Kick-off: Data Privacy Technologies

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

Immanuel Kunz
immanuel.kunz@aisec.fraunhofer.de

Georg Bramm
georg.bramm@aisec.fraunhofer.de

Martin Schanzenbach
martin.schanzenbach@aisec.fraunhofer.de

July 13, 2020

Outline

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 (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

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)

13.07.20	Kick-off meeting (today)
01.-31.08.20	Topic Assignment
18.12.20	Deadline for report (pre-final) submission
21.12.20	Review Assignments
08.01.20	Deadline for review submission
15.01.21	Deadline for rebuttal submission
15.01.21	Deadline for final report submission
20.01.21	Deadline for presentation submission
21.01.21	Presentations and discussion

Before we go on....

... any questions so far?

Topics

- Differential Privacy
  - in Cryptography
  - in Databases
  - in Location Based Services
- Privacy Engineering
  - Privacy Requirements Engineering
  - Quantifying Privacy
  - Privacy in Machine Learning
  - Policy Enforcement in the Cloud
- Building Blocks of Privacy-enhancing technologies
  - Verifyable Random Functions and their Applications
  - Distributed/decentralized Private Information Retrieval
  - Privacy-preserving, distributed Reputation Systems

Differential Privacy

Differential Privacy in Cryptography

Differential privacy can be layered with Cryptography

- from the Functional Domain, like Attribute Based Encryption (ABE)
- from the Homomorphic Domain, like Paillier

Research the current state of the art and the applicability in the context

- of the Industrial Data Space (IDS)
- of an eHealth data set.

Differential Privacy in Databases

Differential privacy can be in incorporated into Databases

- by adopting the query
- by adpoting the insertion

Research the current state of the art and the applicability in the context

- of structured databases
- of unstructured databases

Differential Privacy in Location Based Services

Differential privacy can be used to protect your privacy when using Location Based Services (LBS) Research the current state of the art in the context of

- Location Privacy
- Trajectory Privacy

Present and compare the different systems

Privacy Engineering

Privacy Requirements Engineering

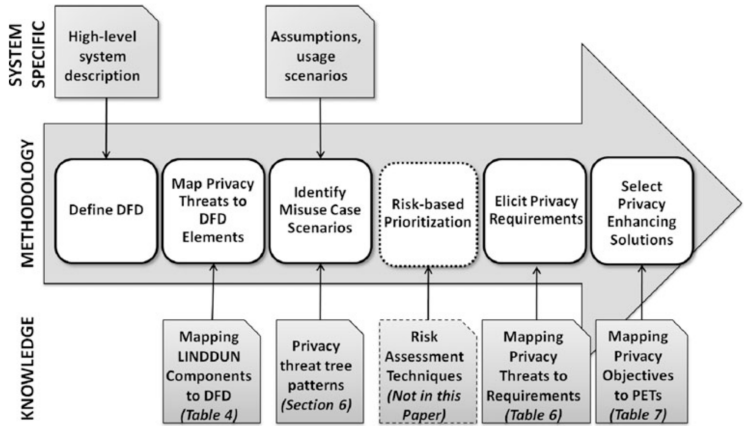

Figure: An overview of the LINDDUN process (Deng et al. 2011).

Quantifying Privacy

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

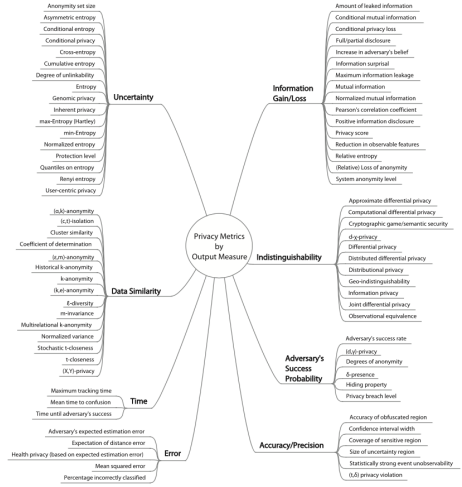

Figure: An overview of privacy metrics (Wagner and Eckhoff 2018).

Privacy in Machine Learning

- Various attacks on ML training data are possible
  - Membership inference
  - Attribute inference
  - ...
- Various defense strategies exist
  - Differential privacy
  - Reduce the model's precision
  - ...
- Review one type of attack and discuss possible defense strategies

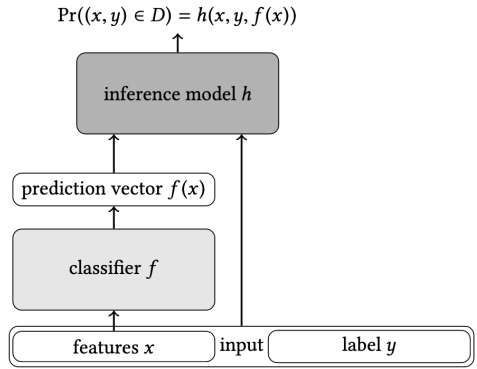

Figure: Building an inference model to predict membership in the training set (Nasr et al. 2018).

Policy Enforcement in the Cloud

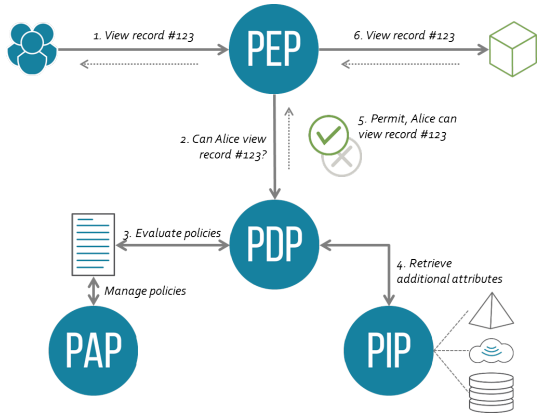

Figure: The components of the XACML standard (Wikimedia Commons).

Fraunhofer AISEC

Building blocks of privacy-enhancing technologies

Figure: High-level overview of VRF.

http://cryptowiki.net/index.php?title=Verifiable_Random_Functions.

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 π. Any verifier may use π 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.

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 PIRs.
- Research and discuss current applications of the above.

Privacy-preserving, distributed reputation systems

Reputation systems have a long history in the research community. RSs are used to establish trust without the need of a trusted third party and instead relying on observed/processed "recommendations".
Goals:

- Understand and present generalized concepts of reputation systems.
- Survey the state of the art in distributed reputation systems.
- Research *current* applications of the above.

Procedure

1. Matching and Topic assignment
   - Matching concludes August 2020. After that 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 $\Rightarrow$ 5.0.
   - Violation of page limit $\Rightarrow$ 5.0.
   - No "buffering" of pages using images with little informational value or oversize.
5. Review phase.
6. Presentation.

Q&A

Fraunhofer AISEC

Q&A ?