Location Privacy Protection
For Smartphone Users

Thanks to Kassem Fawaz and Kang G Shin
Presented By Sam Ostoich and Erin Geoghan
Introduction

- Problem
- Threats
- Related Works
- Design Philosophy
- Design
- Implementation
- Success?
- Future Plans
Location-Tracking Apps

- Help you get where you want to go
  - Navigation apps

- Used to stay connected with friends
  - Social media apps

- Used for convenience
  - Find nearest gas station, restaurant, etc.
Examples
Users care about who accesses their location
Threats

● Tracking Threat
  o Adversary can receive continuous location updates

● Identification Threat
  o Adversary can isolate the user’s frequency

● Profiling Threat
  o Adversary can profile the person based off where user has been
Related Works

- **MockDroid** - disables access to certain resources such as location
  - Problem: never receives location updates

- **Micinski** - coarsened the location
  - Problem: never considered threat model
Related Works

- PlaceMask - allows user to supply fake locations
  - Problem: fake locations are given when real locations are needed

- Koi - cloud-based service for location protection
  - Problem: have to use a different API based on different location criterion
Related Works

- Deficient in terms of effectiveness, efficiency, and practicality
  - MockDroid - effectiveness
  - Koi’s method - practicality

- Solves tracking threat but not profiling or identification
Design Philosophy

- User expects location to be accessed
- Location with a granularity sufficient to produce location-based functionality is provided
- Anonymous apps can’t identify user based on frequently visited places
- Single app alone poses no significant profiling threats
Design Philosophy

- App can’t track user all the time
- Existing mobile ecosystem is used
- Protection comes at a minimal cost in usability and app functionality
Design
Design

Little effect on the functionality of most apps
Design
Design
Implementation with Android

- LMS and GMS
- Location object with context
- Changing context

Figure 4: Location access mechanisms in Android (left & middle) and LP-Guardian’s deployment within Android (right)
User Interface

- Bootstrapping
  - Setting most visited places
  - Setting the anonymization rule for each app

- Per-place/session controls
  - Setting the anonymization rule for each location
  - Setting changes available at all times to the user
Assessment

- Blocks location access in the background
- Most apps can’t track for more than 8 minutes per day
- Stationary vs Mobile effect

- Weather apps
- Messaging/chatting apps
Energy Assessment

![Energy Overhead Graph]

- **5s-plain**
- **5s-Guar**
- **No loc.**
Overall Success?

- Practical - easy to employ, compatible with apps
- Effective - Addresses the three threats
- Efficient - privacy with tolerable loss in app functionality
Future plans

- User friendliness
- Incorporating it as a custom ROM
Questions?