CrowdMixer: Differentially Private Anonymous Communications

Alex Yang and Sebastian Angel, University of Pennsylvania

DISTRIBUTED SYSTEMS LABORATORY

Introduction

In the era of mass surveillance, there is a growing need for anonymous communications systems. Even if the content of anonymous messages is encrypted, adversaries can learn information through metadata such as who they are communicating with, the size of the messages, and the time of communication. The leakage of metadata itself compromises user privacy, posing a problem to individuals who require complete anonymity such as government whistleblowers and activists under repressive regimes.

Previous anonymous communications systems such as Vuvuzela[1] and Karaoke[2] are able to hide metadata, tolerate compromised servers, achieve scalability, and deliver messages with good latency. However, they still face two limitations: First, oftentimes the number of users of an ACN is very small, which makes connecting to the system inherently suspicious and less anonymous. Second, these systems only allow for ephemeral messages that are not retrievable over time. CrowdMixer aims to expand upon existing protocols to address these two challenges. The privacy guarantee can be quantified using the concept of differential privacy, which utilizes the parameters ε and δ. A low ε and δ indicates a higher standard of privacy for a user.

Project Overview

The overall goal of CrowdMixer is to build a system that meets the same standards as previous systems with the addition of 2 capabilities: increasing the number of users connected to the system and allowing messages to be stored for a set period of time. To achieve these goals, the CrowdMixer utilizes a heavily modified version of the Vuvuzela protocol with improved adaptive composition theorems[3] that generate the noise necessary for the storage of messages over time.

CrowdMixer also increases the number of users connected to the system through JavaScript code in a Chrome extension, creating involuntary “passive” users that are indistinguishable from real “active” users of the system. This thereby increases the anonymity set and makes the act of connecting to the system less suspicious. At the same time, we explore a more distributed server topography to spread out computational cost and significantly improve latency.

This system aims to meet standards of ε, δ differential privacy, with parameters for ε not exceeding ln(2) and parameters for δ not exceeding 1×10^{-4} over k rounds of communication. It is important to note that privacy guarantees are independent of the number of connected users.

Composition Theorems and Distributions

To calculate the degradation of differential privacy over multiple rounds, we use an updated k-fold adaptive composition theorem[3] over k rounds:

$$\varepsilon' = \frac{(e^{\varepsilon}-1)\varepsilon k}{e^{\varepsilon}+1} + \varepsilon\sqrt{2k\,\log\left(e + \frac{\sqrt{k\varepsilon^2}}{\tilde{\delta}}\right)}$$

Using the ε’ and δ’ parameters from this theorem, we then draw server noise levels from a Laplace Distribution[1] Laplace(μ - *c, b*) with *c* representing passive messages and *t* representing Laplace sensitivity, *t = 16.*

$$b = \frac{t}{\mu} \qquad \delta = e^{\left(\frac{2-u}{b}\right)} + \frac{1}{2}e^{\left(\frac{14-u}{b}\right)}$$

Finally, the time between noise message deposits and retrievals is sampled from a Poisson distribution with parameter λ = 3.5.

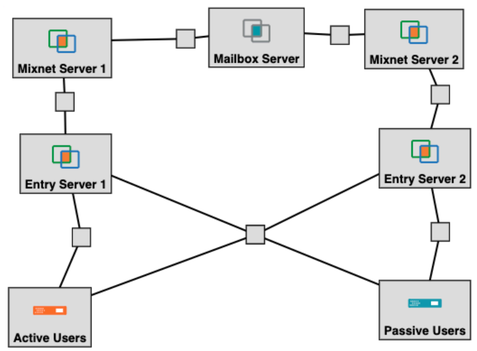
Protocol

CrowdMixer, which operates on discrete rounds each hour, is composed of entry servers, mixnet servers, and a mailbox server. For one active user to communicate with another active user, they must have a shared secret key. During the start of a round, both active users hash to an address in the mailbox server based on the shared secret key and the round number. Then, the messages are onion encrypted and sent to the entry servers. The entry servers generate fake noise messages (based off of the Laplace and Poisson distributions) and perform a random shuffle of the message order before sending them to the mixnet servers, which add more noise and perform another shuffle. Finally, the messages arrive at the mailbox server where the messages are exchanged and sent back down the chain. Active users then connect to the entry servers later in the hour to get their messages back.

If a user is attempting to retrieve messages from past rounds, they must hash to mailbox addresses using the shared secret and past round numbers, with the limitation that past messages are deleted after 6 hours of storage.

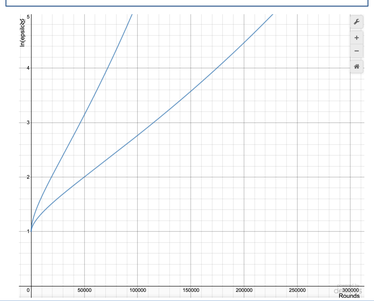
Passive users use the chrome extension to generate noise messages and mailbox numbers, which are then sent to the entry servers as long as the passive user has a chrome instance open. These messages are indistinguishable from active user messages.

Server Topography

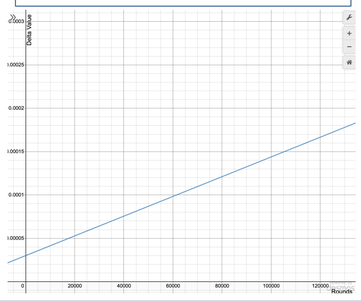


Privacy Degradation

Graph of ln(ε) over k rounds, μ *= 315,000*



Graph of δ over k rounds, μ *= 315,000*



Results and Discussion

In our chosen configuration, we aimed to preserve ε , δ differential privacy standards of $\varepsilon < \ln(2)$ and $\delta < 1 \times 10^{-4}$ with k = 50,000 rounds, which equates to approximately 5.7 years of continuous use of the system. We also assume that there will be *c* = 100,000 passive users, so we are able to scale down μ *to* μ *– 100,000.* The improved k-fold composition theorem[3] brings significant improvement to the noise generation, increasing the k rounds with $\varepsilon < \ln(2)$ from 19,300 to 50,000, which is 260% improvement over the previous composition theorem[4]. Furthermore, due to the more distributed server architecture, each side of the server chain only needs to generate 50% of the total noise message, allowing for significant latency decreases in the entry servers and mix servers. However, this comes at the disadvantage of increasing the total attack surface, since all servers are necessary for the functioning of the system.

Additionally, we find that the optimal noise level is μ = 315,000 and b = 15,000. Under these parameters, we ran 10 trial rounds on the CrowdMixer prototype for an average latency of 286.68 seconds for message processing, well within the 5 minute window that we are aiming for. We can improve the number of rounds k as well as the differential privacy bounds ε , δ, but at the cost of increased latency. As expected, the latency increases linearly with the number of noise messages.

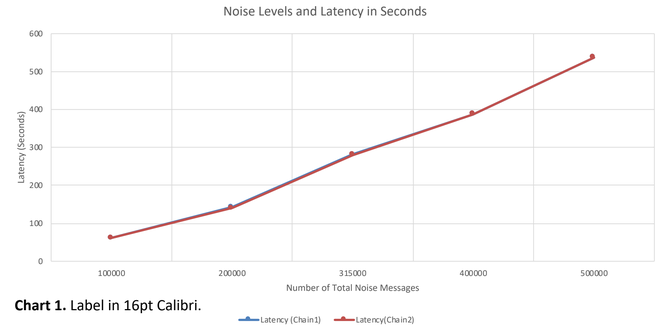


Chart 1. Label in 16pt Calibri.

Conclusions and Future Work

From our work, we can draw several conclusions:

- Bootstrapping existing anonymous communications systems to increase the size of the anonymity set is simple and does not add much overhead to passive user experience
- The chrome extension is also useful for making passive users responsible for noise generation, decreasing the load on the servers proportional to number of passive users
- Adding capabilities for non-ephemeral communications increases the sensitivity linearly, causing a linear increase in the necessary noise
- A more distributed server topography drastically improves latency and evenly the computational costs

There are several improvements that could explored in future research:

- Making the server network more distributed as to decrease vulnerability to DDoS attacks
- Finding a way to decrease the Laplace sensitivity, thus decreasing the necessary noise
- Adopting this protocol for real-time low latency communications
- Expanding the number of concurrent user connections

Contact

Alexander Yang
Distributed Systems Lab, University of Pennsylvania
Email: ayang015@seas.upenn.edu
Phone: 651-280-7946

References

1. J. van den Hooff, D. Lazar, M. Zaharia, and N. Zeldovich. Vuvuzela: Scalable private messaging resistant to traffic analysis. In Proceedings of the ACM Symposium on Operating Systems Principles (SOSP), Oct. 2015.
2. Lazar, D., Gilad, Y., & Zeldovich, N. (2018). Karaoke: Distributed Private Messaging Immune to Passive Traffic Analysis. *OSDI*. Retrieved from https://www.usenix.org/conference/osdi18/presentation/lazar
3. Kairouz, P., Oh, S., & Viswanath, P. (2015). The Composition Theorem for Differential Privacy. *MLR* . Retrieved from http://proceedings.mlr.press/v37/kairouz15.pdf
4. Roth, A., & Dwork, C. *The Algorithmic Foundations of Differential Privacy* (Vol. 9).