RESEARCH GROUP PRIVACY-ENHANCING TECHNOLOGIES

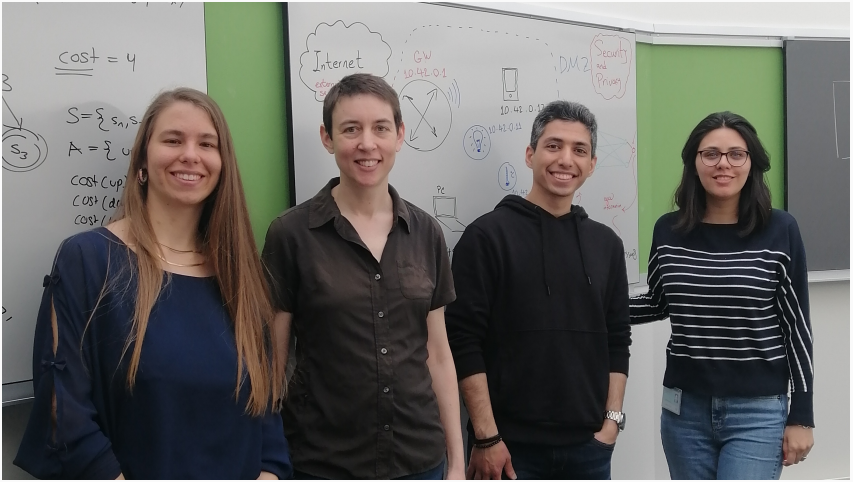
BACHELOR THESES

Isabel Wagner

17 December 2024

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 2025)

- 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

PRIVACY FOR SMART TOYS[1]

- Implement a privacy-friendly AI toy on a Raspberry Pi or ESP32
- Instead of sending audio data to OpenAI, use local models for speech-to-text, chatbot, and text-to-speech
- Computational performance? Minimum hardware requirements?
- Other topics:
  - ML to analyze privacy policies of smart toys

Grok: a voice interface for ChatGPT

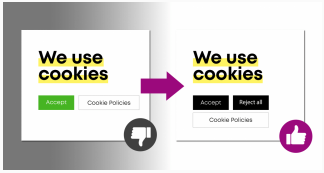
[1] https://www.srf.ch/news/gesellschaft/ki-im-kinderzimmer-spielzeuge-die-mithoeren

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
- Privacy-preserving machine learning
  - Main technique: differentially private stochastic gradient descent
  - How does the structure of a neural network influence privacy?
  - Compare success rates of attacks against networks with different structures
- 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

PRIVACY AND TRANSPARENCY FOR VIRTUAL REALITY

- Dark patterns: user interface designs that trick users into doing things counter to their own interests
  - Cookie banners
  - Low stock warnings and timers on e-commerce websites
- Which dark patterns can we find in VR apps and games? Which types are most common?
- Other topics:
  - Automate user interaction with VR apps



INTERESTED? CONTACT US!

https://pet.dmi.unibas.ch

isabel.wagner@unibas.ch