What are parental control apps?

Parents can monitor the phone usage of their children as well as set rules.

Methodology

- Static analysis:
  - Backstage and Cartographer[3,4]
  - We extract information flows, URLs, libraries and UI elements

- Dynamic analysis:
  - Lumen Privacy Monitor[5]
  - Lower bound on data leaks by an Android app

- Privacy policy analysis:
  - Polisis[6]
  - Semiautomatic analysis of privacy policies

Private information harvesting

- Highly intrusive apps by definition
- Must have parental consent
- Must not share private information

Motivation

- Previous work, dynamic analysis using TaintDroid[1,2]
- We analyzed 7 apps and found:
  - One app gathers private data before parental consent
  - Two apps disseminate private data already stored on the device
  - Two apps share location and web history with third parties
  - Four apps send PII s over an insecure channel (no TLS)

Goals

- Report possible COPPA and GDPR violations
- Map privacy policy to actual behavior
- Shed light on a highly intrusive yet not studied type of mobile apps

Early results

- Private data flows in 33 apps
- Non COPPA compliant libraries in 8 apps
- 12 weeks of privacy policies stored

Ethical considerations

- At no point in this study have we gathered private data from real users.
- All data is generated using fake accounts controlled by us.

References