Fraunhofer AISEC

Application-Oriented Selection of Privacy-Enhancing Technologies (Short Paper)

Immanuel Kunz and Andreas Binder

Fraunhofer AISEC

Annual Privacy Forum '22

Fraunhofer AISEC

Agenda

Fraunhofer AISEC

Motivation and State-of-the-Art

Fraunhofer AISEC

Motivation and State-of-the-Art

- Selection of PETs is application-specific, but can be approached systematically

Fraunhofer AISEC

Motivation and State-of-the-Art

- Selection of PETs is application-specific, but can be approached systematically
- Application-oriented selection criteria are not sufficiently addressed

Fraunhofer AISEC

Motivation and State-of-the-Art

- Selection of PETs is application-specific, but can be approached systematically
- Application-oriented selection criteria are not sufficiently addressed

- Deng et al.: LINDDUN

Fraunhofer AISEC

Motivation and State-of-the-Art

- Selection of PETs is application-specific, but can be approached systematically
- Application-oriented selection criteria are not sufficiently addressed

- Deng et al.: LINDDUN
- Heurix et al.: A taxonomy for privacy enhancing technologies

Fraunhofer AISEC

Classifying Privacy-Enhancing Technologies

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)
- Metric (based on Wagner and Eckhoff)

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)
- Metric (based on Wagner and Eckhoff)
- Functional Scenario (Computation, Messaging, Retrieval, Release, Authentication, Authorization)

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)
- Metric (based on Wagner and Eckhoff)
- Functional Scenario (Computation, Messaging, Retrieval, Release, Authentication, Authorization)
- Maturity (based on TRL)

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)
- Metric (based on Wagner and Eckhoff)
- Functional Scenario (Computation, Messaging, Retrieval, Release, Authentication, Authorization)
- Maturity (based on TRL)
- Performance Impact

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)
- Metric (based on Wagner and Eckhoff)
- Functional Scenario (Computation, Messaging, Retrieval, Release, Authentication, Authorization)
- Maturity (based on TRL)
- Performance Impact
- Architectural Impact

Fraunhofer AISEC

Criteria

- Privacy Protection Goal (LINDDUN)
- Metric (based on Wagner and Eckhoff)
- Functional Scenario (Computation, Messaging, Retrieval, Release, Authentication, Authorization)
- Maturity (based on TRL)
- Performance Impact
- Architectural Impact
- Utility

Fraunhofer AISEC

Name	*Linkability*	*Identifiability*	*Non-Repud.*	*Detectability*	*Disclosure*	*Unawareness*	*Non-Comp.*	*Metrics*	*Functional Scenario*	*Maturity*	*Performance*	*Architecture*	*Utility*
k-anonymity	■							Data similarity	Release	3			◀
Suppression	■	■						Data similarity	Release	3			◀
Anonymous Credentials	■	■						Cryptographic Games	AuthN	2			
Local Differential Privacy			■					Indistinguishability	Release	2			◀
Global Differential Privacy	■							Indistinguishability	Release	2			◀
Homomorphic Encryption					■			Cryptographic Games	Computation	2	◀		
⋮					⋮				⋮				

Fraunhofer AISEC

Example threats

1. **Linkability (Release)**: linkability of transactional data
2. **Identifiability (Release)**: identification via transactional data
3. **Disclosure (Computation)**: disclosure of processed data
4. **Detectability (Messaging)**: detectable messages sent between users

Fraunhofer AISEC

Threat	LINDDUN Result	Our Classification
Linkability (Release)	**k-anonymity**, **Multi-Party Computation**, **(A)symmetric Encryption**, **Homomorphic Encryption**, **Deniable Encryption**, Anonymous Buyerseller Watermarking Prot., Verifiable Encryption, Feedback Tools for User Privacy Awareness, Data Removal Tools	**k-anonymity**, Suppression, Recoding, Aggregation, Swapping, Noise Masking, PRAM, Synthetic Data, Group Signatures, Global Differential privacy
⋮		
Detectability (Messaging)	**Mix Network**, **Steganography**, **Deniable Authentication**, **Dummy Traffic**, ISDN-Mixes, Onion Routing, Tor, Crowds Low-Latency Communication, Java Anon Proxy, Covert Communication, Spread Spectrum Off-The-Record Messaging, Mixmaster Type 2 Mixminion Type 3, Single Proxy, Anonymous Remailer, DC-Networks	**Mix Network**, **Steganography**, **Dummy traffic**

Fraunhofer AISEC

Conclusions

Summary

- Systematic classification (protection goal, metric, functional scenario, maturity, performance impact, architectural impact, utility impact)

Future Work

Fraunhofer AISEC

Conclusions

Summary

- Systematic classification (protection goal, metric, functional scenario, maturity, performance impact, architectural impact, utility impact)
- Comparison with LINDDUN

Future Work

Fraunhofer AISEC

Conclusions

Summary

- Systematic classification (protection goal, metric, functional scenario, maturity, performance impact, architectural impact, utility impact)
- Comparison with LINDDUN

Future Work

- Maintain and extend classification

Fraunhofer AISEC

Conclusions

Summary

- Systematic classification (protection goal, metric, functional scenario, maturity, performance impact, architectural impact, utility impact)
- Comparison with LINDDUN

Future Work

- Maintain and extend classification
- Integrate into threat modeling tools

Fraunhofer AISEC

Conclusions

Summary

- Systematic classification (protection goal, metric, functional scenario, maturity, performance impact, architectural impact, utility impact)
- Comparison with LINDDUN

Future Work

- Maintain and extend classification
- Integrate into threat modeling tools
- In general: only few PET implementations have high maturity

Fraunhofer AISEC

Thank you!

Immanuel Kunz and Andreas Binder

{firstname.lastname}@aisec.fraunhofer.de