On Usable Location Privacy for Android with Crowd-Recommendations

Benjamin Henne[#], Christian Kater[#] and Matthew Smith[♭]

[#]Distributed Computing and Security Group
Leibniz Universität Hannover, Germany
henne@dcsec.uni-hannover.de

[♭]Usable Security and Privacy Group,
Universität Bonn, Germany
smith@cs.uni-bonn.de

Massive use of location-based services on mobile devices

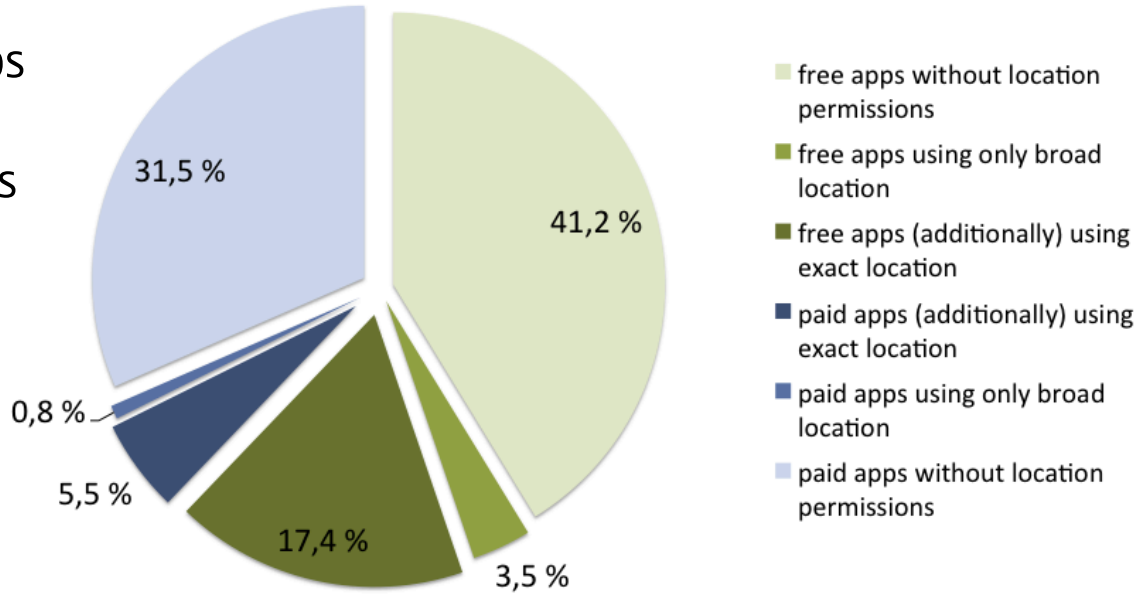
- Still rising adoption of smartphones and tablets entails an increasing use of location-based services ranging from location sharing to the retrieval of location-based information
  - "***74 %*** *of US smartphone owners use their phone to get real-time location-based information*"
  - *"18% of US smartphone owners use a geosocial service to* check in *to certain locations or share their locations with friends"*

(Pew Internet & American Life Project, May 2012, http://pewinternet.org/Reports/2012/Location-based-services.aspx)

- Very different apps adapt location today
  - Navigation, location sharing, geo-tagging photos, local news and weather, local radio stations, find a café nearby or cheapest gas station in range, get schedule of next bus stop, local game high scores, fitness, …, and **ads.**

Location use of Android Apps

- In June 2013, **27.2 % of** 20,681 **Android top apps** found at the Google Play Store on the Web required access to location data
  - 17 % of top paid apps
  - 34 % of top free apps
    - many of those might use location for advertisement



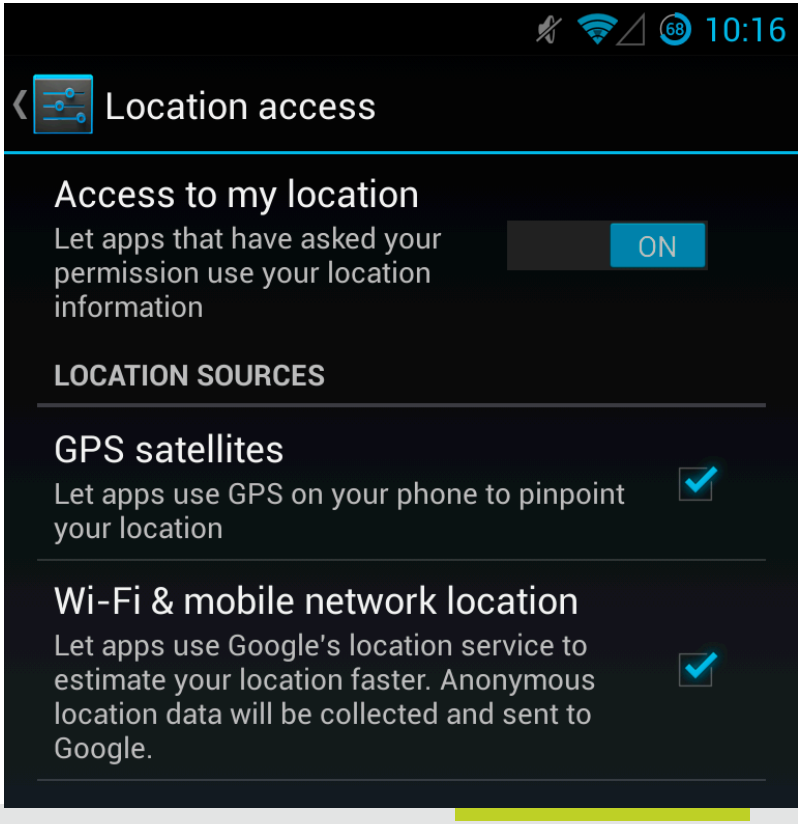
Surveillance Threat by Apps

- If users reveal their location to an app, they **always** reveal it with **full precision** even to those that do not need high accuracy
  - ✓ Navigation software needs full precision
  - ! Weather forecast services for instance do not!
    - example: Clock widget *cLock*

```
HTTP GET
http://query.yahooapis.com/v1/public/yql?
q=select woeid from geo.placefinder
where text="35.337201 25.386001"
and gflags="R“
```

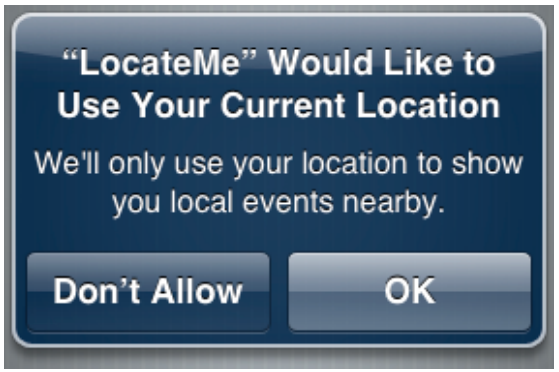
Android Location Features

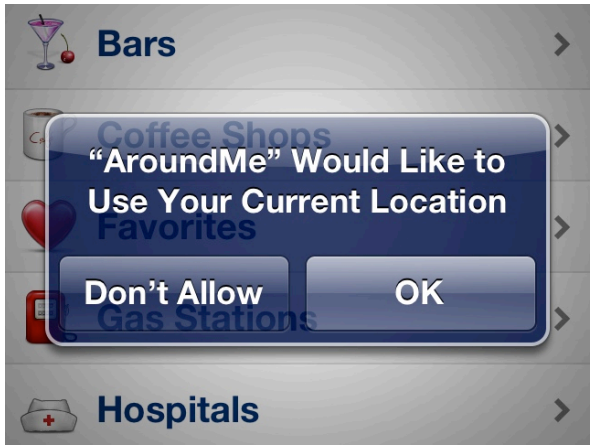
- Android users just can enable/disable location use **for all apps at once**
- Android distinguishes between exact (GPS) and broad (Wi-Fi) location
  - developers define permissions required by an app to be installed
    ⇒ developers determine precision of disclosed data
  - users just control location sources
    ! even "broad" Wi-Fi location create threats to privacy

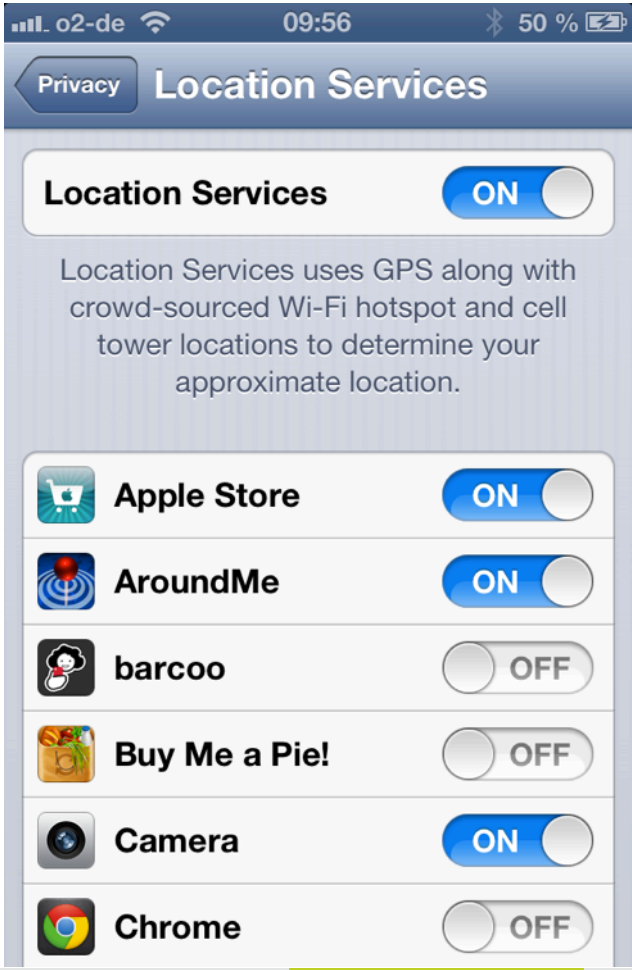


Apple iOS Location Features

- iOS allows users to enable/disable location use **for all apps at once**
- Additionally features **per-app** configuration
- On first location request of an app, a dialog asks the user about the per-app location privacy setting
  - + including optional purpose of location request







How can we preserve location privacy?

- Many apps that request location, but do not need it to function as expected by the users – preventing access is ok here *if possible*
  - *Apple iOS; research: AppFence, MockDroid; Android Cyanogenmod: Privacy Guard*

! However, there are many location-based apps users want to use, but they still have privacy concerns!

⇒ Since many apps would work equally or similarly well with a more rough positioning, we can **improve privacy** by only **disclosing location only** in such **detail as needed** by an app **to function as requested**

- ***Nothing new to research in general, but still missing in real world systems***
- *No mobile system allows any kind of location obfuscation up-to-now*

One reason for missing adoption: Usability!

- Many obfuscation techniques might be hard to understand for users
- Users might not be able to appropriately configure parameters
  - Hard to realize what k=20 means in daily life k-anonymity
  - Even hard to realize the effect of randomly shifting location up to 500m
- Users might not be willing to think about technical details at all
  - Rather interested in obfuscation results
    – but independently of any algorithm concept?
- For users, it might be hard to determine what exactness an app needs to function as expected

Focus Group Study: What do users really want or need?

- Identify users' experiences, requirements, worries and wished towards location privacy and current systems
- Invited 1,510 people from university study mailing list for group discussion on "daily use of mobile apps"
  - Guided discussion to location use and finally to privacy for avoiding bias
- Compiled 3 balanced discussion groups from 98 answers
  - Each discussion took about 90 minutes; 20 € compensation per person
  - 11 female, 8 male; aged 24±4 years; from 14 fields of study
  - 12 Android users, 7 iOS users
  - 9 privacy fundamentalists, 10 pragmatists (Westin's privacy segmentation)
  - diverging technical expertise

FGs: Usage Habits of Location-aware Apps

- All participants reported to use some kind of location-aware apps
  - Navigation, maps, weather report, public transport timetables, …
  - 6 of 19 reported to share location occasionally
- Most participants use location services selectively
  - iPhone users utilize per-app configuration
  - Some Android users resorted to turning services on/off prior to app usage
- 4 participants reported not using location services
  - 3 did not want to be observed by "others" or apps
  - 1 iPhone user was annoyed of location request pop-ups
- Battery drain was second most common reason for selectively enabling
- Convenience was major factor for using although feeling being observed

FGs: Experiences and Requests

- Most iOS users stated to be fairly satisfied
  - One user requested to get to know each app's last location usage
    - Feature exists, however only reports rough "recently"/in last 24h use
  - One user requested apps to specify purpose of location use
    - Other participants rejected: They would not trust developers
- Android users requested **transparency** of information usage
  - Even if not regularly checking
    1. They stated to presumably feel better to be able to
    2. This "should make developers use location more prudently"
  - Over half of them request **per-app** settings
  - Most of them liked **direct feedback** of pop-up dialog
    - Android's Settings app was felt to be very complex

FGs: Inaccuracy of Location

- FG#1: One participant of herself suggest the reduction of accuracy
  - Finding the next bus justifiably needs her exact location, while "her current city would be entirely enough when looking for local shopping coupons"
  - FG#1 discussed two levels of detail: *precise* and *imprecise*
  - Just 1 participant worried about complex settings
- In discussions, FG#2/3 appreciated an imprecise option as well

- Most participants stated to prefer using the imprecise option where possible
- There were different opinions on what would be a good level of imprecision
  - Depending on use case (search restaurant nearby, geo-tagging Facebook posts)
  - City, district, 1 kilometer, …

FGs: Obfuscation Mechanisms

– a briefly discussion in the end

- Fixed (self-determined) locations were perceived as inadequate but for "tricking others concerning their whereabouts"

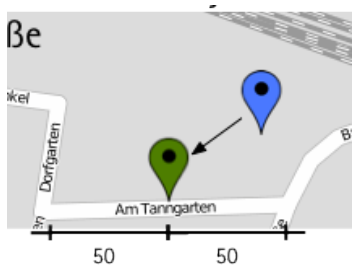
- Random Shifting was criticized, because of its "random" nature; disclosed location "could be at an absolutely unrelated" or "even inadequate place"
  - also applies to rounding or cutting decimal places

- Participants were interested in the concept of k-anonymity, BUT clearly disliked that obfuscation of their location depends on other users' location
  - \+ effective obfuscation "in meter" is hard to predict

FGs: Obfuscation Mechanisms (2)

– a briefly discussion in the end

- Participants mostly liked Mapping to Geographic Objects, at which their current location is mapped to center of the next street or urban district
  - perceived as most intuitive and easy to grasp
  - parts of them fully accepted to share their real location with a single online map service
  - while others rejected using any external service



- Conclusions
  - Users want to be able to control location accuracy
  - Disclosed location should be inaccurate, BUT Inaccuracy should be predictable and understandable to them

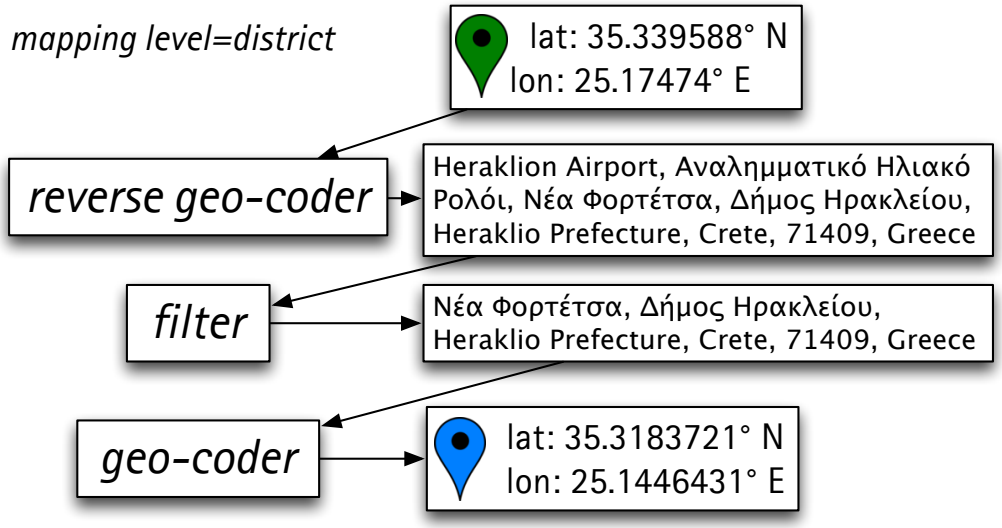
Usable Location Privacy for Android

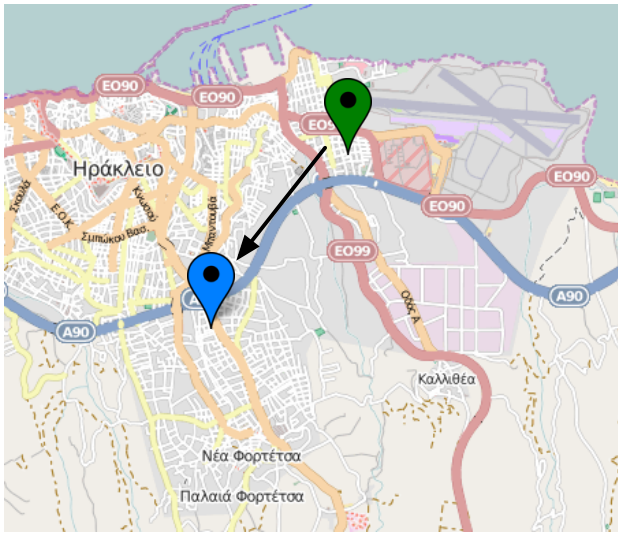
- Based on findings from focus group discussions
- Built on top of Location Privacy Framework for Android[1]
  - ✏ Henne et al.: Selective Cloaking: Need-to-know for Location-based Apps. 11th Annual Conference on Privacy, Security and Trust (PST), July 2013.
- Per-app location privacy settings
  - Allow access to exact location
  - Deny access to location data
  - Select from 3 different levels of location detail (obfuscation)
- Two alternative obfuscation mechanisms
- Statistics about location usage creates transparency
- Uncertain users are supported in configuration by "what others chose"

[1] http://bhenne.github.io/android-location-privacy/

Obfuscation: Geo-data based mapping

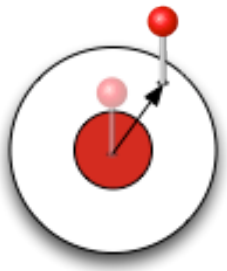
- Maps real location of user to center of nearest geographic object of user selected type of objects
  - Using Android's Geocoder API, alternatively any other free map service
  - Shares location with a single service, but apps get obfuscated locations
- Implemented levels of detail: *city*, *city district (village)*, *street*
  - **Users just select the level of detail for an app**





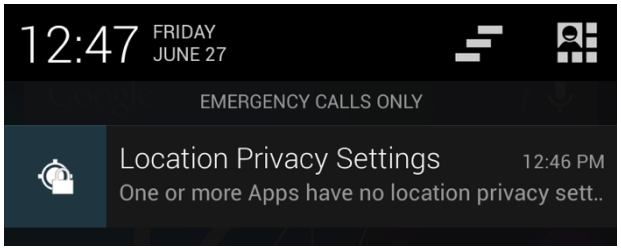
Obfuscation: Random Shifting – "Offline mode"

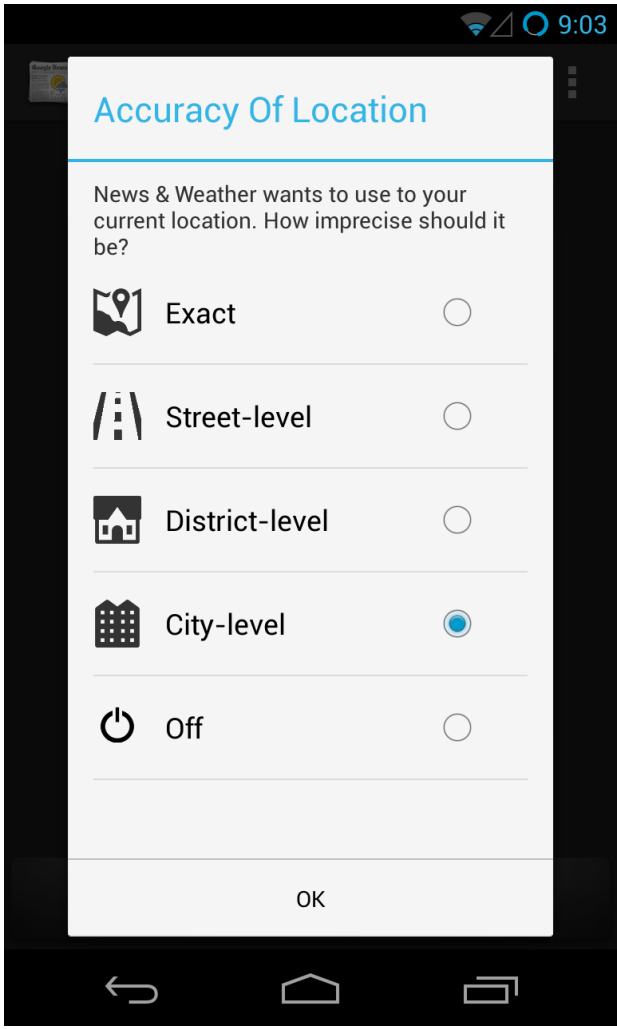
- Alternative mechanisms that completely operates on the device
- Approximating Geo-data based mapping?
  - Geo-data size and algorithm complexity does not fit on mobile devices
- Decided for Random Shifting in random direction
- Specifying minimal/maximum distance
  - Metaphors like "city block" or "playing field" differ across cities, countries, sports and even sport associations – does not fit
  - Decided to re-use the 3 levels *city*, *district* and *street* *(keep it simple!)*
    - User could enter corresponding values **manually**
    - Configure distances using a configuration **wizard**
      - Select representative city, pin some locations on a map
    - **Learn** values from mean obfuscation after having used geo-data mechanism for some time



Usable Location Privacy for Android – UI

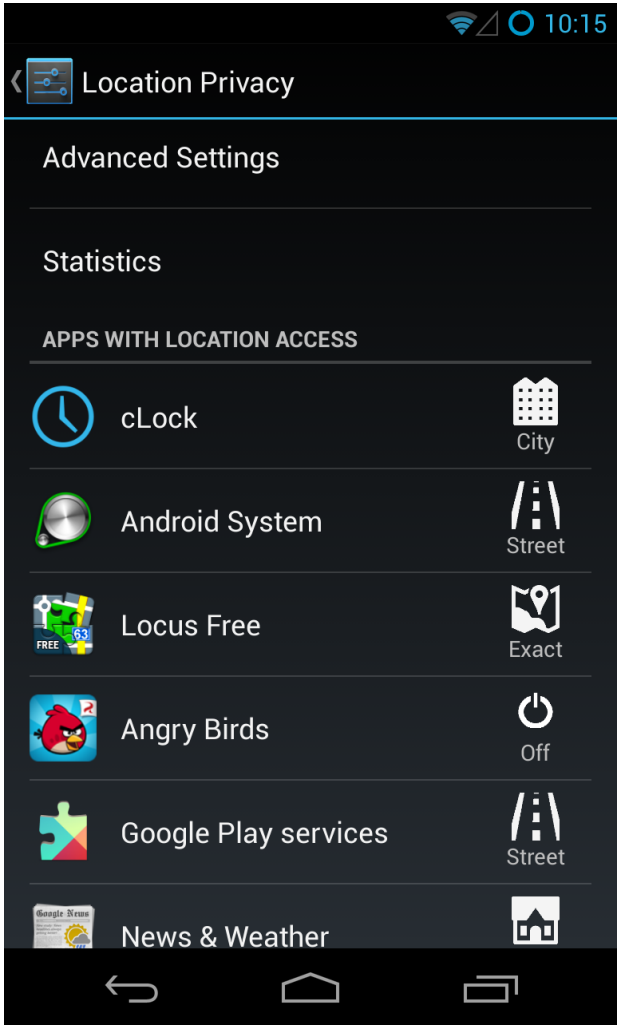
- iOS-like pop-up dialog asks for location accuracy when an app request location data the first time
  - Select one of 5 levels of location detail
- If users cancels (e.g. via home button), no data is disclosed to app until configuration was made
  - Android notifications remind user to configure





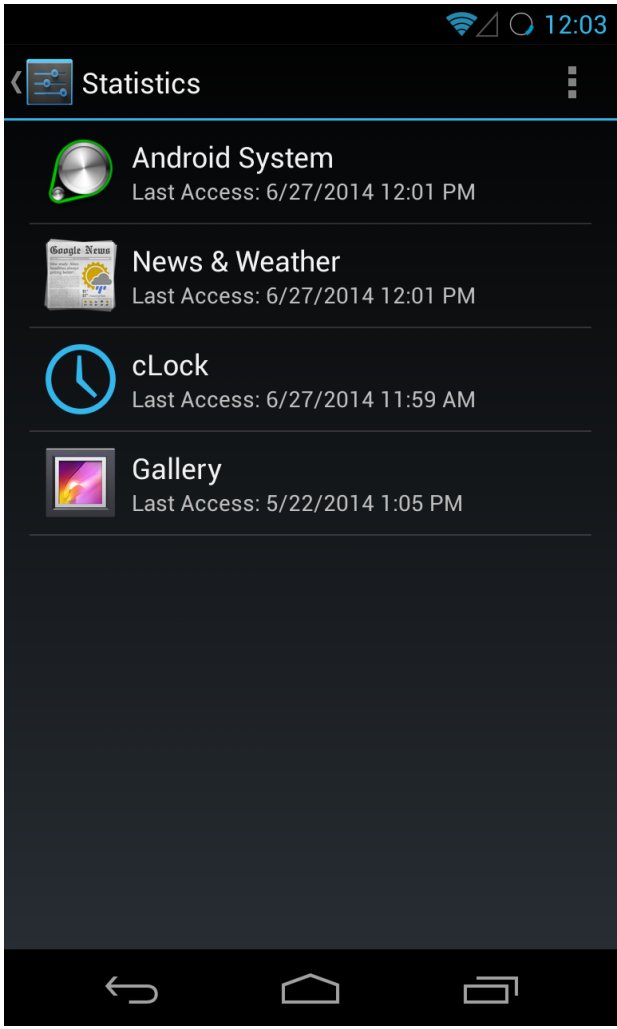
Settings App

- Configuration via Android app Settings
  - App overview instantly shows configured accuracy for each app
  - Advanced Settings
    - Switch online/offline obfuscation
    - Configure offline obfuscation
    - Configure Recommendations/ Sharing of settings



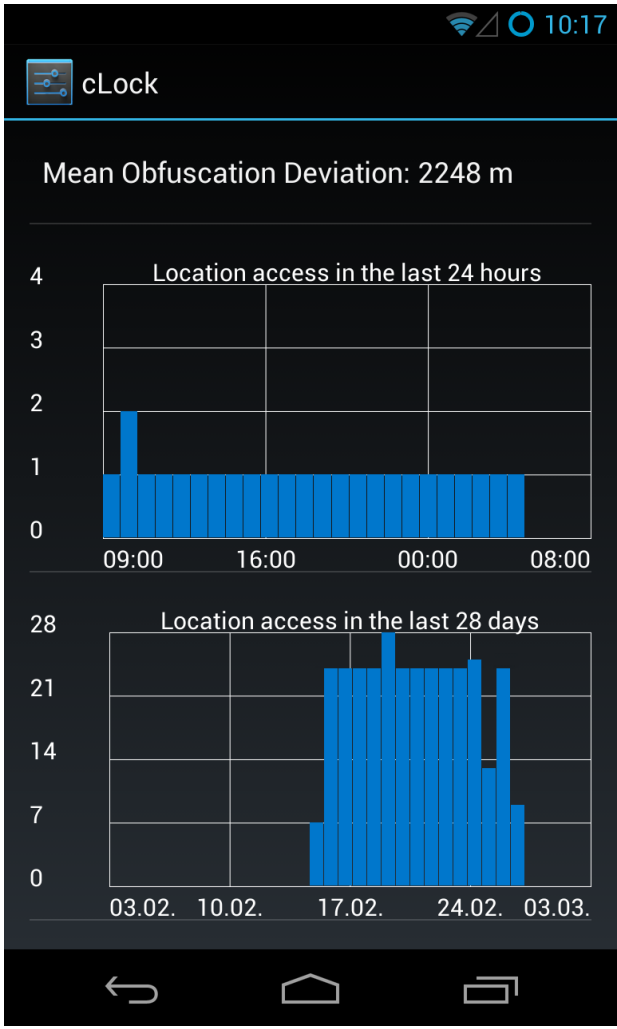
Statistics – Transparency of Location Usage

- Main view shows last location access of all apps having requested location data
  - Ordering by last access
    shows latest tracking by apps
  - Ordering by access count
    identifies data-hungry apps
- No information about disclosed location itself
  - would create additional threats to privacy



Transparency of Location Usage – App Details

- Detailed view allows for investigating an app's tracking behavior
  - past usage: 24 hours, last 4 weeks
  - how often
  - how regular
- *Mean obfuscation deviation* shows mean distance between real locations and locations given to the app
  - Shows effect of configured level of detail



FGs: Supporting Configuration / Decision Making

- Users have to decide which level of detail fits best to their privacy needs while being able to appropriately use location-based features of apps
- **Nobody else should make privacy decision for the participants, but they confirmed to ask others if they were not able to decide**

Discussed Ideas

- Recommendations based on privacy profiles like "concerned", "post privacy" – hard to create due to few levels and diversity of users/apps
- App categories like "games" – rather complicates configuration efforts
- Online communities are mistrusted, being manipulated by app developers
- Recommendations by public non-profit organizations
  - Consumer advice centers, IT security associations

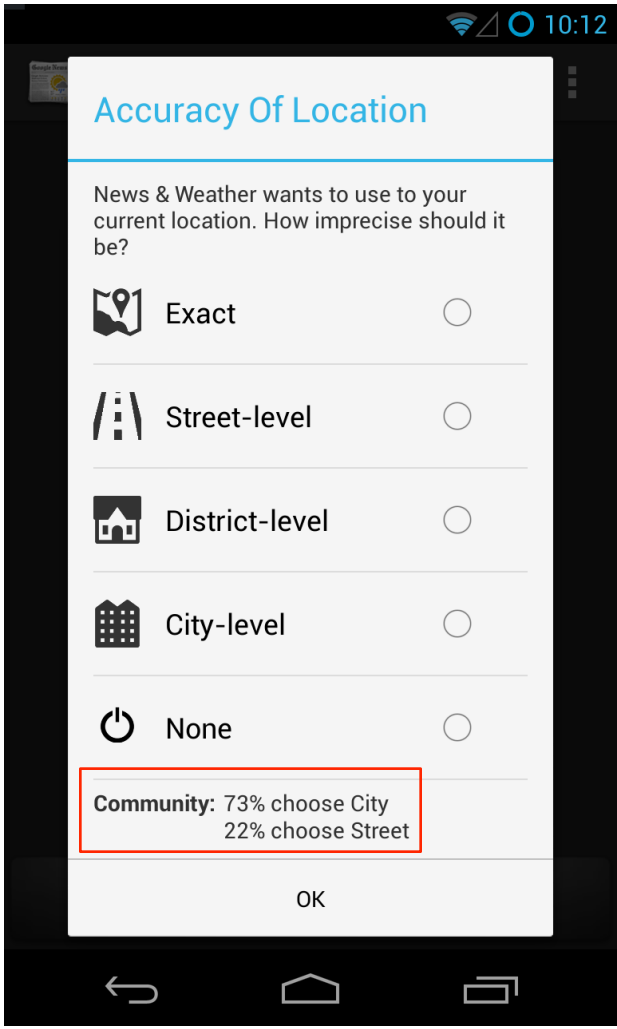
! Any Central service could just give advice for a subset of all app
  - Like recommendation for top-1000 apps

Supporting Decision Making by "what others chose"

- Crowd-based social service shows users what other users chose for an app as privacy setting
  - most adaptive to changing landscape of apps
  - covers any app that is used by some people

Implementation

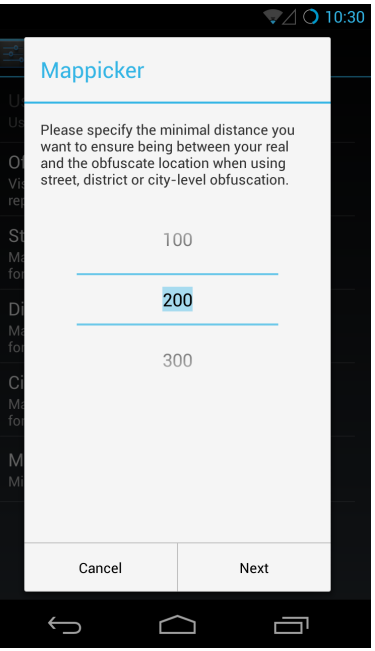
- If a user is asked to configure a new app, the most common selections of others are displayed
- User MUST select own option
- If users configures app, his configuration is anonymously shared with others
- In *offline mode* numeric values of levels are used to map others' levels to own levels

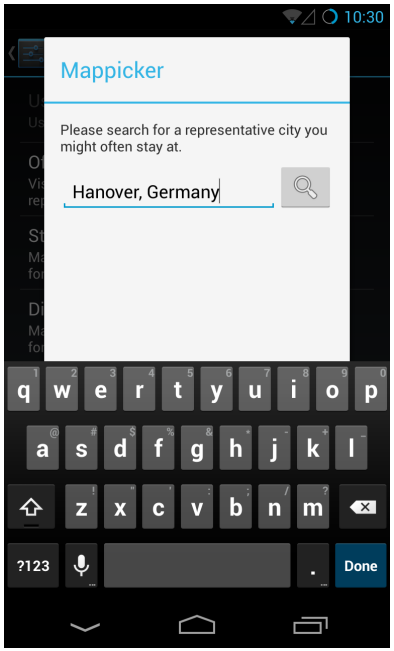


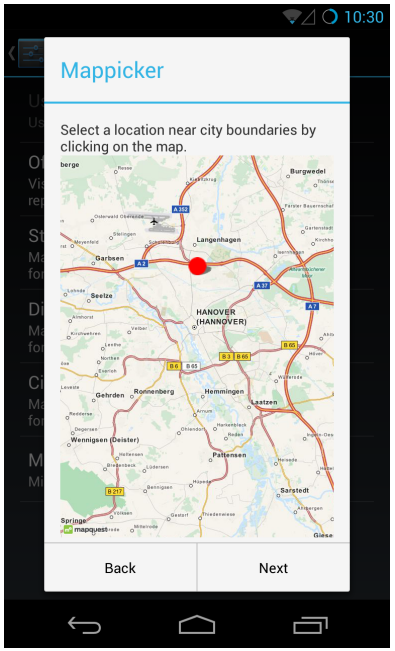
Conclusion

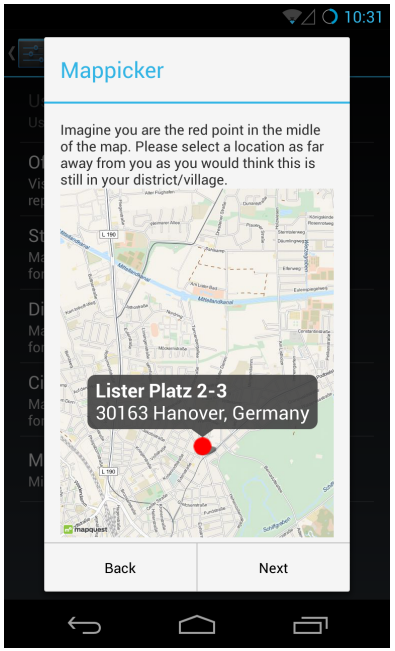
- Based on focus group results we implemented location obfuscation for Android
  - https://github.com/bhenne/android-usable-location-privacy
  - It implements simple but sufficient obfuscation that fits users' needs
    - ! Study participants rejected—from their point of view—complex or unpredictable algorithms like k-anonymity
  - The obfuscation configuration is simple as well
    - Once decide to allow the use of an online map service or not
    - Just select one of five options of detail for each app
  - Users that are undecided about what level of detail an app should receive are supported by information about what the crowd chose
  - Location access statistics create transparency about the potential surveillance threat raised by different apps

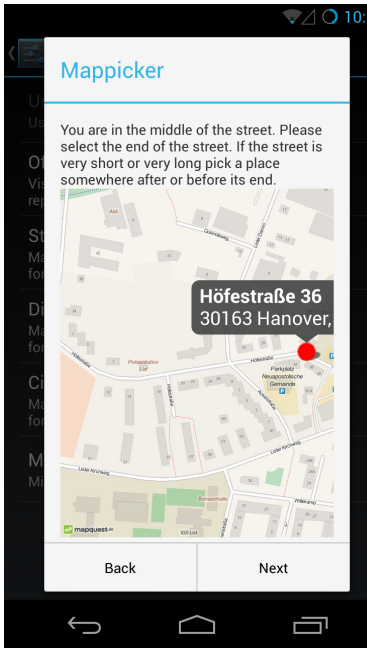
"Offline Mode" – Configuration Wizard

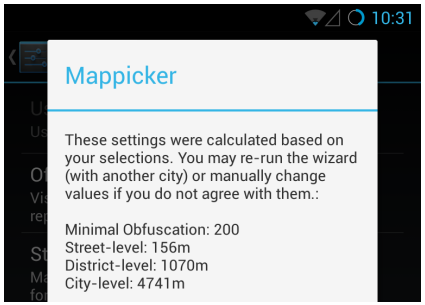












Crowd Service

1. If a user is asked to configure a new app, service is queried
2. Configuration pop-up displays most common selections of others
   - No pre-selection
   - Information is not displayed besides items to minimize influence
3. User selects his own configuration
4. His configuration is anonymously shared with service
   - Users are differentiated based on Google accounts
     - Google Play Services OAuth

- Current basic service implementation assumes users as equally skilled
  - ➢ Future work