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

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 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

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%)

Time Table (tentative)

05.07.21	Kick-off meeting (today)
16.08.21	Topic Assignment
01.10.21	Introduction to scientific writing (recommended)
22.10., 05.11., 19.11., 03.12., 17.12., 07.01	Bi-weekly meeting with status updates
14.01.22	Deadline for report (pre-final) submission
17.01.22	Review Assignments
28.01.22	Deadline for review submission
04.02.22	Deadline for rebuttal submission
04.02.22	Deadline for final report submission
until 11.02.22	Deadline for presentation submission
until 11.02.22	Presentations and discussion

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

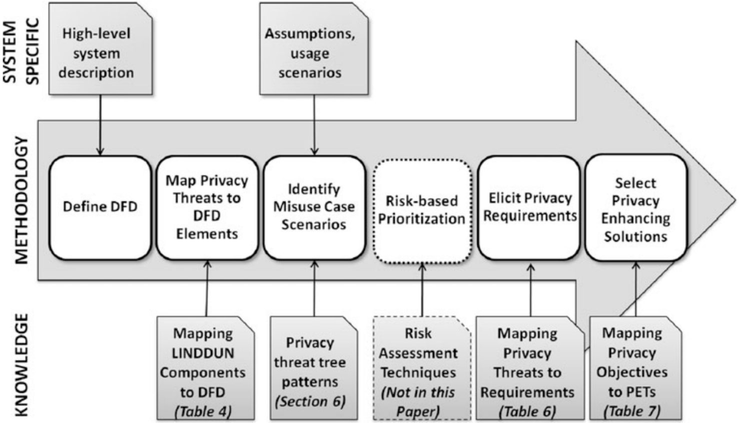

SYSTEM SPECIFIC
High-level system description
Assumptions, usage scenarios
METHODOLOGY
Define DFD
Map Privacy Threats to DFD Elements
Identify Misuse Case Scenarios
Risk-based Prioritization
Elicit Privacy Requirements
Select Privacy Enhancing Solutions
KNOWLEDGE
Mapping LINDDUN Components to DFD (Table 4)
Privacy threat tree patterns (Section 6)
Risk Assessment Techniques (Not in this Paper)
Mapping Privacy Threats to Requirements (Table 6)
Mapping Privacy Objectives to PETs (Table 7)

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

Topics: Privacy By Design

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

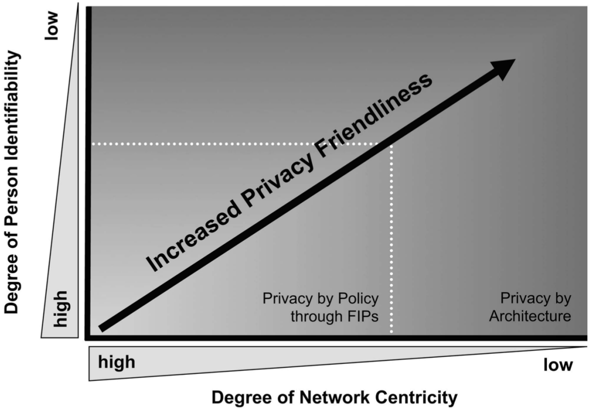

Degree of Person Identifiability
low
high
Increased Privacy Friendliness
Privacy by Policy through FIPs
Privacy by Architecture
high
low
Degree of Network Centricity

Figure: Spiekermann and Cranor (2008).

Topics: Privacy By Design

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

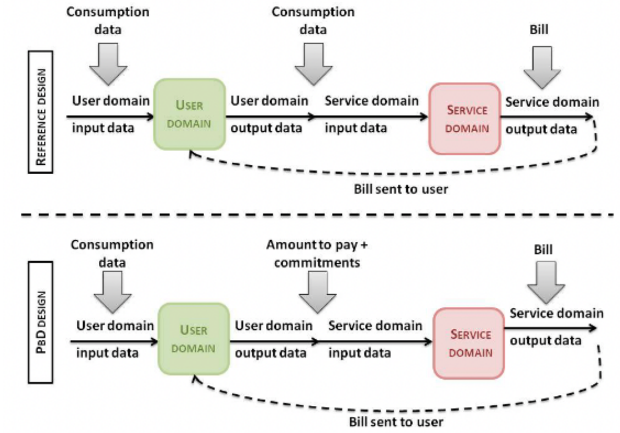
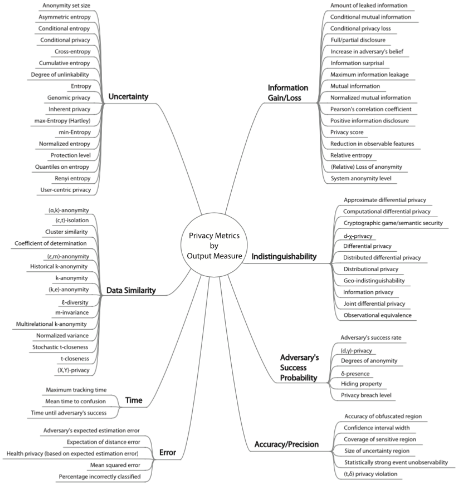


Figure: Gürses et al. (2015).

Topics: Quantifying Privacy

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



Privacy Metrics
by
Output Measure

Uncertainty
Anonymity set size
Asymmetric entropy
Conditional entropy
Conditional privacy
Cross-entropy
Cumulative entropy
Degree of unlinkability
Entropy
Genomic privacy
Inherent privacy
max-Entropy (Hartley)
min-Entropy
Normalized entropy
Protection level
Quantiles on entropy
Renyi entropy
User-centric privacy

Information Gain/Loss
Amount of leaked information
Conditional mutual information
Conditional privacy loss
Full/partial disclosure
Increase in adversary's belief
Information surprisal
Maximum information leakage
Mutual information
Normalized mutual information
Pearson's correlation coefficient
Positive information disclosure
Privacy score
Reduction in observable features
Relative entropy
(Relative) Loss of anonymity
System anonymity level

Data Similarity
(α,k)-anonymity
(c,t)-isolation
Cluster similarity
Coefficient of determination
(ε,m)-anonymity
Historical k-anonymity
k-anonymity
(k,e)-anonymity
ℓ-diversity
m-invariance
Multirelational k-anonymity
Normalized variance
Stochastic t-closeness
t-closeness
(X,Y)-privacy

Indistinguishability
Approximate differential privacy
Computational differential privacy
Cryptographic game/semantic security
d-χ-privacy
Differential privacy
Distributed differential privacy
Distributional privacy
Geo-indistinguishability
Information privacy
Joint differential privacy
Observational equivalence

Adversary's Success Probability
Adversary's success rate
(d,γ)-privacy
Degrees of anonymity
δ-presence
Hiding property
Privacy breach level

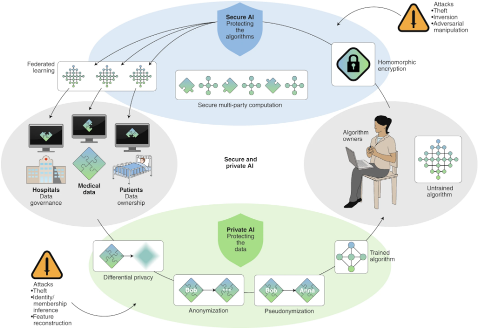
Time
Maximum tracking time
Mean time to confusion
Time until adversary's success

Error
Adversary's expected estimation error
Expectation of distance error
Health privacy (based on expected estimation error)
Mean squared error
Percentage incorrectly classified

Accuracy/Precision
Accuracy of obfuscated region
Confidence interval width
Coverage of sensitive region
Size of uncertainty region
Statistically strong event unobservability
(t,δ) privacy violation

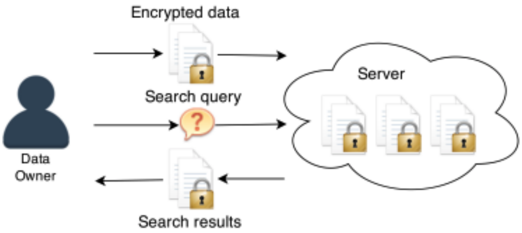
Figure: An overview of privacy metrics (Wagner and Eckhoff 2018).

Topics: Privacy-Preserving Data Analysis



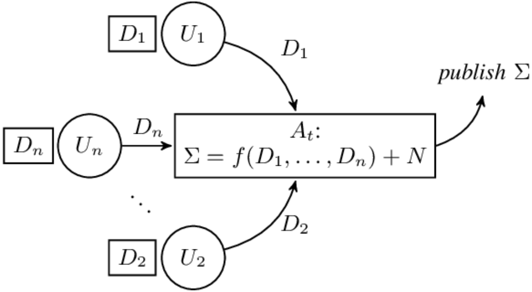
- Understand and present privacy preserving computation concepts based on
  - garbled circuits
  - secure multiparty computation
  - homomorphic encryption
- Compare the approaches regarding the privacy for the participating parties.

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.

Verifiable Random Functions and their Applications in PETs

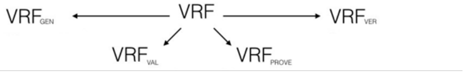


Figure: High-level overview of VRF.

`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.

A Survey on Hierarchical Deterministic Key Derivation.

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)

Procedure

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 ⇒ 5.0.
   - Violation of page limit ⇒ 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.