HM Hochschule München University of Applied Sciences

Privacy-compliant heat maps of incidents and "unsafe" zones

Outline

1. Objective: Heat maps
2. Available and required data
3. Problem definition
4. Possible solutions
5. Local Differential Privacy vs Central Differential Privacy
6. Further considerations

SafeNow

Objective: Heatmaps

- **Goals**:
  - Provision of fine grained statistics on unsafe areas for zone operators
  - Evaluation of triggered attention modes and alarms

- **Advantages for the zone operators**:
  - Better insight into where security personnel should be positioned
  - Possibility of other improvements, e.g. more lights

SafeNow

Available and required data

- **Available**:
  - Alarms:
    - Start and end time
    - Start and end location
    - Corresponding user -> not transmitted to zone operator
  - Attention mode:
    - Start and end time
    - Start and end location
    - Anonymized
- **Required**:
  - Path between start and end location
  - Pseudonymised user

SafeNow

Problem definition

- Privacy <-> data quality
- Differentiation between users is required for more informative value
  - 90% attention mode from the same person vs. many different people feel unsafe
- Path can be used to create a movement profile
- Determination of required sample size
  - Number of users
  - Number of alarms/attention modes

SafeNow

Possible solutions

1. Randomized Response

- Survey technique (1965, Warner)
- Proposed to decrease bias caused by nonresponse to sensitive questions
- Respondents use a randomization device (like a coin flip) not observed by the interviewer
- Introduces random noise to hide individual responses to ensure respondent privacy
- Protects the privacy of any individual respondent for a one-time data collection
  - Vulnerable to repeated collection

SafeNow

Possible solutions

1. Randomized Response

- Problems
  - Mapping of location data to randomized response
  - Repeated collection probable

“[the randomized response] privacy guarantee degrades if the survey is repeated—e.g., to get fresh, daily statistics—and data is collected multiple times from the same respondent. In this case, to maintain both differential privacy and utility, better mechanisms are needed”

- „RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response“ (2014), Erlingsson, Pihur, Korolova

SafeNow

Possible solutions

2. Google RAPPOR

- Based on Randomized Response
  - for repeated anonymized data gathering
- Basic Concept: Bloom Filter that contains all responses to determine the prevalence
  - a possible value is hashed and tested against the bloom filter
- Randomized reports yield usable aggregate insights
  - Analyzing trends without compromising user identity
- Technique and codebase open source for transparency and collaboration
  - But: GitHub-Repository was archived in September of 2023

SafeNow

Possible solutions

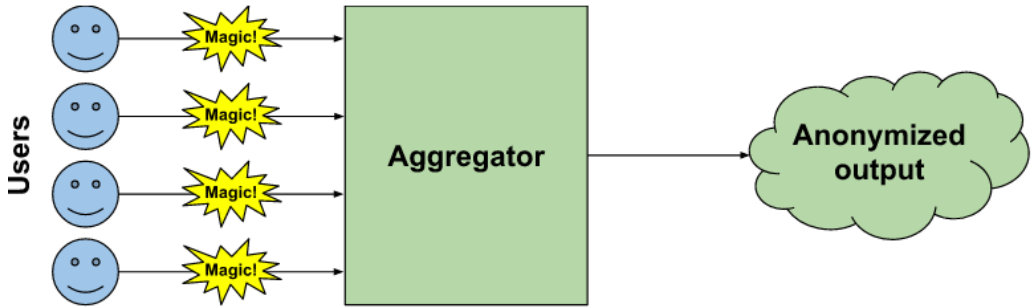
2. Google RAPPOR

- Possibly suited
- Problem:
  - mapping path to discrete values -> partition area into squares
- Transmission of sum of traversed squares
  - Additional benefit: masks exact path
- Further research is needed

SafeNow

Local Differential Privacy

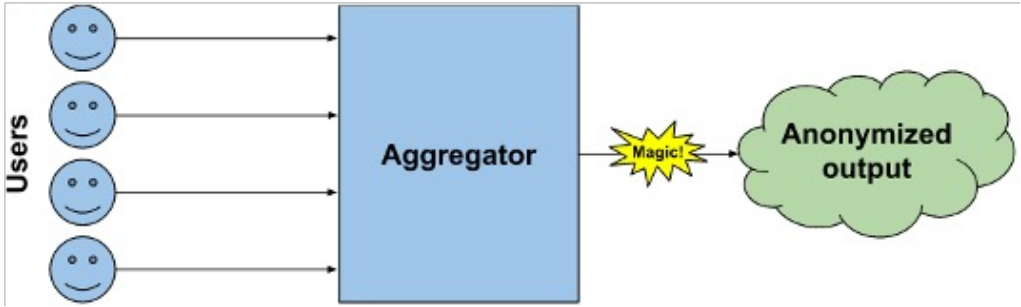
- The methods considered in this scenario are based on local differential privacy
- SafeNow would not need to have access to the data as it is randomized before transmission on the smartphone
- Would prevent data compromise in the event of a hack
- A drawback of this approach is that the data can be quite noisy



SafeNow

Central Differential Privacy

- The other possibility is central differential privacy
- Current data model of SafeNow
- More accurate data



SafeNow

Further considerations

- Local differential privacy vs central differential privacy
- Viability of new approach: “*ESA*: Encode, Shuffle, Analyze”
- Future support for Google RAPPOR
- Minimum number of required SafeNow users

SafeNow

Sources

[1] https://dimewiki.worldbank.org/Randomized_Response_Technique

[2] „RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response“ (2014), Erlingsson, Pihur, Korolova

[3] https://github.com/google/rappor

[4] https://desfontain.es/privacy/local-global-differential-privacy.html

[5] „PROCHLO: Strong Privacy for Analytics in the Crowd “ (2017), Bittau, Erlingsson, et. al