Blacklisting Spam Callers with Local Differential Privacy

Presented by: Joe-Ansel Puplava

Motivation

Spam phone calls have rapidly increased

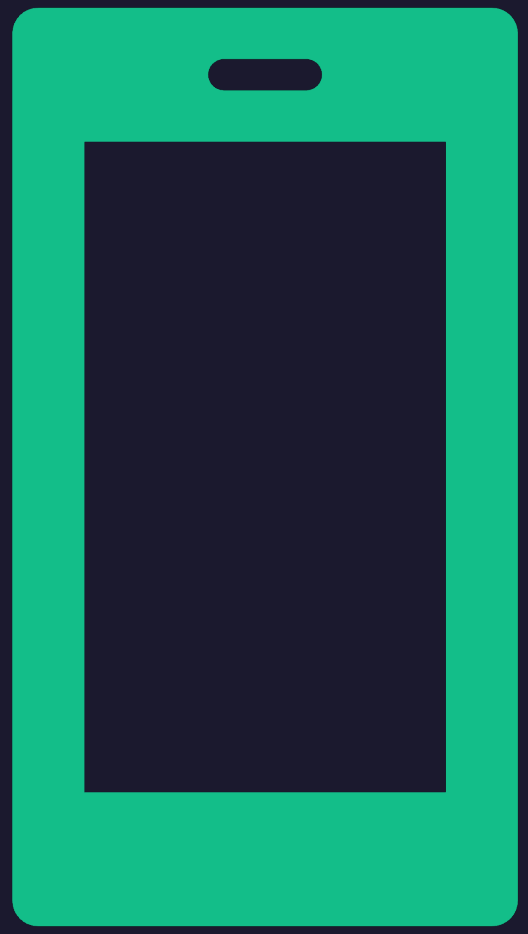
Technological advances made robocalls cheaper and easier

Efforts to counter this attack from the US FTC and various smartphone apps

Mostly rely on blacklisting known numbers involved in spamming calls

Problem

- Apps collect information that is private to the user
  - TrueCaller collects users' contacts to learn which callers are legitimate
- Phone honeypot records are not the reliable
  - Skewed towards business-oriented campaigns



Problem
Approach

Leverage Local Differential Privacy for generic heavy-hitter detection

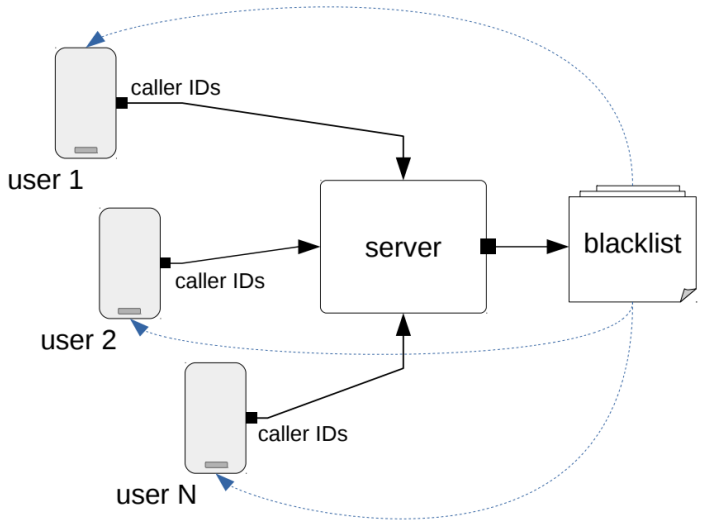


Figure 1: System overview. Caller IDs are collected with local differential privacy. After learning, blacklist updates are propagated back to users.

Implementation of LDP

- Uses The Succinct Histogram Protocol
  - A ε-LDP protocol for detecting heavy hitters over a large domain V
  - The protocol applies after a few modifications

1. Encode the item, X, into a bit string making Y
2. Add noise to the item, Y, making Z and send Z to the server
3. Aggregates noisy reports and rounds to the nearest valid encoding, Yi.
4. Decode the heavy hitter, Yi, into Xi

Algorithm 1: $\mathcal{R}_{\text{bas}}(\mathbf{x},\varepsilon)$: ε-Basic Randomizer

Input: m-bit string $\mathbf{x}$, privacy budget ε

Sample $r \leftarrow [m]$ uniformly at random.

if $\mathbf{x} \neq \mathbf{0}$ **then**

$$z_r = \begin{cases} c \cdot m \cdot x_r & \text{w.p. } \frac{e^{\varepsilon}}{e^{\varepsilon}+1} \\ -c \cdot m \cdot x_r & \text{w.p. } \frac{1}{e^{\varepsilon}+1} \end{cases}, \text{ where } c = \frac{e^{\varepsilon}+1}{e^{\varepsilon}-1}.$$

else

Choose z_r uniformly from $\{c\sqrt{m}, -c\sqrt{m}\}$

return $\mathbf{z} = (0, \ldots, 0, z_r, 0, \ldots, 0)$

Results

- Blacklist utility
  - Maximum budget of $\varepsilon = 15$
  - Reasonable utility with $\varepsilon = 10$
- It is possible to learn a phone blacklist that:
  - Preserves privacy
  - Maintains the utility of the blacklist

References

- "Stop Unwanted Robocalls and Texts." Federal Communications Commission, 30 January 2024, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts.
- Ucci, Daniele, et al. "Building a Collaborative Phone Blacklisting System with Local Differential Privacy." *Annual Computer Security Applications Conference*, 2020, pp. 100–15. *arXiv.org*, https://doi.org/10.1145/3427228.3427239.
- Bassily, Raef, and Adam Smith. "Local, Private, Efficient Protocols for Succinct Histograms." *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, 2015, pp. 127–35. *arXiv.org*, https://doi.org/10.1145/2746539.2746632.