RESEARCH GROUP PRIVACY-ENHANCING TECHNOLOGIES

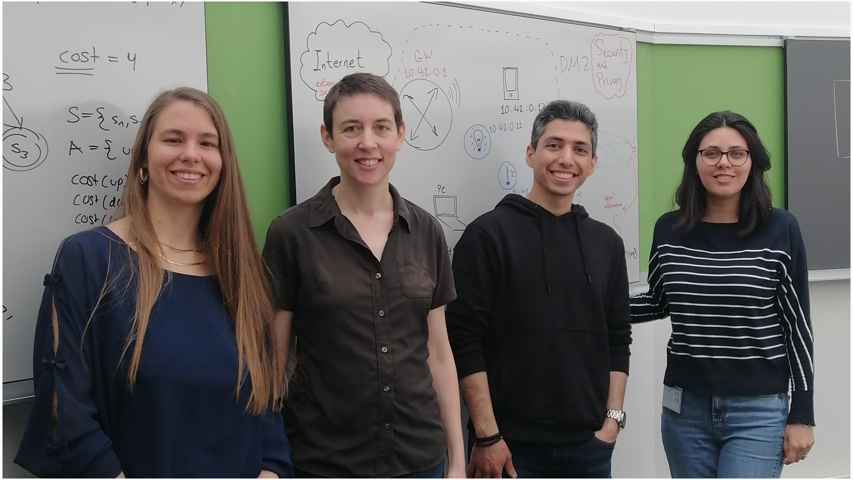
BACHELOR THESES

Isabel Wagner

19 December 2023

University of Basel

WHO ARE WE? PRIVACY ENHANCING TECHNOLOGIES GROUP



Valentyna Pavliv – Isabel Wagner – Nima Akbari – Shiva Parsarad

Teaching

TEACHING

Fall semester 2023

- Privacy-Enhancing Technologies & Performance (Bachelor seminar)
- Foundations of Distributed Systems (Master)
- Computer Architecture (Bachelor, 3rd semester)

Spring semester 2024

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

LECTURE: CYBER SECURITY (SPRING 2024)

- 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

IOT PRIVACY AND TRANSPARENCY

- Analyze data flows:
  - Which data flows from the devices to the internet?
  - Indoor maps, cameras, TV viewing habits,...?
- Analyze network traffic:
  - How is the data transmitted?
  - Communication protocols, cryptography
- Create a testbed:
  - Reproducible traffic recording & storage
- Automation:
  - Simulate user interaction with the device → recordings of *interesting* behavior can be done without human intervention

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
  - Analyze computational performance during training of proposed optimizations
- 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

TRANSPARENCY FOR BRAIN-COMPUTER INTERFACES

- Analyze data flows:
  - Which data flows from the devices to their companion app, and from the app to the internet?
  - Raw EEG data, processed EEG data,...?
- Analyze network traffic:
  - How is the data transmitted?
  - Communication protocols, cryptography
- Create a testbed:
  - Reproducible traffic recording & storage

PRIVACY AND TRANSPARENCY FOR VIRTUAL REALITY

- Record data flows to/from the VR headset
- Analyze privacy aspects, for example:
    - To what extent are users tracked?
    - To what extent is user data shared with first/third parties?
- Automate interaction with VR apps

INTERESTED? CONTACT US!

🌐 https://pet.dmi.unibas.ch

✉ isabel.wagner@unibas.ch