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

Martin Schanzenbach
martin.schanzenbach@aisec.fraunhofer.de

February 2, 2021
Outline

1. Organization
2. Requirements
3. Grading
4. Time Table
5. Topics
Organization

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 6 pages (references don’t count)
- 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 (30%)
   ▶ Slides, Execution, Contents, Understandability
3. Reviews (15%)
   ▶ Written Reviews and Rebuttal
4. Participation and discussion (5%)
Time Table (tentative)

02.02.21 • Kick-off meeting (today)
15.03.21 • Topic Assignment
02.04.21 • Introduction to scientific writing (recommended)
18.06.21 • Deadline for report (pre-final) submission
21.06.21 • Review Assignments
02.07.21 • Deadline for review submission
09.07.21 • Deadline for rebuttal submission
09.07.21 • Deadline for final report submission
09.07.21 • Deadline for presentation submission
until 17.07.21 • Presentations and discussion
Before we go on....

... any questions so far?
Topics

▶ Building Blocks of Privacy-enhancing technologies
   1. A comparison between identity standards (OpenID, DID).
   2. Verifiable Random Functions and their Applications.
   5. Privacy at the Transport Layer.

▶ Privacy in Machine Learning
   1. Training data privacy
   2. Input/Output privacy
   3. Model privacy
   4. Privacy-preserving Federated Learning
   5. Privacy attacks on Machine Learning Models
Topics

▶ Building Blocks of Privacy-enhancing technologies
  1. A comparison between identity standards (OpenID, DID).
  2. Verifiable Random Functions and their Applications.
  5. Privacy at the Transport Layer.

▶ Privacy in Machine Learning
  1. Training data privacy
  2. Input/Output privacy
  3. Model privacy
  4. Privacy-preserving Federated Learning
  5. Privacy attacks on Machine Learning Models

▶ Bring your own interesting topic.
Building blocks of privacy-enhancing technologies
A comparison between identity standards (OpenID, DID)

There are currently two standards for identity and attribute representation: JSON-Web-Tokens (OpenID Connect) and Decentralized Identifiers (DIDs).

Goals:

- Understand both standards/protocols and their differences.
- Show what privacy considerations exists in both concepts.
- Compare both approaches.
Verifiable Random Functions and their Applications in PETs

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.

Figure: High-level overview of VRF.

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.
Distributed Private Information Retrieval Schemes

PIR is used to protect user privacy when working with outsourced data. It allows users to retrieve data from a remote store without revealing to third parties which item was retrieved.

Goals:
- Understand and present generalized concepts of PIR.
- Survey the state of the art in decentralized/distributed PIR schemes.
- Research and discuss current applications of the above.
Privacy at the transport layer is a difficult endeavour. Especially protection of metadata is crucial but difficult. Recent proposals from leveraging TCP Fast Open and TLS 1.3. try to tackle the issue.

Goals:

- Research existing transport layer privacy approaches.
- Systematically present and compare the approaches.
Privacy in Machine Learning
Privacy-preserving Machine Learning (1-3)

Figure: https://towardsdatascience.com/perfectly-privacy-preserving-ai-c14698f322f5.

Research and discuss latest improvements and techniques in perfectly-privacy preserving ML:

1. Training Data Privacy. (protect data creator.)
2. Input/Output Privacy. (protect user input/output.)
3. Model Privacy. (protect model creator.)
Research, compare and discuss existing privacy-preserving federated learning architectures, like NVIDIA's approach\(^1\) or the sherpa.ai approach\(^2\) or others of your choice.

\(^1\)https://arxiv.org/abs/1910.00962
Research, compare and discuss privacy attacks against machine learning systems:

- Membership inference attack.³ ⁴
- Model inversion attack.⁵
- Measuring unintended neural network extraction attack.⁶
- Others of your choice

³https://arxiv.org/abs/1610.05820
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. Writing phase.
   – The first version for review must be acceptable!
   – No submission ⇒ 5.0.
   – Violation of page limit ⇒ 5.0.
   – No “buffering” of pages using images with little informational value or oversize.

5. Review phase.

6. Presentation.
See first slide for contact emails.