

16 December 2025

University of Basel

WHO ARE WE? PRIVACY ENHANCING TECHNOLOGIES GROUP



Valentyna Pavliv – Isabel Wagner – Nima Akbari – Shiva Parsarad

Teaching

Fall semester

- Reproducibility and Performance of Privacy-Enhancing Technologies (Bachelor seminar, with Prof. Ciorba)
- Foundations of Distributed Systems (Master)

Spring semester

- Cyber Security (Bachelor, 4th/6th semester)
- Privacy-Preserving Methods for Data Science and Distributed Systems (Master)

Lecture: Cyber Security (Spring 2026)

- Bachelor semester 4 or 6, 6 CP
- Topics: introduction to important concepts and methods in cyber security, including:
  - Cryptography
  - System and hardware security
  - Network security
  - Design of secure systems
- Exercises: apply security technologies and combine them to create secure systems

Theses

WHAT DO WE DO? PET GROUP

Mission

Build technical solutions to help individuals benefit from modern technology while protecting their human rights.

Questions

Transparency
Privacy measurement
Privacy mechanisms

Challenges

Black boxes
Functionality (loss), UIs
Performance
Reproducibility

Applications

Internet of Things
Smart cities
Virtual reality, metaverse
Brain-computer interfaces

Tools & Techniques

Network measurement
Edge computing
Cryptography
Synthetic data
Federated learning
Differential privacy

- Collect datasets of interaction with devices
  - Building on *varys*, our tool for automated interaction with voice assistants
- Build automated analysis tools
  - Privacy policy analysis with machine learning
  - Information flow analysis for mobile apps
  - Network traffic analysis
  - Extraction and analysis of firmware

Smart toys

AI wearables

PRIVACY FOR MACHINE LEARNING

- We take a *systems* view on machine learning
- Federated learning
  - Clients train on their local data, server aggregates
  - Compare privacy and utility of existing implementations
- Recommender systems
  - Proposed inference attacks learn whether someone was part of the training data, and what their attributes are
  - Implement an inference attack and analyze its performance against a privacy-preserving recommender system

- Automated interactions with VR apps
  - Difficult because interaction relies on head movement and hand gestures
  - But: we can fool hand tracking with videos of hands shown on a screen
  - Build a system to synthesize video of hand gestures
- Traffic fingerprinting
  - Looking only at encrypted network traffic, can we identify which VR app someone is interacting with?
  - Adapt ML techniques for voice assistant fingerprinting, web fingerprinting

INTERESTED? CONTACT US!

https://pet.dmi.unibas.ch

isabel.wagner@unibas.ch