Why does this app need my Location? Context-Aware Privacy Management on Smartphones

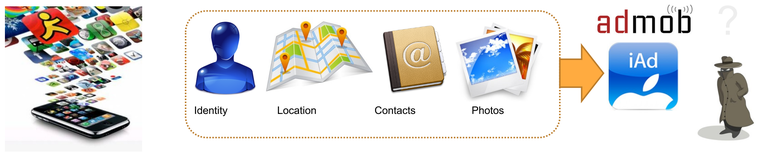
Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I. Hong, Yuvraj Agarwal
schitkar@andrew.cmu.edu, yuvraj@cs.cmu.edu

synergy
systems, networking and energy efficiency

android.protectmyprivacy.org/

Carnegie Mellon University

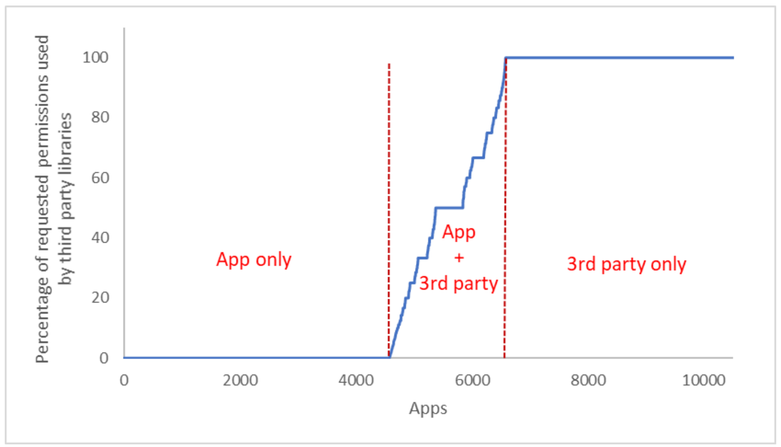
Motivation



- **Purpose of Data Access?**
  - Why is the private data needed?
  - Where does the data flow?
- **Decision Overload**
  80 Apps * ~ 5 Permissions => 400 Decisions
- **App Level Controls**
  Can not allow data access on the basis of functionality

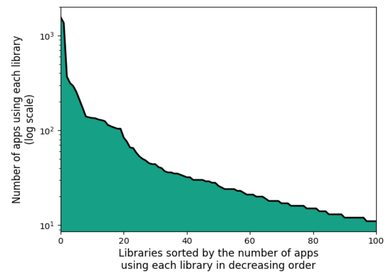
Third-Party Libraries

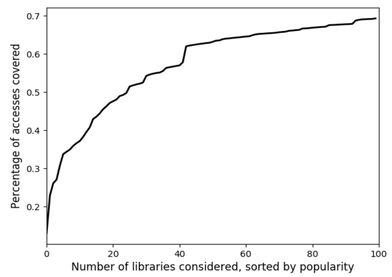
- **Routinely Used**
  - Provide functionality like *Targeted Ads*
- **Run with the same permissions**
  - The libraries can collect any data requested by app



- Libraries are even solely responsible for data collection!

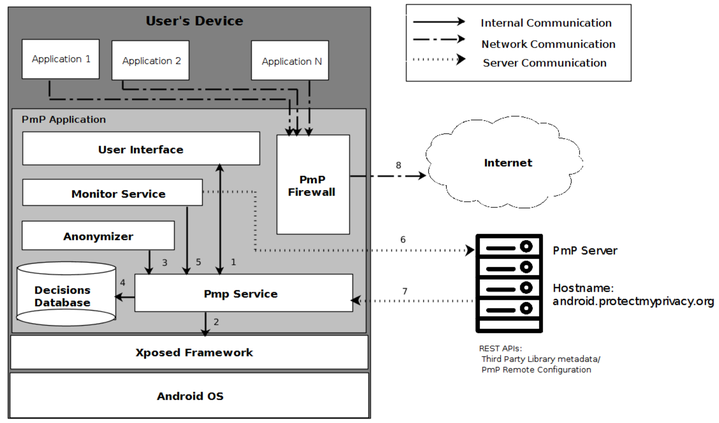
{App, Permission, Purpose} controls

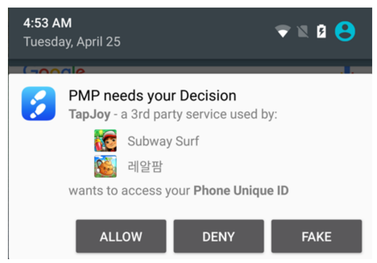


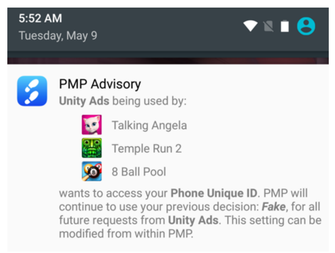


- **Limited set of libraries matter**
  - Only 30 libraries are responsible for more than half of the accesses to ALL sensitive data.
  - Library purpose can be easily mapped
- **{App, Permission} + {Library, Permission}**
  - Separate out data flows between app and library

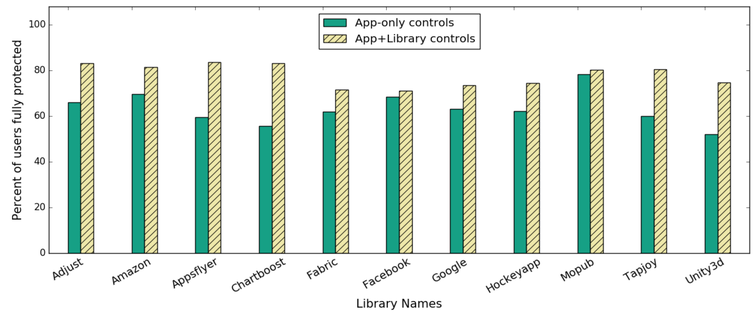
Protect My Privacy App

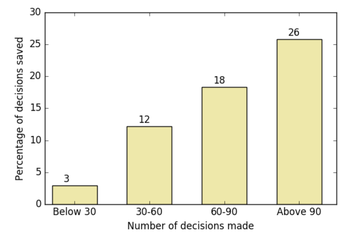






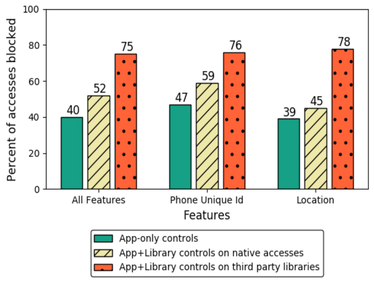
Results



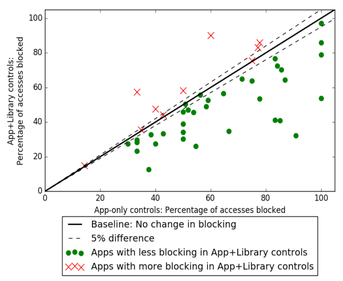


- 1300+ real world users
- 25% more users fully protected!
- 26% reduction in user decisions

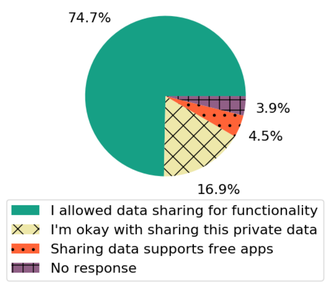
Analysis



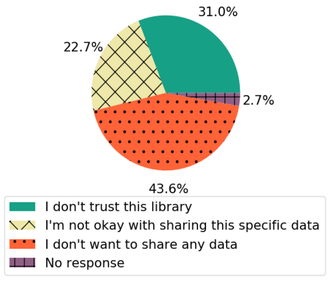
Overall Trend: Users block more decisions



Long Term Users: More comfortable in allowing data to app developers



Why did the users allow data to libraries?



Why did the users block data to libraries?

Full Paper: http://www.synergylabs.org/yuvraj/docs/Chitkara_Ubicomp2017_ContextAwarePrivacy.pdf