AppPETs

A Framework for Privacy-friendly Apps

M. Sc. Erik Sy
University of Hamburg

Privacy Enhancing Techniques Convention
Hamburg, 11th September 2017

Motivation

- Research is aware of techniques for data minimization such as:
  - Anonymous communication networks (ACN)
  - Private information retrieval (PIR)
  - Attribute-based credentials (ABC)
  - Secure multi-party computation (MPC)

- These techniques have an overhead regarding computational complexity, time delay or amount of data traffic

- Can we create prototypes where it is reasonable to use privacy enhancing technologies (PETs) in apps?
  - How do we make these techniques easier accessible for other app developer?

Anonymity types

- App developer perceive anonymization techniques as a mean to data protection[1]

Sender anonymity	Data file anonymity
Receiver anonymity	Data modification anonymity
Server anonymity	Query anonymity

- Encryption strategies and ACNs contribute to 5 of theses anonymity types

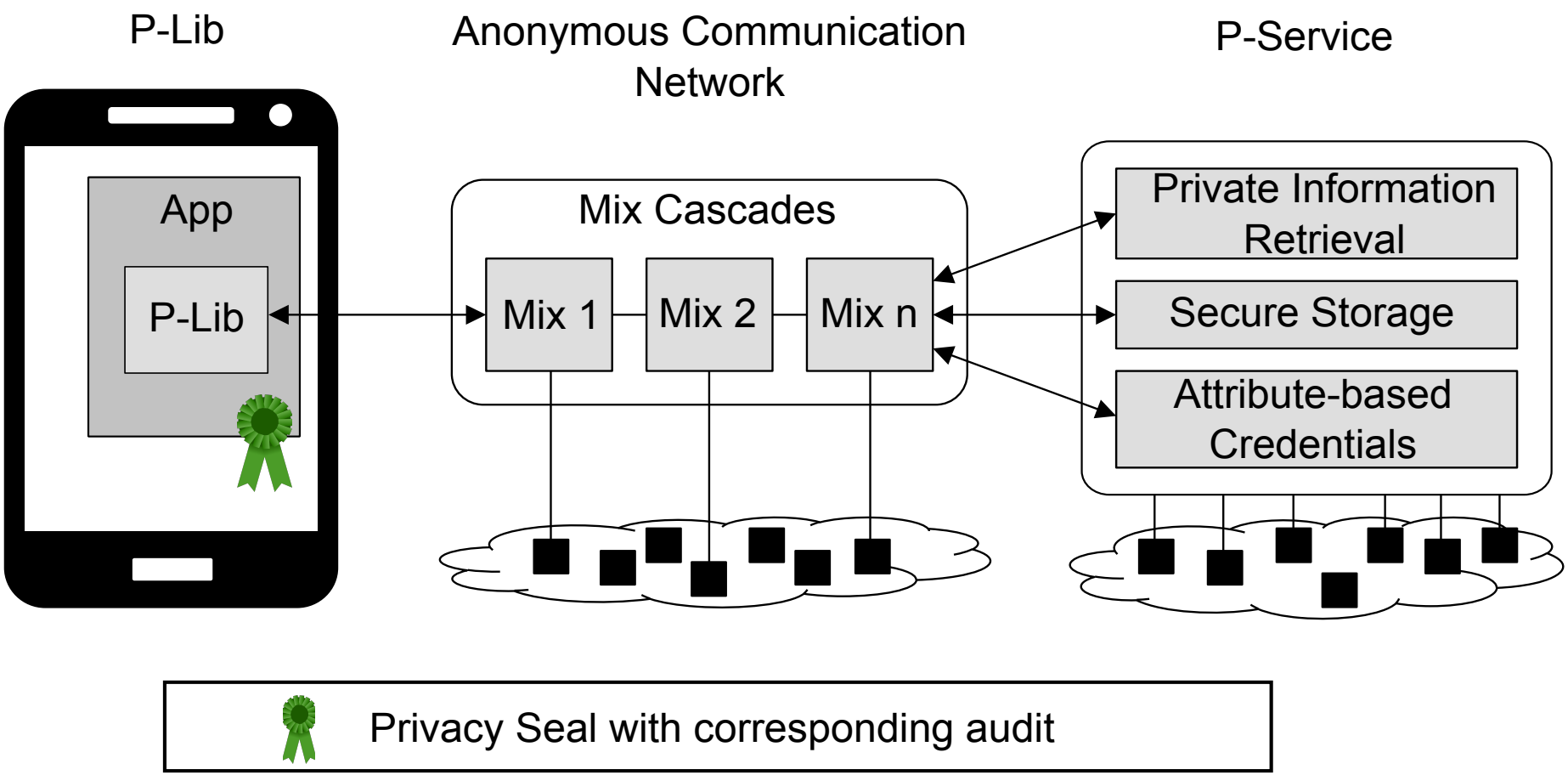
[1]: Swapneel Sheth, Gail Kaiser, and Walid Maalej. Us and them: a study of privacy requirements across North America, Asia, and Europe. 2014

Use cases for ABC, MPC, and PIR on mobile devices

- Authentication of attributes of a user account like age or payment status without revealing additional information about the user (ABC)
  - Requires trusted third party
- Calculation of distance between two locations without revealing the geoposition (MPC)
  - Issues with active probing
- Hide popularity of a file from the server (PIR)
  - Overhead increases with the size of the database

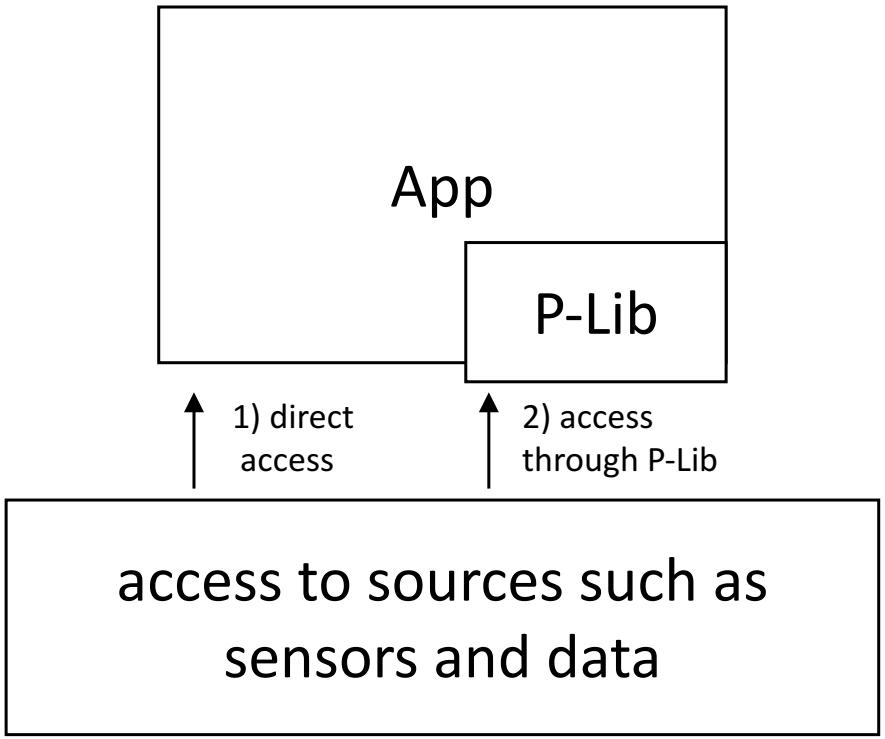
- Many apps have use cases suitable for encryption strategies, ACNs and ABCs
- Marginally PIR and MPC can be integrated into existing apps

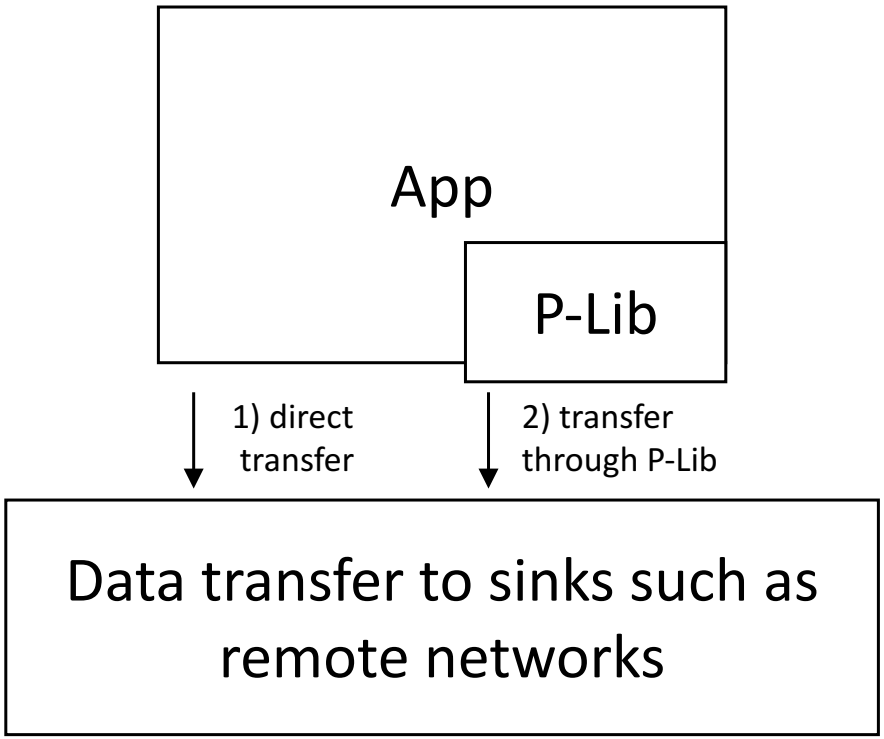
Design of the AppPETs infrastructure



P-Lib

- Implementation of PETs for mobile device





P-Service

- Provide the server-side implementation for certain PETs such as PIR, MPC, ABC or secure storage
- Services are hosted in a distributed infrastructure similar to ACNs such as JAP, which reduce the chance of colluding server

Audit

- Optional app audit which inspects security and privacy aspects of the app
- Validates whether an app fulfils a certain data protection guideline
- Audit combines static and dynamic app analysis
- Results of automatic audits are published (www.androlyzer.de)
- A privacy seal will be given to apps, which successfully undergo a charged audit (including manual analysis)

Future Work

- Implementation of PETs for mobile devices
  - Prototypes for secure storage and ACNs are implemented for iOS and Android
  - P-Service which supports ABC (planned)

- Automatization of the security and privacy app audit
  - Audits can be realized for iOS and Android apps
  - Increasing coverage of audits (planned)

Conclusion

- Encryption, ACNs and ABCs have many use cases in popular apps
- An distributed infrastructure is required to make PETs like ABC, PIR, MPC usable for app developer
- Security and privacy audits should be an inherent part of app development