Kick-off: Data Privacy Technologies

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

Georg Bramm
georg.bramm@aisec.fraunhofer.de

Immanuel Kunz
immanuel.kunz@aisec.fraunhofer.de

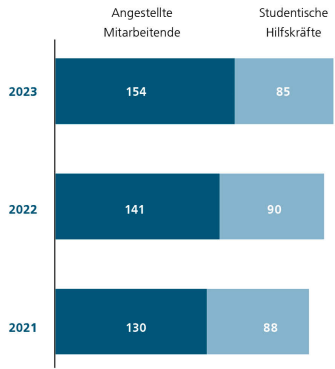
July 9, 2024

Outline

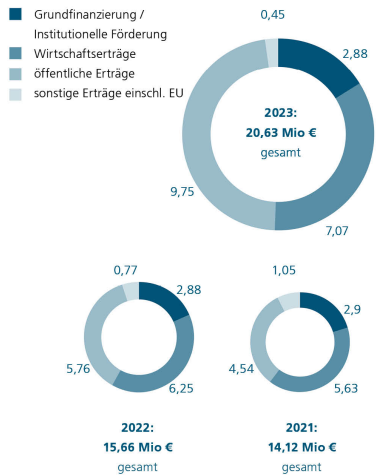
Who we are

Who we are in numbers

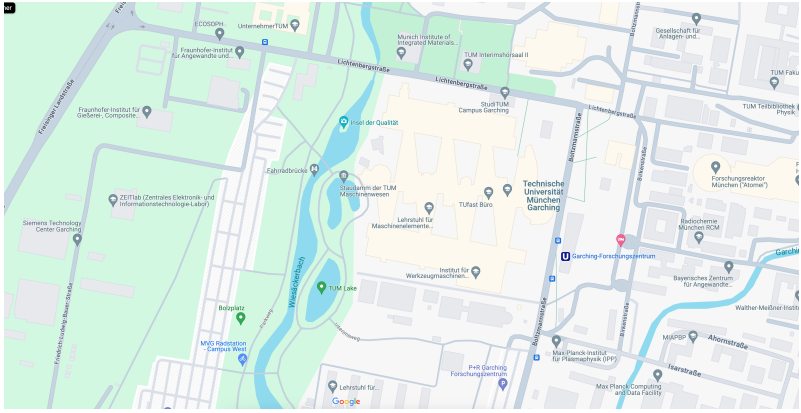
Zahl der Mitarbeitenden



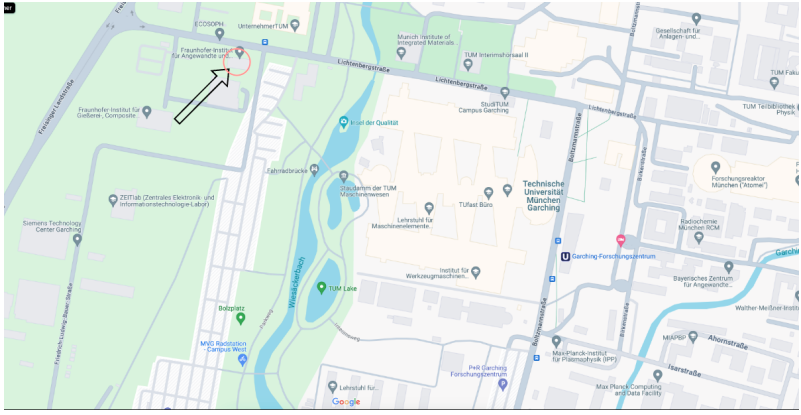
Forschungsvolumen (in Mio €)



Where we are


ECOSOPH
Unternehmer TUM
Fraunhofer-Institut für Angewandte und...
Lichtenbergstraße
Fraunhofer-Institut für Gießerei-, Composite...
Insel der Qualität
Fahrradbrücke
Stautarhm der TUM Maschinenwesen
ZEITlab (Zentrales Elektronik- und Informationstechnologie-Labor)
Siemens Technology Center Garching
Lehrstuhl für Maschinenelemente...
TUFast Büro
Studi TUM Campus Garching
Technische Universität München Garching
Boltzmannstraße
Garching-Forschungszentrum
Institut für Werkzeugmaschinen...
TUM Lake
Wissenschaftspark
Beiplatz
MVG Radstation Campus West
Max-Planck-Institut für Plasmaphysik (IPP)
P+R Garching Forschungszentrum
Lehrstuhl für...
Max Planck Computing and Data Facility
Gesellschaft für Anlagen- und...
TUM Interimshörsaal II
Murnich Institute of Integrated Materials...
Forschungsreaktor München ("Atomei")
Radiochemie München RCM
Bayerisches Zentrum für Angewandte...
Walther-Meißner-Institu
MPAP&P
Ahornstraße
Isarstraße
TUM Bibliothek Physik
Google

Where we are


ECOSOPH
Unternehmer TUM
Fraunhofer-Institut für Angewandte und...
Fraunhofer-Institut für Gießerei-, Composite...
Lichtenbergstraße
Freisinger Landstraße
Munich Institute of Integrated Materials...
TUM Interimshörsaal II
StudTUM Campus Garching
Insel der Qualität
Fahrradbrücke
Staudamm der TUM Maschinenwesen
Lehrstuhl für Maschinenelemente...
TUfast Büro
Technische Universität München Garching
Boltzmannstraße
Informatikstraße
Lichtenbergstraße
Gesellschaft für Anlagen und...
TUM Fakultät...
TUM Teilbibliothek Physik
Forschungsreaktor München ("Atomei")
Radiochemie München RCM
Garching-Forschungszentrum
Bayerisches Zentrum für Angewandte...
Walther-Meißner-Institut...
ZEITlab (Zentrales Elektronik- und Informationstechnologie-Labor)
Siemens Technology Center Garching
Friedrich-Ludwig-Bauer-Straße
Institut für Werkzeugmaschinen...
TUM Lake
Würmkanal
Bolzplatz
MVG Radstation Campus West
Lehrstuhl für...
PHK Garching Forschungszentrum
Max-Planck-Institut für Plasmaphysik (IPP)
MPCDF
Ahornstraße
Isarstraße
Max Planck Computing and Data Facility
Google

This seminar

will be organized as a scientific conference:

1. Familiarization phase (2 Weeks)
2. Writing phase (12 Weeks)
3. Review phase (2 Weeks)
4. Improvement phase (1 Week)
5. Talk preparation (min 1 Week)
6. Talk and Discussion

Requirements

- Report
  - Written report in the form of a scientific paper
  - Mandatory length of 10 pages (without references and appendix)
  - Usage of LaTeX is mandatory
  - Formatting with the provided LaTeX-Style (IEEE 2-column)
- Review
  - Every Student creates 2 anonymous reviews
  - Review template will be provided
  - Approximately 1/2 page
  - Every Student writes a rebuttal
- Presentation
  - 30 minutes presentation
  - 15 minutes discussion

Grading

Grading considers all contributions to this seminar:

1. Scientific Paper (SoK or specific research question(s)) (50%)
   - Contents, Accuracy, Style, Effort, Grasp
2. Mandatory Peer Review (10%)
3. Presentation (40%)
   - Slides, Execution, Contents, Understandability (30%)
   - Discussion (10%)

Time Table (tentative)

09.07.24	Kick-off meeting (today)
14.08.24	Send choice of assignment/topic to supervisor
16.08.24	Topic Assignment
tbd	Introduction to scientific writing (recommended)
as soon as possible	Organize at least one meeting with your supervisor.
10.01.25	Deadline for draft paper
13.01.25	Review Assignments
23.01.25	Deadline for (2x) review submission(s)
31.01.25	Deadline for own rebuttal
31.01.25	Deadline for final paper
31.01.25	Deadline for presentation
between 03.02.25 and 14.02.25	Presentations and discussion

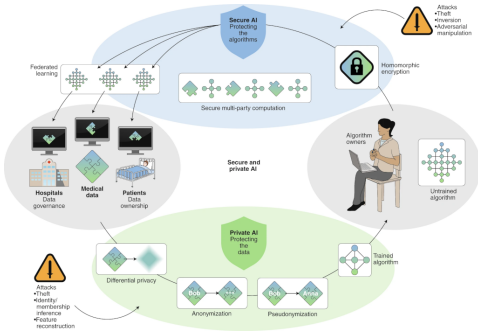
Before we go on....

... any questions so far?

Topics

- Privacy Preserving Computation (supervisor: Bramm)
  - Privacy-Preserving Data Analysis
  - Privacy-Preserving Search
- Privacy-enhancing cryptography in ML (supervisor: Bramm)
  - Proof of Learning
  - Proof of Training
  - Proof of Intelligence
- Privacy Engineering (supervisor: Kunz)
  - Privacy Threat Modeling and Risk Analysis
  - Privacy Data Flow Analysis
  - Privacy in the Software Development Lifecycle
  - Methods for Privacy by Design
  - Privacy, Security, and Data Protection

Topic: Privacy-Preserving Data Analysis / Bramm



- Understand and present a privacy preserving computation concept in data analysis based on (either)
  - federated learning
  - differential privacy
  - garbled circuits
  - secure multiparty comp.
  - homomorphic encryption
- Compare the chosen approach regarding advantages and disadvantages for each participating party.

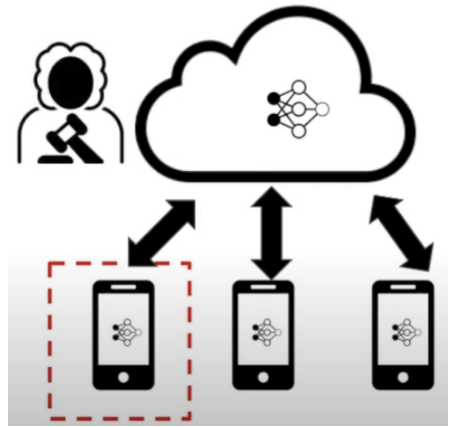
- Understand and present privacy preserving searchable encryption concepts based on post quantum primitives.
- Survey the state of the art in different existing approaches.

Case 1: ownership resolution

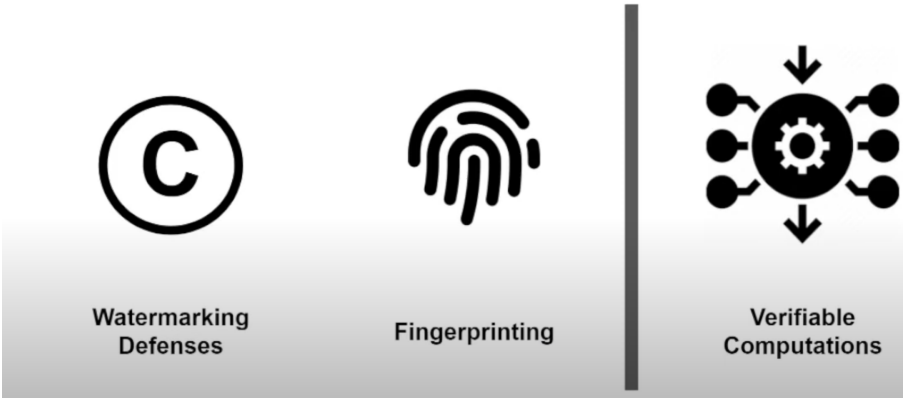
- Given some publicly hosted model.
- An adversary can reverse that model an generate a stolen one.
- How does the original owner of the original input data cryptographically prove that he generated the model?

Case 2: delegated computation

- A central ML model on a server. The central model is generated using distributed/colaborative learning.
- An adversary deviates from the protocol and wants to attack the central model.
- Is there a way to cryptographically prove that a worker is misbehaving? ?



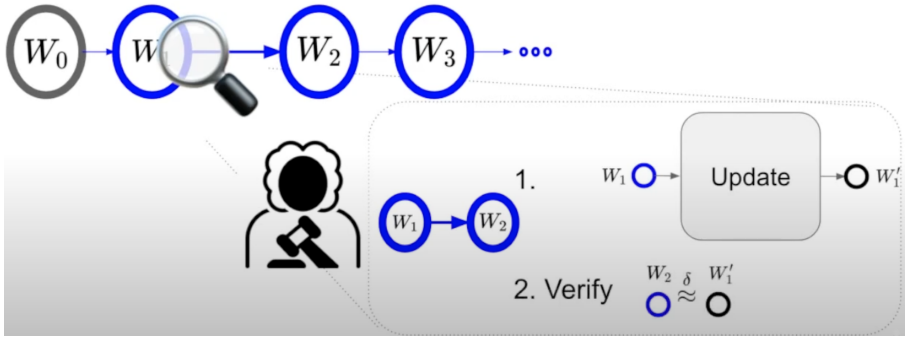
Old solution attempts



Old solution problems

Why a proof would help ?

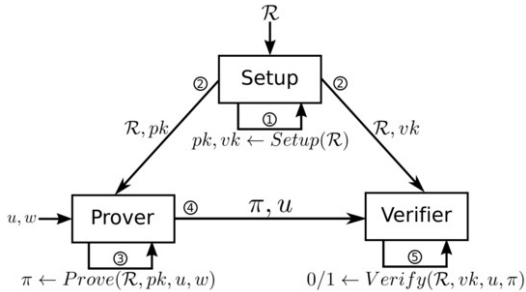
Topic: Proof of Learning / Bramm



PoL

- Blockchain based approaches
- Consensus based approaches
- also other approaches

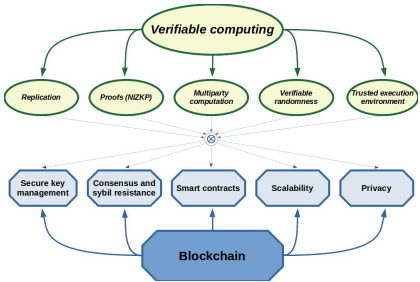
Topic: Proof of Training / Bramm

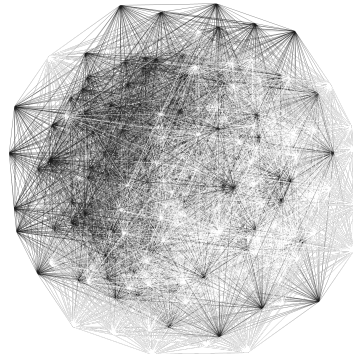


PoT

- Zero Knowledge based approaches
- zkSnarks, zkStarks approaches

Topic: Proof of Intelligence / Bramm

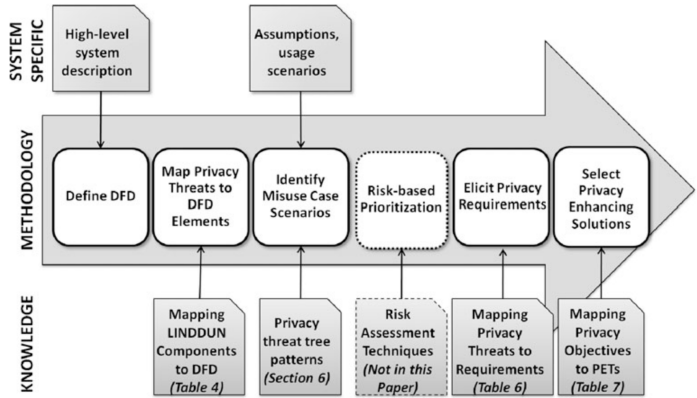




PoI (corner/special case)

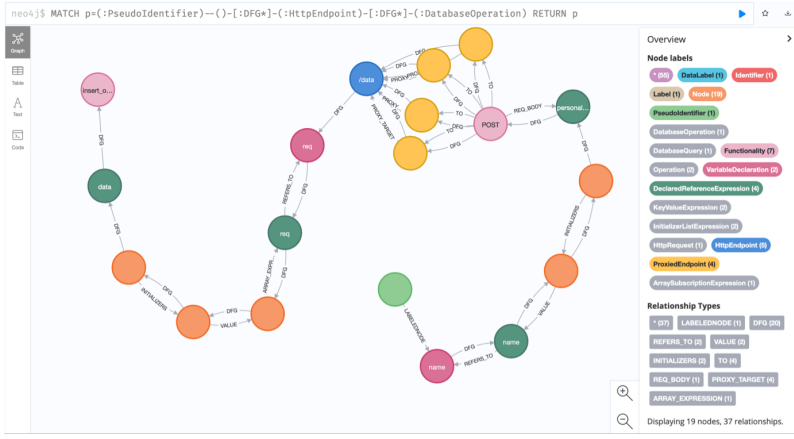
- Proof of not only input data utilization, but also on the training application itself
- Consensus-based approach.
- Bittensor / Tao

Topic: Privacy Threat Modeling and Risk Analysis / Kunz

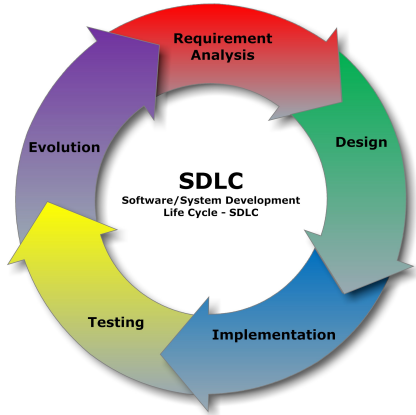


- Compare privacy and security threat modeling / risk assessment approaches
- LINDDUN, LINDDUN GO, STRIDE, Kill chains
- Which types of threats can be found with the different frameworks?

Topic: Privacy Data Flow Analysis / Kunz



- Various approaches exist for tracking personal data in software applications
- Analyze and compare different proposals
- How can privacy engineers be supported with these tools? Which threats can(‘t) they find?



- There are software development lifecycles
- There are *secure* software development lifecycles
- Compare SDLCs regarding their privacy focus

Topic: Methods for Privacy by Design / Kunz

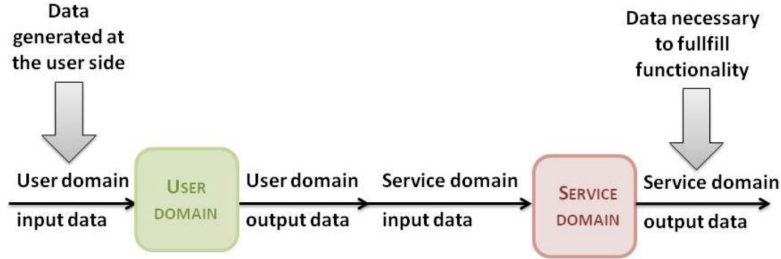
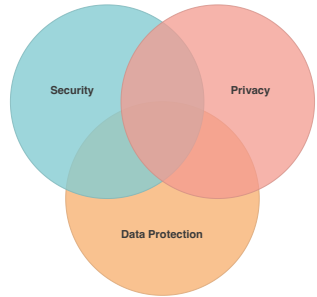


Figure: Privacy by Design method by Gürses et al.

- Many scientific approaches propose privacy by design methods
- Select a number of papers regarding a specific PbD aspect (like data minimization)
- Review, compare, and discuss them; possibly apply to a use case

- What are the overlaps and conflicts between privacy, security and data protection?
- How is "privacy" regulated by the GDPR and other regulations?
- Review methods and privacy-enhancing technologies in the context of *data protection by design*



Procedure

1. Matching and Topic assignment
   - Register via DocMatching
   - After the matching concludes, we'll get in touch with the participants.
   - If you want to deregister
     - do so timely to avoid penalty or brace yourself for a 5.0.
   - Participants send top 3 topics via email to Georg Bramm until 16.08.24, we'll assign the topics.
2. Familiarization phase:
   - Literature research.
   - Get an overview of your topic by reading initial literature
   - Research additional follow-up or proceeding literature
   - Create paper bibliothek.
   - Create paper structure.
3. Introduction to scientific writing possibly provided by chair.
4. ... (next slide)

Procedure

3. ... (previous slide)
4. Writing phase.
   - one initial meeting with supervisor where you present your writing plans
   - and discuss and solve questions with your supervisor
   - ideally: a second meeting with your supervisor for final questions / hints, before:
5. Paper submission
   - The first draft must be acceptable!
   - No submission $\Rightarrow$ 5.0.
   - Violation of page limit $\Rightarrow$ 5.0.
   - No "buffering" of pages using images with little informational value or oversize.
6. Review phase.
   - You are given 2 papers to review
   - A good review should be about 1/2 page.
   - It should contain: Summarization, Critiques, Suggestions, Hints for improvement, Formal (Spelling, Figures, ...).
7. Final Presentations. (30min/15min each)

Q&A

Fraunhofer AISEC

See first slide for contact emails.