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

Martin Schanzenbach
martin.schanzenbach@aisec.fraunhofer.de

July 5, 2021
Outline

1. Organization
2. Requirements
3. Grading
4. Time Table
5. Topics
The 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 two anonymous reviews
  - Review template will be provided
  - Approximately 1/2 page
  - Every Student writes a rebuttal

- **Presentation**
  - Presentation with slides
  - 30 minutes presentation
  - 15 minutes discussion
Grading considers all contributions to this seminar:

1. Report (50%)
   - Contents, Accuracy, Style, Effort, Grasp

2. Presentation (40%)
   - Slides, Execution, Contents, Understandability (30%)
   - Discussion (10%)

3. Feedback (10%)
   - Written Reviews and Rebuttal (5%)
   - Participation and discussion (5%)
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.07.21</td>
<td>Kick-off meeting (today)</td>
</tr>
<tr>
<td>16.08.21</td>
<td>Topic Assignment</td>
</tr>
<tr>
<td>01.10.21</td>
<td>Introduction to scientific writing (recommended)</td>
</tr>
<tr>
<td>22.10., 05.11., 19.11., 03.12., 17.12., 07.01</td>
<td>Bi-weekly meeting with status updates</td>
</tr>
<tr>
<td>14.01.22</td>
<td>Deadline for report (pre-final) submission</td>
</tr>
<tr>
<td>17.01.22</td>
<td>Review Assignments</td>
</tr>
<tr>
<td>28.01.22</td>
<td>Deadline for review submission</td>
</tr>
<tr>
<td>04.02.22</td>
<td>Deadline for rebuttal submission</td>
</tr>
<tr>
<td>04.02.22</td>
<td>Deadline for final report submission</td>
</tr>
<tr>
<td>until 11.02.22</td>
<td>Deadline for presentation submission</td>
</tr>
<tr>
<td>until 11.02.22</td>
<td>Presentations and discussion</td>
</tr>
</tbody>
</table>
Before we go on....

... any questions so far?
Topics

- Privacy Engineering
  - Privacy Requirements Engineering
  - Privacy-By-Design
  - Quantifying Privacy
- Privacy Preserving Computation
  - Privacy-Preserving Data Analysis
  - Privacy-Preserving Search
  - Private Stream Aggregation
- Privacy-enhancing cryptography
  - Verifiable random functions
  - Hierarchical deterministic key derivation
  - Privacy-friendly online payments
Topics: Privacy Requirements Engineering

Figure: An overview of the LINDDUN process (Deng et al. 2011).
Compare and discuss different approaches to privacy by design from the literature.

Figure: Spiekermann and Cranor (2008).
Topics: Privacy By Design

- Compare and discuss different approaches to privacy by design from the literature

**Figure:** Gürses et al. (2015).
Topics: Quantifying Privacy

- Pick out a few metrics from one metric type
- Compare them and discuss their limitations in different attacker models

Figure: An overview of privacy metrics (Wagner and Eckhoff 2018).
Topics: Privacy-Preserving Data Analysis

- Understand and present privacy preserving computation concepts based on
  - garbled circuits
  - secure multiparty computation
  - homomorphic encryption
- Compare the approaches regarding the privacy for the participating parties.
Topics: Privacy-Preserving Search

- Understand and present privacy preserving searchable encryption concepts based on lattices.
- Survey the state of the art in different lattice based approaches.
Topics: Private Stream Aggregation

- Understand and present generalized concepts of PSA.
- Survey the state of the art in different PSA schemes.
- Research and discuss current applications of the above.
A VRF is a cryptographic concept that can be used to create publicly verifiable proofs or commitments on data in a privacy-preserving fashion. It allows a prover to calculate a function \( y = f(x) \) and provide a proof \( \pi \). Any verifier may use \( \pi \) that the \( y \) is actually the result of \( f(x) \) without being able to calculate it.

Goals:

- Understand and present generalized concepts of VRF.
- Survey applications and uses of VRFs in PETs.
Hierarchical Deterministic Key Derivation (HDKD) are cryptographic key derivation schemes which are used for key blinding as well as derivation of crypto wallets.

Goals:

▶ Understand and present generalized concepts of HDKD.
▶ Present and compare existing HDKDs.
▶ Present use cases of HDKD.
Privacy-friendly payment systems.

Digital payment systems are ubiquitous. We know that payment information and transactions are (ab)used by governments and criminals alike. In order to counter this issue, private and privacy-friendly payment systems have been proposed in literature and in practice. Goals:

▶ Understand and present the technological concepts behind selected payment systems.
▶ Present and compare privacy-friendly payment systems.
Procedure

1. Matching and Topic assignment
   - 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, we’ll assign the topics.

2. Familiarization phase:
   - Literature research.
   - Get an overview of your topic.
   - Create report structure.

3. Introduction to scientific writing possibly provided by chair.

4. ... (next slide)
3. . . . (previous slide)

4. Writing phase.
   – Bi-Weekly Meetings on 22.10., 05.11., 19.11., 03.12., 17.12., 07.01. at 10:00 o’clock
   – Each student presents the work progress in a short review
   – Discussion and Questions afterwards

5. Paper submission
   – The first version for review 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.

7. Final Presentations.
Q&A

See first slide for contact emails.